Politica della Sicurezza delle informazioni

Politiche del Sistema di Gestione per la Sicurezza delle Informazioni

redatto da:	**F. Marabini**	verificato da:	**F. Marabini**	approvato da:	**D. Metta**
revisione:	**7**	data emissione:	**10 ottobre 2022**		
doc ID	**PL_01**				

Note di riservatezza: Documento pubblico
Copia non controllata; il documento controllato è disponibile nella cartella di rete "Agrea ISO 27001 Documentazione"

Stato del documento

revisione	data	sintesi dei cambiamenti	(approvato da)
0	19/09/2012	Prima emissione	Spatari
1	08/07/2016	Aggiornamenti organizzativi e normativi	Lorenzini
2	07/09/2017	Aggiornamenti organizzativi e normativi	Lorenzini
3	13/09/2018	Aggiornamenti organizzativi e normativi	Metta
4	04/09/2019	Aggiornamenti normativi, Politica Analisi dei rischi, Politica Continuità operativa	Metta
5	7/10/2020	Aggiornamento della struttura del documento ed integrazione di principi specifici per diversi ambiti (Uso accettabile degli asset, Gestione degli asset, Backup, Compliance, Gestione degli incidenti e Sicurezza nelle comunicazioni) e di una politica specifica sui Dispositivi rimovibili e sulla Gestione dei cambiamenti.	Metta
6	02/08/2021	Aggiornamento del documento con specifico paragrafo sul lavoro da remoto.	Metta
7	10/10/2022	Aggiornamenti normativi ed organizzativi	Metta

Acronimi

Acronimo	Descrizione
CDS	Comitato Direttivo per la Sicurezza
COS	Comitato Operativo per la Sicurezza
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni

Riferimenti

Codice	Titolo
ISO/IEC 27001:2013	Tecnologie informatiche. Tecniche per la sicurezza – Sistemi di gestione per la sicurezza delle informazioni – Requisiti

Diffusione & Riservatezza del documento

Il presente documento è considerato “Pubblico” in quanto contiene informazioni che possono essere comunicate liberamente senza che vi possano essere conseguenze negative per AGREA o che proprio per la loro natura devono essere diffuse senza limitazioni o preclusioni.

Contenuti

1 INTRODUZIONE

AGREA considera il sistema di gestione e le informazioni gestite, per il particolare rilievo che hanno assunto per il perseguimento dei propri fini istituzionali, parte integrante del proprio patrimonio. E' obiettivo di assoluta priorità per AGREA, salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

In tale contesto si intende per:

Riservatezza la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati.

Integrità la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico e sia stata modificata in modo legittimo da soggetti autorizzati.

Disponibilità la garanzia di reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura.

Autenticità la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa.

La Politica di Sicurezza delle Informazioni in AGREA ha quindi l'obiettivo di proteggere le risorse informative da tutte le minacce, siano esse organizzative o tecnologiche, interne o esterne, accidentali o intenzionali.

A tal fine AGREA approva il presente documento finalizzato a:

- garantire la riservatezza delle informazioni;
- mantenere l'integrità delle informazioni;
- assicurare la disponibilità dei servizi informatici;
- rispettare i requisiti normativi, legislativi e le regole interne;
- formare il personale alla sicurezza delle informazioni;
- tenere traccia e studiare qualsiasi incidente, reale o presunto, che interessi la sicurezza delle informazioni;
- stabilire regole, elaborare piani e adottare misure per attuare la migliore politica di sicurezza delle informazioni;

ed inoltre di:

- indicare il Direttore dell'Agenzia quale responsabile della attuazione della Politica di sicurezza delle informazioni;
- stabilire che i Dirigenti ed i Responsabili di Posizioni Organizzative (P.O.) sono responsabili nei rispettivi servizi e funzioni, della applicazione e del rispetto della Politica di sicurezza delle informazioni;
- assegnare ad ogni operatore dell'Agenzia, dipendente e/o collaboratore, la responsabilità per il rispetto della politica di sicurezza delle informazioni.

2 CAMPO DI APPLICAZIONE E DESTINATARI

La politica di sicurezza delle informazioni è valida per l'intera Agenzia, con riferimento principale alla funzione di Organismo Pagatore Regionale.

La politica si applica a tutte le informazioni trattate nell'ambito sopra definito, qualsiasi natura e forma esse abbiano o prendano, e a tutti i sistemi di gestione e supporti di memorizzazione utilizzati per il loro trattamento e conservazione.

I destinatari della politica sono tutti i collaboratori dell'Agenzia dipendenti o consulenti, a tempo pieno e a tempo determinato. Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi di AGREA, nonché i visitatori e gli ospiti.

In particolare, sono tenuti al rispetto della politica di sicurezza, i fornitori di servizi informatici per la loro tipica condizione di operare direttamente sui sistemi di gestione delle informazioni.

A tal proposito, nei contratti con tutti fornitori di servizi vengono inserite apposite clausole di riservatezza e di sicurezza delle informazioni.

3 RIFERIMENTI NORMATIVI

La materia della sicurezza delle informazioni è disciplinata dalla legislazione comunitaria e dalla legislazione italiana. Qui si riportano le norme più recenti e più importanti in materia di protezione dei dati personali e le norme che si riferiscono in modo specifico alla certificazione ISO 27001 degli organismi pagatori.

Normativa sulla protezione dei dati personali

Regolamento UE 679/2016, "Regolamento generale sulla protezione dei dati personali" (GDPR);

D.lgs. n.196 del 30 giugno 2003, "Codice in materia di protezione dei dati personali";

D.lgs. n.101 del 10 agosto 2018, "Modifiche al Codice in materia di protezione dei dati personali";

D.lgs. 7 marzo 2005 n.82, "Codice Amministrazione Digitale" (CAD);

D.lgs. 22 agosto 2016 n.179 modifiche al CAD;

D.lgs. 13 dicembre 2017 n.217 ulteriori modifiche al CAD;

Normativa sulla certificazione ISO 27001 degli organismi pagatori

Reg. (CE) 11/03/2014, n. 907/2014 "Regolamento delegato della Commissione che integra Regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio per quanto riguarda gli organismi pagatori e altri organismi, la gestione finanziaria, la liquidazione dei conti, le cauzioni e l'uso dell'euro".

D.M.12/1/2015 del MIPAAF Ministero delle politiche agricole, alimentari e forestali "Semplificazione della gestione della PAC 2014-2020".

