Agenzia Regionale per le Erogazioni in Agricoltura
per l'Emilia-Romagna

Politica della Sicurezza delle informazioni

Il Sistema di Gestione per la Sicurezza delle Informazioni di AGREA

redatto da:	**F. Marabini**	verificato da:	**F. Marabini**	approvato da:	**D. Metta**
revisione:	**4**	data emissione:	**4 settembre 2019**		
doc ID	**PL_01**				

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

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. DICHIARAZIONE DI PRINCIPIO

La Politica di Sicurezza delle Informazioni in AGREA ha 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. ASPETTI GENERALI

La Politica di sicurezza delle informazioni di AGREA è attuata 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 questo documento è indicare le esigenze, gli obiettivi, le finalità, ed i modelli organizzativi della strategia di sicurezza che AGREA intende perseguire, al fine di orientare lo sviluppo, la gestione, il controllo e la verifica dell'efficacia della sua attuazione.

2.1 Esigenza di una politica della sicurezza delle informazioni

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. Per fronteggiare questa eventualità è stato predisposto, accanto al sistema informativo "operativo", il sistema di sicurezza della parte "comunicativa" che, dotato di adeguata strumentazione tecnologica ed organizzativa, consente di proteggere l'integrità e l'autenticità dell'informazione trasmessa.

2.2 Scopo

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.

AGREA pone a base della politica di tutela delle informazioni, 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.

La consapevolezza che non è possibile ottenere, in ambito informatico come del resto in natura, una condizione di sicurezza assoluta, comporta che lo scopo della politica di sicurezza delle informazioni è quello di gestire il rischio ad un livello accettabile attraverso la progettazione, l'attuazione ed il mantenimento di un "Sistema di Gestione della Sicurezza delle Informazioni" (SGSI).

2.3 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.

2.4 Obiettivi

- 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;
- Garantire un livello adeguato dei requisiti di riservatezza, integrità e disponibilità nei servizi erogati attraverso specifici applicativi.

2.5 Revisione, controllo e gestione dei cambiamenti

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.

Nel caso di cambiamenti significativi, questi vengono gestiti a livello progettuale, con dei progetti specifici, documentati a cura di un Responsabile definito, secondo l'ambito di competenza.

2.6 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 diritti personali e le norme che si riferiscono in modo specifico alla certificazione ISO 27001 degli organismi pagatori.

Normativa sulla protezione dei diritti personali

Decreto Legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (GU n.205 del 4-9-2018) Vigente al: 19-9-2018.

Legge n. 163 del 25/10/2017 in particolare articolo 13 Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017.

Regolamento 2016/679 del Parlamento europeo e del Consiglio, del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) pubblicato su GUUE del 4 maggio 2016, entrato in vigore il 24 maggio 2016, applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Decreto legislativo n. 196 del 30/06/2003 Codice in materia di protezione dei dati personali.

Normativa riferita alla 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.

3. USO DEI SISTEMI DI ELABORAZIONE DELL'INFORMAZIONE

AGREA considera i sistemi di elaborazione delle informazioni, come strumenti di lavoro ed il loro uso, da parte di coloro che vi operano, a qualunque livello e a qualsiasi rapporto, è regolato dal "*Disciplinare per utenti dei sistemi informativi* della Regione Emilia-Romagna", recepito e pubblicato sulla intranet dell'Agenzia.

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.

AGREA, perseguirà a norma di legge e del vigente contratto di lavoro il collaboratore che utilizza in modo non appropriato i sistemi di elaborazione delle informazioni, poiché l'eventuale esposizione al rischio impedirebbe all'Agenzia lo svolgimento dei compiti istituzionali.

Per verificare il corretto utilizzo di tutte le strumentazioni informatiche messe a disposizione degli utenti, AGREA ha recepito con propria determinazione, pubblicata nell'Intranet dell'Agenzia, quanto stabilito dal *"Disciplinare Tecnico su modalità e procedure per verifiche di sicurezza sui Sistemi Informativi, per controlli sull'utilizzo dei beni messi a disposizione dall'ente per attività lavorativa con riferimento alle strumentazioni informatiche e telefoniche ed esemplificazioni di comportamenti per il corretto utilizzo dei beni, da applicare nella Giunta e nell'Assemblea Legislativa della Regione Emilia-Romagna"*.