In materia di certificazione ISO 27001 degli Organismi Pagatori la Commissione Europea aveva emanato una apposita circolare che stabiliva quanto segue:

- Ai sensi degli articoli 1 e 2 del Regolamento (UE) n 907/2014, gli organismi pagatori possono essere accreditati dagli Stati membri solo se rispettano determinati criteri minimi e se hanno una struttura amministrativa e un sistema di controllo interno conformi con i criteri di cui all'allegato I (criteri di accreditamento) di tale regolamento.

- Ai sensi del punto 3 dell'allegato I del suddetto Regolamento, la sicurezza dei sistemi informativi degli organismi pagatori, responsabili per la gestione e il controllo di una spesa annua superiore a 400 milioni di euro, sono certificati in conformità agli Standard Organizzativi Internazionali 27001 relativi ai Sistemi di Gestione della Sicurezza delle Informazioni (Requisiti ISO) a partire dal 16 ottobre 2016. In questo contesto, si ricorda che vari organismi pagatori sono già certificati o in corso di certificazione entro la fine dell'esercizio 2016.

- Nel caso in cui la spesa dell'organismo pagatore è inferiore a 400 milioni di euro lo standard di sicurezza scelto è ISO 27002; la versione corretta è ISO 27002:2013 nel corso dell'esercizio 2016.

4 PROFILO DI MINACCIA

AGREA istituita con L.R. n. 21 del 23 luglio 2001 e dotata di piena autonomia amministrativa, organizzativa e contabile, è l'Ente regionale che, in qualità di Organismo Pagatore Regionale (OPR) riconosciuto dall'Unione Europea, ha come "mission" l'erogazione di aiuti, contributi e premi previsti da disposizioni comunitarie, nazionali e regionali, a favore degli operatori del settore agricolo.

AGREA per supportare in modo efficiente e tempestivo il complesso delle azioni connesse alla sua missione, oltre ad avvalersi dei servizi informatici e di rete della Regione Emilia-Romagna, ha realizzato un proprio sistema informativo ad alto contenuto innovativo.
Il sistema informativo che supporta la gestione delle attività di AGREA è in grado di governare le diverse fasi attraverso cui si perviene all'erogazione del contributo e, per ciascuna fase, tramite check-list guida l'operatore nelle attività da svolgere. Il sistema memorizza i dati dell'utente, individua la struttura/ente a cui appartiene e registra le variazioni apportate ai dati a cui ha accesso.
Il Sistema informativo utilizza, per l'ampiezza territoriale ed il numero di attori coinvolti, in modo intenso le tecnologie della comunicazione.
Questa necessità rende le informazioni trasmesse, soggette ad intrusioni e conseguenti rilevazioni illegali e possibili modifiche.

In generale, le minacce a cui deve far fronte AGREA, sono riassumibili nelle seguenti (elenco non esaustivo):

- accesso e/o diffusione non autorizzata di dati, anche contenenti informazioni personali comuni/particolari (requisito minacciato: riservatezza);
- salvataggio di un dato non corretto (requisito minacciato: integrità);
- perdita di dati (requisito minacciato: integrità);
- indisponibilità dei servizi specifici erogati dall'Organismo pagatore (requisito minacciato: disponibilità).

5 OBIETTIVI SULLA SICUREZZA DELLE INFORMAZIONI

Gli obiettivi di sicurezza delle informazioni sono legati alla missione di AGREA come Organismo Pagatore:

- Garantire un livello adeguato dei requisiti di riservatezza, integrità e disponibilità nei servizi erogati attraverso specifici applicativi;
- Garantire un adeguato livello di consapevolezza al personale, ai collaboratori, ai soggetti convenzionati e ai fornitori esterni;
- Mantenere allineato l'SGSI rispetto ai cambiamenti nelle procedure interne e nelle modalità di erogazione dei Servizi di AGREA;
- Garantire un adeguato Governo dei Fornitori al fine di assicurare il rispetto dei requisiti di sicurezza delle informazioni.

6 SISTEMA DI GESTIONE E POLITICHE

Le politiche di sicurezza delle informazioni di AGREA sono attuate per proteggere, per quanto possibile e comunque ad un livello ottimale e ad un costo compatibile con le specificità dell'Agenzia, il Sistema di gestione delle informazioni da eventi intesi come *minacce* o *incidenti*, esterni e/o interni, oggettivi e/o soggettivi che possono compromettere l'erogazione dei servizi.

Lo scopo di questi paragrafi è illustrare i principi che AGREA ha definito per la sicurezza delle informazioni, al fine di allineare i comportamenti del personale alla strategia dell'organizzazione.

6.1 *Uso accettabile degli asset*

L'obiettivo della seguente politica è indirizzare i comportamenti degli utenti relativamente agli asset utilizzati, allo scopo di prevenire l'accesso non autorizzato informazioni.

L'uso dei sistemi di elaborazione delle informazioni, da parte di coloro che vi operano, a qualunque livello e a qualsiasi rapporto, è regolato dal "Disciplinare tecnico per utenti dei servizi informativi della Regione Emilia – Romagna".

La verifica del corretto utilizzo di tutte le strumentazioni informatiche messe a disposizione degli utenti, è regolata dal "Disciplinare tecnico per le verifiche di sicurezza sul sistema informativo regionale".

Tali disciplinari regionali trovano applicazione anche con riferimento all'Agenzia.

Di seguito si elencano regole e principi applicabili:

- AGREA considera i sistemi di elaborazione delle informazioni, come strumenti di lavoro. Gli strumenti messi a disposizione devono essere utilizzati per lo svolgimento dell'attività lavorativa in modo strettamente pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi stessi e della rete, e tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche;
- AGREA, conformemente alla normativa regionale, ammette l'uso degli strumenti informatici ed in particolare di Internet, per motivi personali, soltanto in caso di urgenza e comunque non in modo ripetuto e per periodi di tempo prolungati, in ogni caso sempre nel rispetto del principio di riservatezza e dell'esigenze di funzionalità della rete e di semplificazione dei processi lavorativi;
- Al fine di evitare il rischio di perdita di dati importanti, i collaboratori sono invitati a utilizzare lo spazio in modalità "cloud" per la memorizzazione dei dati personali degli utenti, in linea con quanto previsto dalle policy regionali;
- In caso di furto o smarrimento, è necessario provvedere tempestivamente alla segnalazione dell'evento, secondo quanto descritto nella procedura di gestione degli incidenti di sicurezza.

6.2 *Lavoro da remoto*

L'obbiettivo della seguente politica è quello di garantire che, nel caso di Telelavoro, Smart-working Ordinario/Straordinario ed in generale di attività svolte al di fuori della sede di AGREA, siano rispettati gli stessi requisiti di sicurezza garantiti dall'utilizzo delle postazioni di lavoro all'interno della sede di AGREA.

Di seguito si elencano regole e principi applicabili:

- È necessario attenersi al "*Disciplinare tecnico per utenti dei sistemi informativi della regione Emilia-Romagna*", con particolare attenzione al Capitolo 8;
- È necessario rispettare quanto indicato nella presente "Politica della Sicurezza delle informazioni", con particolare attenzione al Capitolo "Uso accettabile degli asset".

Qualora si utilizzino PC personali per lo svolgimento delle attività lavorative, sono valide le seguenti raccomandazioni:

- i dispositivi personali utilizzati devono essere periodicamente aggiornati, tramite l'installazione dei pacchetti software resi disponibili dai Vendor;
- i dispositivi personali utilizzati devono essere provvisti di Antivirus/Antimalware;
- i dispositivi personali devono essere protetti tramite una password a protezione del dispositivo ed un blocca schermo che si attiva dopo 15 minuti dall'abbandono della postazione;
- la documentazione relativa alle attività lavorative non deve essere archiviata sul dispositivo, ma deve essere memorizzata in cloud, in linea con quanto previsto dalle policy regionali;
- in caso di furto o smarrimento, è necessario provvedere tempestivamente alla segnalazione dell'evento, secondo quanto descritto nella procedura di gestione degli incidenti di sicurezza.

Inoltre, AGREA sconsiglia e limita l'utilizzo dello smartphone personale per lo svolgimento di attività lavorative e raccomanda quanto segue:

- un costante aggiornamento del sistema operativo e delle applicazioni utilizzate nel dispositivo personale;
- il download delle applicazioni utilizzate da piattaforme sicure/certificate (quali ad esempio: Play Store o App Store);
- l'utilizzo (se possibile) di applicazioni che impongano l'uso di un canale sicuro end-to-end durante l'invio di informazioni su qualsiasi rete;
- l'utilizzo di un sistema di criptaggio del dispositivo protetto tramite password di sicurezza;
- di evitare di memorizzare mai la password e lo username dell'account lavorativo all'interno del dispositivo;
- l'installazione sul dispositivo di un Antivirus/Antimalware;
- di evitare di archiviare la documentazione relativa all'attività lavorativa nello smartphone, privilegiando l'utilizzo del cloud;
- in caso di furto o smarrimento, di provvedere tempestivamente alla segnalazione dell'evento, secondo quanto descritto nella procedura di gestione degli incidenti di sicurezza.

6.3 *Dispositivi rimovibili*

L'obiettivo della seguente politica è indirizzare i comportamenti degli utenti relativamente ai supporti rimovibili (es. floppy disk, dischi ZIP, CD-ROM, nastri,..), allo scopo di prevenire l'accesso non autorizzato ai documenti.

Informazioni sulle modalità di utilizzo dei dispostivi mobili sono contenute nel ***Disciplinare per utenti*** adottato dalla Regione Emilia-Romagna.
Di seguito si elencano regole e principi applicabili:

- AGREA limita l'utilizzo dei supporti removibili e prescrive quanto segue:
  - i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) ed azioni non consentite: in particolare, essi devono essere

conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare a distruggere il supporto, se necessario, per i fini in esame.

6.4 *Gestione degli asset*

L'obiettivo della presente politica è assicurare che tutti gli asset associati al servizio di conservazione siano stati opportunamente identificati e inventariati e che sia stato individuato un responsabile al fine di gestire le minacce associate alla sicurezza delle informazioni.

Di seguito si elencano regole e principi applicabili:

- le risorse hardware e software utilizzate dall'Agenzia devono essere identificate**,** classificate e registrate, al fine di tracciare l'intero "ciclo di vita": acquisizione, assegnazione, aggiornamento, manutenzione, dismissione;
- deve essere utilizzato un inventario delle risorse informatiche per monitorare l'obsolescenza delle risorse utilizzate, pianificare il loro ammodernamento, rinnovare le licenze e programmare gli investimenti in tecnologie dell'informazione;
- deve essere individuato un gestore ed un Responsabile dell'inventario delle risorse informatiche; la gestione è affidata al Referente della informatizzazione interna e gestione infrastrutture informatiche mentre la responsabilità è in capo al Responsabile dei sistemi informativi e gestione della sicurezza informatica;
- le risorse hardware devono essere classificate e per ciascuna di esse sono definite le caratteristiche tecniche, il fornitore da cui sono state acquisite, l'anno e la modalità di acquisizione, ecc., utili sia per una corretta gestione delle garanzie, sia per una gestione efficace della manutenzione e/o aggiornamento;
- I programmi software devono essere classificati e per ciascuno di essi deve essere individuata la tipologia, il produttore, il fornitore, e nel caso di acquisizione con licenza d'uso l'anno di acquisizione utile per il pagamento dei relativi canoni di licenza annuali;
- ogni qualvolta si dismette un dispositivo che contiene dati personali (comuni o particolari), è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

6.5 *Analisi dei rischi*

L'obiettivo della presente politica è assicurare che i rischi associati ai servizi siano identificati, valutati e trattati.

Di seguito si elencano regole e principi applicabili:

- a base della politica di tutela delle informazioni deve essere posta una idonea Analisi dei Rischi di tutte le risorse (asset) che costituiscono il sistema di gestione delle informazioni, al fine di comprendere le vulnerabilità, di valutare le possibili minacce e di predisporre le necessarie contromisure (di prevenzione e di protezione) per ridurre il rischio ad un livello accettabile;
- tutte le attività di controllo, le Politiche in merito alla sicurezza e le procedure operative legate alla sicurezza delle informazioni devono discendere dall'Analisi dei Rischi;
- deve essere definita un'analisi dei rischi che consenta ad AGREA di:

  - Analizzare e gerarchizzare i rischi e le opportunità nell'organizzazione (*Analisi a livello di processo di security: che cosa è accettabile e che cosa non lo è*),
  - Valutare e pianificare azioni per affrontare i rischi (*Come posso evitare, eliminare o mitigare i rischi*),
  - Attuare il piano definito (*Condurre le azioni*),
  - Controllare l'efficacia delle azioni (*Le azioni adottate funzionano?*),
  - Apprendere dall'esperienza (*Miglioramento continuo*).
- l'Analisi dei Rischi deve essere condotta da AGREA con cadenza periodica e regolare, a garanzia del permanere dell'efficacia delle misure di mitigazione identificate e attuate.