4. ORGANIZZAZIONE E RESPONSABILITÀ DELLA SICUREZZA

L' organizzazione e responsabilità della sicurezza è relativa all'individuazione delle procedure dirette alla gestione e controllo delle misure di sicurezza adottate e si concretizza nell'individuazione di ruoli, funzioni e responsabilità coinvolte nella realizzazione e gestione del Sistema di sicurezza delle informazioni.

4.1. *Obiettivo*

Assicurare che i dirigenti ed i collaboratori, considerato che la sicurezza delle informazioni sia una responsabilità comune, siano adeguatamente informati e formati sul ruolo che possono svolgere al fine di minimizzare i rischi derivanti dalle minacce alla sicurezza del sistema di gestione delle informazioni.

4.2. *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 4.3 e 4.4, per la definizione e attuazione della politica di sicurezza dell'informazione.

4.3. *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 Servizio Tecnico e di Autorizzazione
- Dirigente del Servizio Gestione Contabile dell'OPR, Approvvigionamenti e Certificazioni.

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.

4.4. *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 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
- Referente dell'informatizzazione interna e gestione infrastrutture informatiche.
- Referente del sistema di gestione della sicurezza delle informazioni.

Dal momento che il Direttore 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 ala COS i responsabili delle funzioni pertinenti gli specifici aspetti che devono essere affrontati (es. Responsabili delle pertinenti Linee di Servizio).

4.5. *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 nell'Intranet (InAgrea) alla voce *"Tutela della Privacy e Sicurezza delle Informazioni"*;

b) la documentazione del Servizio/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.

4.6. *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 servizio/ufficio così come specificato nel documento di "*Analisi dei Rischi delle risorse informative"*;
- 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 la procedura prevista da "*Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e della Assemblea legislativa della Regione Emilia - Romagna".*
- 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".

4.7. *Responsabile della Sicurezza delle informazioni*

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 dell'*"Accordo di Servizio per l'utilizzo, da parte di AGREA, dei servizi informatici e di rete della Regione Emilia-Romagna"*.

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.

4.8. *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.

4.9. *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 Servizio Informativo Informatico Regionale 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.

4.10. *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 la procedura prevista da "*Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e della Assemblea legislativa della Regione Emila - Romagna".*

4.11. *Contatti con le autorità e gruppi specialistici*

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 (Servizio Sistemi Informativi) 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.

5. 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.

6. GESTIONE DEI RISCHI

6.1 Obiettivo e metodologia

L'obiettivo dell'Analisi dei Rischi è identificare e contrastare le possibili minacce alla sicurezza dei sistemi e delle informazioni dell'Agenzia, al fine di predisporre adeguate misure di prevenzione e protezione.

L'Analisi dei Rischi è l'elemento principale da cui discendono tutte le attività di controllo, le Politiche in merito alla sicurezza e le procedure operative legate alla sicurezza delle informazioni.

A tale proposito AGREA adotta una propria metodologia che le consente 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 viene condotta da AGREA con cadenza periodica e regolare, a garanzia del permanere dell'efficacia delle misure di mitigazione identificate e attuate

7. TRATTAMENTO DEI DATI PERSONALI

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".

I collaboratori di AGREA sono 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, vengono nominati Responsabili del trattamento dei dati personali, con tutti gli obblighi previsti dal codice della privacy.

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.

8. CONTINUITÀ OPERATIVA (BUSINESS CONTINUITY)

La responsabilità della "Continuità Operativa" dell'Agenzia è del Direttore che predispone *il "Piano di Continuità di Servizio"* ***(Business Continuity Plan - BCP),*** inteso come indicazione delle attività organizzative e tecnologiche, finalizzate alla continuità dei processi che concorrono alla missione dell'Agenzia.