6.6 *Controllo degli accessi*

L'obiettivo della seguente politica è garantire l'accesso sicuro alle informazioni conservate, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti (interni o esterni) che non possiedono i necessari diritti.

Per l'accesso alla rete regionale (autenticazione) si fa riferimento alle regole tecniche ed organizzative per la sicurezza della rete, dei dati e delle informazioni trattate con l'ausilio di strumenti elettronici, descritte nel "*Disciplinare per utenti dei sistemi informativi* della Regione Emilia-Romagna". AGREA provvede a dotare i propri collaboratori all'atto del proprio insediamento, della credenziale d'accesso alla rete regionale.

Di seguito si elencano regole e principi applicabili:

- devono essere impediti accessi non autorizzati tramite procedure di controllo dei collaboratori dell'Agenzia e dei soggetti appartenenti a strutture esterne che, in forza di titolo (delega, contratto, accordo o convenzione), accedono alle applicazioni dell'Agenzia.
- devono essere protette le informazioni ed i sistemi di elaborazione e di comunicazione con misure tecnologiche ed organizzative atte a garantire il controllo degli accessi, la qualità delle informazioni, nonché la loro riservatezza ed integrità.
- devono essere adottate le seguenti Regole di Accesso:
  - I collaboratori interni ed i soggetti esterni (utenti) devono accedere solo ai sistemi a cui sono stati autorizzati. Ogni abuso di accesso a sistemi diversi da quelli autorizzati, è perseguito ai sensi dell'**articolo 615-ter del Codice Penale "Accesso abusivo ad un sistema informatico o telematico**.
  - Qualora gli utenti dovessero accedere in modo incidentale a sistemi o ad applicazioni AGREA senza autorizzazione, sono tenuti a disconnettersi e segnalare l'anomalia all'indirizzo di posta *agreautenze@regione.emilia-romagna.it .*
  - Per l'Accesso alle applicazioni (autorizzazioni)
    - devono essere abilitati collaboratori propri ed appartenenti ad enti o organizzazioni con i quali è in essere un rapporto, ad essere autorizzati come utenti dei propri sistemi di elaborazione dell'informazione.
    - deve essere adottata la *profilazione degli utenti*, sia interni che esterni, per la concessione della credenziale d'accesso alle applicazioni e deve essere utilizzata a tal fine una "procedura formale" mantenendo documentazione, cartacea ed elettronica, delle autorizzazioni concesse.

- deve essere effettuato, da parte del Responsabile della Sicurezza, un controllo periodico (almeno una volta all'anno) della validità funzionale di tutte le autorizzazioni attive per l'accesso alle applicazioni di AGREA
- la revoca all'accesso ai sistemi di elaborazione delle informazioni di AGREA deve essere attuata qualora decadano le caratteristiche di abilitazione di un utente.

- Per quanto riguarda le Caratteristiche e la gestione delle password:
  - la password, conformemente alle norme di sicurezza informatica, deve essere considerata come una "informazione confidenziale di autenticazione composta da una serie di caratteri e/o simboli", utilizzata per l'accesso ai sistemi di elaborazione dell'informazione.
  - devono essere generate e assegnate password individuali e l'utente è responsabile della sua riservatezza.
  - La struttura delle password generate dai sistemi di AGREA deve presentare le seguenti caratteristiche informative e gestionali:
    - lunghezza minima 10 caratteri
    - dovrà contenere almeno un carattere numerico
    - dovrà contenere almeno una lettera maiuscola ed almeno una minuscola
    - dovrà contenere almeno un carattere non alfanumerico (esempio: *, _, %...)
    - dovrà essere diversa dalle precedenti 3 password già utilizzate
    - Durata password 90 giorni.

6.7 *Sicurezza nello sviluppo applicativo*

L'obiettivo della seguente politica è quello di assicurare che gli aspetti di sicurezza siano inclusi nelle fasi di progettazione e sviluppo del software di conservazione, anche in relazione all'architettura di erogazione del servizio.

Il processo di realizzazione delle applicazioni informatiche in AGREA deve essere realizzato in coerenza con gli obiettivi indicati nelle linee di sviluppo del Sistema Informativo dell'Agenzia, contenuto nella Relazione di Bilancio, ed uniformato alle indicazioni contenute nel "Disciplinare Tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna".

Di seguito si elencano regole e principi applicabili:

- Lo sviluppo delle applicazioni software (fuori ambito SGSI) deve avvenire in coerenza con la strategia dell'Agenzia e deve essere orientato al supporto delle attività operative e direzionali, in una logica di ottimizzazione dell'efficienza, efficacia, qualità e sicurezza della informazione ed in un contesto di massimizzazione del rapporto tra costi/benefici.
- Il processo di realizzazione delle applicazioni informatiche in AGREA, siano esse nuove applicazioni o modifiche e/o manutenzioni di natura correttiva o evolutiva di quelle esistenti richiesti da variazioni normative, organizzative o da utenti, devono svolgersi secondo i seguenti criteri:
  - pianificazione e controllo delle varie fasi: analisi, disegno, sviluppo, deployment, test;
  - conformità alle direttive comunitarie e nazionali sulla sicurezza delle informazioni.

6.8 *Gestione delle licenze*

L'obiettivo della seguente politica è quello di assicurare la corretta gestione del ciclo di vita delle licenze, in conformità alla normativa.

Di seguito si elencano regole e principi applicabili:

- i collaboratori, gli utenti e gli amministratori sono autorizzati ad utilizzare il software, acquisito da AGREA tramite pagamento delle relative licenze;
- è consentito l'uso solo di software autorizzato installato sui sistemi all'atto della consegna ed è considerato illegale, ai sensi del D.Lgs. 9 aprile 2003, n. 68 "Attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione", l'uso di software acquisito ed utilizzato senza regolare licenza d'uso. La Regione Emilia - Romagna si riserva di effettuare dei controlli a campione sul rispetto di questa policy.
- Nel caso sia necessaria l'installazione di software aggiuntivi, deve esserne fatta specifica richiesta al Responsabile della sicurezza delle informazioni.

6.9 *Sicurezza fisica*

L'obiettivo della seguente politica è quello di prevenire l'accesso non autorizzato alle sedi e ai locali dell'organizzazione e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.

L'accesso ai locali ove risiedono i sistemi server del sistema informativo OPR presso i Datacenter della Regione Emilia – Romagna è regolamentato da "*Disciplinare Tecnico relativo al controllo degli accessi ai locali della Regione Emilia-Romagna*". L'accesso ai locali di AGREA è regolamentato nel documento "Gestione e controllo della Sicurezza fisica".

Di seguito si elencano regole e principi applicabili:

- devono essere previste misure fisiche dirette a garantire i servizi di controllo contro accessi non autorizzati ai locali ove sono ubicati i sistemi di gestione dell'informazione, al fine di preservare l'integrità e la disponibilità dei sistemi di elaborazione dell'informazione di AGREA.
- le aree che comprendono i locali ove risiedono i sistemi di gestione dell'informazione dell'Agenzia devono essere dotate di porte ad accesso controllato.
- i locali devono essere dotati di sistemi, atti a garantire e mantenere la sicurezza e l'integrità delle apparecchiature e degli impianti, al fine di evitare guasti che possono causare interruzione fisica al funzionamento delle attività.
- Tutti i sistemi e apparecchiature di rete devono essere ubicati in edifici sicuri e con accesso vigilato. In particolare, i locali ove risiedono i sistemi server del sistema informativo OPR sono "*aree ad accesso ristretto"* e l'ammissione è consentita solo in presenza di personale interno autorizzato.

6.10 *Backup*

L'obiettivo della seguente politica è quello di considerare opportunamente, nella fase di realizzazione ed esercizio, gli aspetti di sicurezza relativamente all'adozione di procedure di backup e ripristino dei dati.

Di seguito si elencano regole e principi applicabili:

- adeguate misure e strumenti di backup in funzione dell'importanza dei sistemi e dei dati;
- supporti di backup devono essere conservati in una location differente rispetto a quella in cui sono conservati i dati originari;
- il processo di back up e restore dei dati deve essere periodicamente testato e gli esiti documentati.

6.11 *Compliance*

L'obiettivo della seguente politica è quello di garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni reputazionali.

AGREA adotta la politica e le misure previste per il trattamento dei dati personali come descritta nel "Documento programmatico della Sicurezza" (DPS), redatto annualmente ai sensi del "Codice della protezione dei dati personali".

In conseguenza della completa entrata in vigore del GDPR (Regolamento 2016/679 del Parlamento europeo e del Consiglio, del 27/04/2016) e dell'approvazione del relativo decreto di adeguamento (Decreto Legislativo 10 agosto 2018, n. 101) la disciplina in materia di trattamento dei dati personali ha ricevuto una nuova organizzazione da parte della Regione Emilia - Romagna stabilita con la delibera della Giunta regionale n.1123 del 15 luglio 2018, che è stata recepita e contestualizzata nell'organizzazione dell'Agenzia con la determina n. 1539 del 21 dicembre 2018.

Successivamente l'organizzazione in materia di trattamento dei dati personali è stata aggiornata con delibera della Giunta regionale n.1004 del 20 giugno 2022, che è stata recepita e contestualizzata nell'organizzazione dell'Agenzia con determinazione n.1279 del 26 settembre 2022.

Deve essere garantito il rispetto dei requisiti in merito a:

- disposizione di legge applicabili in merito alla protezione dei dati personali e relativi Provvedimenti del garante, in riferimento ai dati trattati sia in qualità di titolare del trattamento, sia in qualità di responsabile del trattamento nell'ambito dei servizi erogati da AGREA. In particolare:
    - i collaboratori di AGREA devono essere autorizzati annualmente con apposita determina del Direttore a determinati trattamenti dei dati personali, venendo in tal modo formalmente incaricati a tali specifici trattamenti e sono conseguentemente informati e formati sulle modalità e comportamenti da mantenere durante il trattamento dei dati personali medesimi.
    - i dipendenti ed i collaboratori di enti e imprese che a vario titolo utilizzano, in nome e per conto ovvero autorizzati in base ad uno specifico titolo (convenzione, contratto, accordo, ecc.), i sistemi di gestione delle informazioni e di rete dell'Agenzia, sono tenuti ad osservare le regole contenute nel DPS.
    - i fornitori di servizi informatici, trattando dati personali di cui l'Agenzia è titolare, devono essere nominati Responsabili del trattamento dei dati personali, con tutti gli obblighi previsti dal codice della privacy.
- disposizioni di legge in merito agli organismi pagatori;
- norma ISO/IEC 27001:2013;

- obblighi contrattuali legati al servizio, con particolare riferimento agli obblighi in materia di protezione dei dati.

6.12 *Gestione degli incidenti*

L'obiettivo della seguente politica è quello di garantire che gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza delle informazioni dell'organizzazione siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.

Per incidente di sicurezza delle informazioni (di seguito "incidente") si intende un evento accidentale o un'azione deliberata potenzialmente in grado di compromettere almeno uno dei requisiti di sicurezza del sistema di conservazione.

Un incidente, nell'ambito della sicurezza dell'informazione, è un evento sospetto o una vulnerabilità tale da violare l'integrità, la riservatezza e/o la disponibilità delle applicazioni, dei dati e/o dei sistemi di elaborazione delle informazioni.

Tutti gli utenti devono attenersi alle indicazioni ricevute in materia di sicurezza delle informazioni e contenute nel *"Disciplinare per utenti dei sistemi informativi della Regione Emilia-Romagna" e nel "Disciplinare per la gestione degli Incidenti di sicurezza e Data breach".*

Di seguito si elencano regole e principi applicabili:

- Gli utenti che individuano o abbiano il sospetto riguardante un incidente al sistema di sicurezza, devono segnalarla tempestivamente, secondo le modalità previste dalle procedure interne.
- Gli incidenti rilevati devono essere comunicati a tutti i soggetti coinvolti (comprese le autorità rilevanti).
- Gli eventi/incidenti devono essere rilevati e gli eventuali danni devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure condivise con tutti i soggetti interessati.
- Deve esistere un sistema di registrazione e classificazione degli incidenti per effettuare analisi volte al miglioramento dei livelli di sicurezza delle informazioni coerentemente con le reali problematiche riscontrate.

6.13 *Continuità operativa*

L'obiettivo della seguente politica è quello di garantire la continuità operativa del servizio di conservazione e l'eventuale ripristino tempestivo dei servizi erogati nel momento in cui siano stati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze di tali eventi sia all'interno che all'esterno del contesto dell'organizzazione.

L'obiettivo della Gestione della Continuità Operativa è assicurare la continuità dei processi/servizi essenziali di un'organizzazione (processi critici) ad un determinato livello di servizio, nell'eventualità di un evento disastroso.

L'Agenzia riconosce che i sistemi di elaborazione delle informazioni sono elementi di criticità per la corretta erogazione dei servizi e una loro prolungata indisponibilità risulta essere altamente dannosa per l'operatività dell'Agenzia, in particolare per l'erogazione dei servizi in qualità di OPR.

Di seguito si elencano regole e principi applicabili:

- deve essere definito un Business Continuity Plan - BCP, inteso come indicazione delle attività organizzative e tecnologiche, finalizzate alla continuità dei processi che concorrono alla missione dell'Agenzia, al fine di contenere l'impatto di eventuali avvenimenti disastrosi con impatto sui servizi erogati da AGREA, nell'ambito dei requisiti di ripristino definiti.
- il piano deve essere opportunamente comunicato e aggiornato;
- il piano deve essere periodicamente sottoposto a test di verifica;
- deve essere definita all'interno dell'organizzazione la responsabilità relativa alla "Continuità Operativa" e alla redazione del BCP, che per l'Agenzia è in capo al Direttore.

6.14 *Sicurezza delle comunicazioni*

L'obiettivo della seguente politica è quello di garantire che siano opportunamente considerati gli aspetti di sicurezza nelle tematiche relative alla sicurezza delle comunicazioni (Network security: segregazione delle reti, monitoraggio dei gateway (firewall)).

Per garantire la sicurezza delle reti e delle comunicazioni occorre prevenire l'accesso alle reti e l'utilizzo illegale di informazioni, da parte di soggetti non autorizzati al fine di preservare la riservatezza dei dati e la disponibilità del servizio.

Il "*Disciplinare per utenti dei sistemi informativi* della Regione Emilia-Romagna" contiene le raccomandazioni sulla sicurezza della rete interna, le regole per la navigazione in Internet e le indicazioni per l'uso appropriato della posta elettronica e la protezione contro il software malevolo.

Di seguito si elencano regole e principi applicabili:

Tutti i flussi contenenti pacchetti informativi in entrata e in uscita nell'esercizio dei servizi di AGREA devono essere protetti mediante opportuni protocolli di crittografia (HTTPS).

6.15 *Relazioni con autorità esterne e gruppi specialistici*

L'obiettivo della seguente politica è quello di garantire che siano stati identificati i referenti per mantenere le necessarie relazioni con le autorità esterne.

AGREA intrattiene contatti, se necessario, con la Polizia Postale e le autorità di pubblica sicurezza.

L'Agenzia mantiene e sviluppa relazioni continue e specifiche con la Regione Emilia - Romagna (Settore innovazione digitale, dati, tecnologia e polo archivistico) su aspetti per la sicurezza delle informazioni.

Inoltre, gli Amministratori di sistema ricevono la Newsletter di Agenzia digitale, che consultano per aspetti di sicurezza delle informazioni.

6.16 *Gestione dei Cambiamenti*

L'obiettivo della seguente politica è quello di garantire che i cambiamenti che coinvolgono i servizi di AGREA siano opportunamente gestiti al fine di evitare impatti negativi sulla sicurezza delle informazioni.

Di seguito si elencano regole e principi applicabili:

- I cambiamenti devono essere opportunamente comunicati ai soggetti interessati;
- Nel caso di cambiamenti significativi, questi devono essere gestiti tramite progetti specifici, documentati a cura di un Responsabile definito, secondo l'ambito di competenza.

7 ORGANIZZAZIONE PER LA SICUREZZA DELLE INFORMAZIONI

Per attuare una politica di Sicurezza delle Informazioni efficiente ed efficace è necessario stabilire una struttura organizzativa che sia in grado di definire, implementare e controllare l'applicazione della Politica stessa. Per questo motivo, a supporto della gestione della sicurezza delle informazioni, AGREA si è dotata di un'adeguata struttura organizzativa descritta nel presente paragrafo.

7.1 *Direzione*

Il Direttore è il responsabile dei contenuti della politica di sicurezza delle informazioni, della sua emanazione, attuazione ed aggiornamento. Il Direttore si avvale del supporto tecnico ed organizzativo del Comitato Direttivo per la Sicurezza (CDS) e del Comitato Operativo per la Sicurezza (COS), di cui ai successivi punti 7.2 e 7.3, per la definizione e attuazione della politica di sicurezza delle informazioni.

Le responsabilità della Direzione posso essere così riassunte:

- stabilire e approvare la Politica per la Sicurezza delle Informazioni, che includa Obiettivi di Sicurezza delle Informazioni compatibili con gli indirizzi strategici dell'organizzazione;
- garantire che la Politica per la Sicurezza delle Informazioni sia comunicata all'interno dell'organizzazione e alle parti interessate, laddove necessario;
- divulgare l'importanza di un'implementazione efficace del SGSI e promuovere un incremento complessivo della cultura della sicurezza all'interno dell'Organizzazione;
- assicurare le risorse necessarie per il sistema di gestione per la sicurezza delle informazioni (strumentali, finanziarie, umane), coerenti con i livelli di rischio dell'Organizzazione;
- riesaminare, ad intervalli pianificati, il Sistema di Gestione per la Sicurezza delle Informazioni, per assicurarne la continua idoneità, adeguatezza ed efficacia.

7.2 *Comitato Direttivo per la Sicurezza (CDS)*

Il CDS (Comitato Direttivo per la Sicurezza), è l'organo decisionale in termini di politiche ed investimenti da sostenere e la sua composizione, definita in armonia all'organizzazione di AGREA è descritta di seguito in questo paragrafo.

La partecipazione al CDS può essere ampliata di volta in volta qualora ci sia l'esigenza di esaminare temi specifici. Il CDS ha la funzione di supportare il Direttore nella ricerca ed indicazione delle linee guida e delle migliori modalità di applicazione della politica di sicurezza delle informazioni.

Il CDS è composto da:

- Direttore AGENZIA
- Dirigente del SETTORE Tecnico e di Autorizzazione
- Dirigente del SETTORE Gestione Contabile dell'OPR, Approvvigionamenti e Certificazioni
- Dirigente AREA Servizi IT

Il CDS si riunisce con cadenza annuale, salvo necessità specifiche. In assenza di problematiche di sicurezza specifiche la riunione di riesame di direzione ha valenza di riunione annuale.

Tale Comitato ha il compito di supportare il Responsabile della Sicurezza stesso per i seguenti temi:

- diffondere la Politica per la Sicurezza delle Informazioni e, più in generale una cultura della sicurezza all'interno dell'organizzazione;
- assicurare il presidio strategico sulla continuità delle attività previste dal SGSI;
- definire metodologie e processi specifici per la Sicurezza delle Informazioni;
- valutare l'adeguatezza dei controlli posti in essere per la Sicurezza delle Informazioni e il relativo monitoraggio, anche in relazione a modifiche di contesto che interessino l'organizzazione;
- ottenere consenso dalle diverse Funzioni aziendali in merito alle priorità identificabili in ambito sicurezza ed ai compromessi eventualmente necessari per lo sviluppo del programma di sicurezza;
- prendere decisioni sull'allocazione delle risorse disponibili e favorire la risoluzione di eventuali conflitti nella gestione delle risorse stesse;
- coadiuvare le funzioni preposte nella gestione di gravi incidenti di sicurezza;
- effettuare il riesame periodico del SGSI, anche in preparazione al riesame da parte della Direzione.

7.1 *Responsabile della Sicurezza delle Informazioni*

Il Responsabile della Sicurezza svolge, con il supporto del COS, le seguenti attività:

- definizione del modello di gestione dei rischi per la sicurezza delle informazioni;
- coordinamento delle attività di analisi dei rischi per la sicurezza delle informazioni;
- supporto ai Responsabili di Processo nella definizione di azioni necessarie alla riduzione del rischio;
- definizione delle strategie (opzioni) e degli obiettivi di sicurezza delle informazioni;
- definizione del programma annuale per la sicurezza delle informazioni e stima delle risorse necessarie;
- definizione dei programmi di sensibilizzazione e formazione sui temi della sicurezza delle informazioni (in collaborazione con la funzione HR);
- definizione delle Politiche e degli standard di sicurezza delle informazioni (in collaborazione con le strutture operative);
- verifica dello stato della sicurezza delle informazioni attraverso attività di revisione e verifiche tecniche e comunicazione dei risultati alle funzioni interessate;
- verifica dell'avanzamento del programma per la sicurezza delle informazioni, dei piani di trattamento e di remediation, revisione delle valutazioni di rischio residuo e comunicazione dello stato alle funzioni interessate;
- tracciamento e analisi degli incidenti di sicurezza;
- coordinamento della gestione degli incidenti di sicurezza (inclusi quelli con impatti per la compliance normativa, in coordinamento con le altre funzioni di assurance aziendale);
- consulenza e parere esperto sui temi di sicurezza delle informazioni (requisiti, gestione incidenti, minacce, …);
- coordinamento dello sviluppo dei piani di business continuity (BIA, strategy, plan development, test).

Il responsabile della sicurezza delle informazioni definisce, di concerto con CDS E COS, il Piano di sviluppo del Sistema Informativo (contenuto nella Relazione al Bilancio) nel rispetto degli obiettivi dell'Agenzia e della "Convenzione per la fruizione dei Servizi Informatici erogati dal Servizio ICT Regionale".

Il Responsabile fornisce inoltre idonea garanzia del pieno rispetto delle disposizioni vigenti in materia di sicurezza dell'informazione e dei suoi trattamenti. Organizza e sovrintende, in collaborazione con la Direzione Generale preposta della Regione Emilia-Romagna, la realizzazione della "struttura di sicurezza" finalizzata a prevenire e proteggere, in armonia con le misure di sicurezza regionali, il complesso degli archivi, delle procedure e dei sistemi, da minacce ed eventi critici al fine di garantire la continuità del servizio dell'Agenzia.

La Responsabilità della sicurezza delle informazioni è in capo al Direttore; il Referente SGSI è il Referente operativo della gestione della Sicurezza delle informazioni; Responsabile dei sistemi informativi e gestione della sicurezza informatica è Referente tecnico della sicurezza delle informazioni.

7.2 *Comitato Operativo per la Sicurezza (COS)*

Il COS è l'organo deputato ad affrontare e risolvere le problematiche di carattere operativo che possono insorgere sia nelle attività di definizione e miglioramento del Sistema di Gestione per la Sicurezza delle Informazioni, sia nell'attuazione dello stesso.

Il COS ha il compito di supportare il Responsabile della Sicurezza e si riunisce con cadenza semestrale, salvo necessità specifiche.

Il COS è composto da:

- Responsabile della funzione audit interno.
- Responsabile dei sistemi informativi e gestione della sicurezza informatica
- Responsabile degli approvvigionamenti e logistica
- Referente dell'informatizzazione interna e gestione infrastrutture informatiche.
- Referente del sistema di gestione della sicurezza delle informazioni.

Il Responsabile SGSI, coadiuvato dal COS, svolge le seguenti attività:

- definire la struttura del sistema di gestione (processi, procedure, indicatori e documentazione) integrando sia i requisiti cogenti delle normative applicabili sia i requisiti della ISO27001;
- verificare che la redazione e l'aggiornamento dei documenti del sistema di gestione rispetti i requisiti ISO 27001 e la coerenza con l'impianto di controlli definito in azienda per la gestione della sicurezza delle informazioni;
- coordinare i percorsi formativi attinenti al SGSI e verificarne l'efficacia, con il supporto del Responsabile della Sicurezza e del COS;
- interfacciarsi verso dipendenti, enti esterni ed Organismo di certificazione su tutto quanto concerne il SGSI.

Dal momento che il Responsabile della Sicurezza può scegliere e convocare i membri del COS garantendo l'adeguatezza della composizione in riferimento agli ambiti e le problematiche del caso, possono essere chiamati a partecipare al COS i responsabili delle funzioni pertinenti gli specifici aspetti che devono essere affrontati (es. Responsabili delle pertinenti Linee di Servizio).

7.3 *Responsabilità dei Dirigenti e dei Responsabili di Funzione*

E' responsabilità dei dirigenti e dei responsabili di funzione assicurarsi che:

a) i propri collaboratori
   - siano informati delle clausole di riservatezza contenute nel contratto di lavoro;
   - siano istruiti, tramite appositi corsi, previsti nel "*Piano annuale di Formazione*", circa la loro responsabilità rispetto alla sicurezza delle informazioni;
   - siano autorizzati all'accesso a sistemi o applicazioni o dati a seguito dei profili di autorizzazione definiti, coerenti con il ruolo e le attività svolte. La comunicazione per l'autorizzazione dei diritti di accesso da inviare all'Amministratore di sistema deve essere effettuata nel rispetto delle procedure specifiche di accesso dei sistemi o applicazioni o dati;
   - siano addestrati all'uso dei sistemi di elaborazione dei quali sono stati autorizzati;
   - abbiano accesso e abbiano preso conoscenza delle politiche di sicurezza dell'informazione dell'Agenzia, consultabile nei documenti della pagina Orma di Agrea.

b) la documentazione del Settore/Ufficio inerente le attività di gestione dell'informazione sia aggiornata affinché tutte le attività di lavoro ritenute critiche possano svolgersi con continuità nel caso di indisponibilità dei collaboratori addetti;

c) i cambiamenti nelle mansioni o attività dei collaboratori (per esempio in caso di spostamenti organizzativi) che comportano variazioni del profilo d'accesso ai sistemi, applicazioni e dati, siano comunicati ai relativi amministratori di sistema e, per conoscenza al Responsabile della Sicurezza delle informazioni, per variare o, se necessario, cancellare il profilo e le credenziali di accesso. La comunicazione deve essere effettuata nel rispetto delle procedure specifiche di accesso.

7.4 *Referenti dei dati*

Il Responsabile di ogni Servizio o Funzione, in qualità di "*referente dei dati"* ha la responsabilità dei seguenti aspetti:

- la conoscenza delle basi dati e dei sistemi di pertinenza del Settore/Ufficio;
- la definizione del "*profilo di accesso*" degli utenti (*chi* può accedere a *quali* informazioni, *come* e *quando)* in relazione alla responsabilità organizzativa e della *classificazione dei dati* definita nel relativo documento;
- l'assicurazione che ogni eventuale violazione delle norme di sicurezza che avviene sui dati di cui è proprietario sia denunciata al Responsabile della Sicurezza adottando le opportune procedure"*;*
- la diffusione ed il rispetto nel proprio ambito di attività, delle istruzioni sull'utilizzo dei supporti di memorizzazione mobili dei dati, descritte nel "*Disciplinare per utenti dei sistemi informativi* della Regione Emilia-Romagna".

7.5 *Referente informatizzazione interna e gestione infrastrutture informatiche*

Predispone il piano per l'acquisizione di hardware e ne esegue o controlla la successiva installazione fisica. Provvede all'installazione dei sistemi operativi e del SW applicativo, alla manutenzione sistemistica delle stazioni di lavoro degli utenti interni; alla gestione dell'attività sistemistica sui server

(salvataggi, aggiornamenti, ecc.), comprese le basi dati multiutente. E' amministratore del sistema di accesso alla rete regionale e in tale ruolo, gestisce le credenziali di accesso dei collaboratori.

7.6 *Responsabile dei sistemi informativi e gestione della sicurezza informatica*

Cura lo sviluppo e la manutenzione evolutiva e correttiva dei sistemi informatici dell'Agenzia. In particolare, cura la realizzazione, anche avvalendosi di risorse esterne, di procedure informatiche per la gestione delle funzioni di Organismo Pagatore Regionale e del SIGC (Sistema Integrato di Gestione e Controllo).

Concorda i requisiti delle soluzioni applicative, ne presidia la progettazione e lo sviluppo, gestisce nel tempo le evoluzioni funzionali e la manutenzione correttiva, anche attraverso il coordinamento ed il controllo delle attività dei fornitori; collabora nella definizione degli standard tecnologici e architetturali dell'infrastruttura applicativa; coopera con la Direzione Agricoltura alla progettazione ed allo sviluppo di un sistema informativo integrato in materia agricola.

Coopera con il Settore innovazione digitale, dati, tecnologia e polo archivistico (SID) al fine della gestione coordinata dei progetti ICT della Regione Emilia-Romagna; garantisce l'allineamento degli applicativi alle strategie vigenti di sicurezza e di qualità dei sistemi informativi e alle architetture standard dell'Ente; collabora, con i gruppi di lavoro istituzionali in materia di ICT ed in particolare di Open Data, semplificazione e trasparenza, interscambio dati.

Collabora alla stesura dei capitolati di gara per l'acquisizione di beni e servizi IT di competenza e dei relativi contratti; presidia la gestione tecnica dei contratti di beni e servizi IT di competenza monitorando i livelli di servizio erogati dai fornitori; partecipa all'analisi dei costi dei servizi IT e alla pianificazione del budget.

7.7 *Dipendenti e collaboratori*

Ogni collaboratore di AGREA, a qualunque titolo, è tenuto:

- al rispetto, nello svolgimento delle sue attività lavorative, delle misure di sicurezza delle informazioni e della applicazione delle relative procedure;
- a segnalare violazioni delle misure di sicurezza delle informazioni, adottando le procedure interne.

7.8 *Flussi informativi con altre organizzazioni*

Gli scambi di informazioni con determinate strutture esterne, enti e/o organizzazioni pubbliche e private, sono gestiti senza compromettere l'integrità e la riservatezza delle informazioni, garantendo la sicurezza e la correttezza dell'operatività dei sistemi di elaborazione e di comunicazione.

AGREA scambia informazioni con soggetti regionali, nazionali ed europei che rivestono un ruolo specifico nella missione dell'Agenzia e, comunque, gli scambi avvengono sulla base di norme di legge, accordi o protocolli d'intesa.

I flussi informativi con i soggetti esterni sono caratterizzati dalla conformità alle regole concordate al fine di preservare l'integrità, la riservatezza, l'autenticità delle informazioni scambiate e la sicurezza dei sistemi di elaborazione nel rispetto della normativa, nazionale e comunitaria, vigente.

8 VIOLAZIONI

Qualunque violazione a queste norme deve essere individuata e gestita. Il personale che contravviene alle politiche definite in questo documento potrà essere sanzionato secondo quando definito nel contratto di lavoro con il dipendente.

9 CICLO DI REVISIONE

Il Direttore dell'Agenzia è responsabile della revisione periodica della politica affinché sia allineata agli eventuali e significativi cambiamenti intervenuti nell'organizzazione e/o nelle tecnologie utilizzate per la protezione delle informazioni.

La revisione sarà fatta secondo necessità, in occasione di significative modifiche organizzative e/o tecnologiche rilevanti per la gestione delle informazioni, oppure in occasione del Riesame della Direzione annuale.