Nella predisposizione del suddetto Piano 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 precedenti punti 4.3 e 4.4.

8.1. *Obiettivo*

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.

8.2. *Requisiti per l'operatività*

AGREA mediante le precauzioni contenute nel **BCP** ritiene di poter contenere l'impatto di eventuali avvenimenti disastrosi, nell'ambito dei requisiti di ripristino definiti.

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.

8.3. *Elementi di pianificazione*

Le metodologie che consentono di redigere, realizzare e mantenere un **BCP** sono diverse e fanno riferimento a standard emanati da importanti istituti internazionali. Gli elementi comuni a tutti gli standard sono:

- identificazione delle strutture di coordinamento della strategia di ripristino; in AGREA sono state individuate le seguenti strutture: *Comitato Direttivo per la Sicurezza (CDS) di cui al punto 4.3; Comitato Operativo per la Sicurezza (COS) di cui al punto 4.4;*
- valutazione dei risultati della Business Impact Analisys per l'individuazione dei processi e dei servizi critici e delle priorità di intervento;
- predisposizione delle procedure da effettuare in caso di attuazione del **BCP**; per i sistemi server le procedure sono definite dalla Regione ER stessa;
- sviluppo, documentazione e verifica del **BCP**. In AGREA la verifica del **BCP** sarà annuale e comunque successiva a significativi cambiamenti degli elementi che lo compongono.

9. INVENTARIO DELLE RISORSE INFORMATICHE

9.1. *Obiettivo*

Identificare**,** classificare e registrare le risorse hardware e software utilizzate dall'Agenzia, al fine di tracciare l'intero "ciclo di vita": acquisizione, assegnazione, aggiornamento, manutenzione, dismissione.

L'inventario delle risorse informatiche è necessario per monitorare l'obsolescenza delle risorse utilizzate, pianificare il loro ammodernamento, rinnovare le licenze e programmare gli investimenti in tecnologie dell'informazione.

9.2. *Inventario*

AGREA è dotata di un "Inventario informatizzato delle risorse informatiche" che compongono il sistema di gestione delle informazioni e 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

9.3. *Inventario hardware*

Le risorse hardware sono classificate e per ciascuna di esse è 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.

9.4. *Inventario software*

I programmi software sono classificati e per ciascuno di essi viene 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.

10. SICUREZZA FISICA ED AMBIENTALE

Costituisce la forma di tutela che attiene alla protezione dei sistemi di elaborazione delle informazioni e si manifesta con 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.

10.1Obiettivo

Minimizzare gli impatti delle minacce ai sistemi di elaborazione delle informazioni dovuti a danni o intrusioni.

10.2 Sicurezza delle aree

Le aree che comprendono i locali ove risiedono i sistemi di gestione dell'informazione dell'Agenzia, sono dotate di porte ad accesso controllato.

10.3 Sicurezza dei locali

I locali sono 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.

10.4 Controllo accessi ai locali

Tutti i sistemi e apparecchiature di rete sono ubicati in edifici sicuri e con accesso vigilato. In particolare, i locali ove risiedono i sistemi server del sistema informativo OPR presso il CED

della Regione Emilia - Romagna sono "*aree ad accesso ristretto"* e l'ammissione è consentita solo in presenza di personale interno autorizzato, come previsto dalle procedure descritte nel "*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 degli accessi ai locali di AGREA".*

11. CONTROLLO DEGLI ACCESSI LOGICI

11.1Obiettivo

Impedire 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.

Proteggere 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.

11.2Accesso ai sistemi ed alle applicazioni

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 .*

Accesso alla rete regionale (autenticazione)

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

Accesso alle applicazioni (autorizzazioni)

AGREA abilita i 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.

AGREA adotta la *profilazione degli utenti*, sia interni che esterni, per la concessione della credenziale d'accesso alle applicazioni ed utilizza a tal fine una "procedura formale" mantenendo documentazione, cartacea ed elettronica, delle autorizzazioni concesse.

Il Responsabile alla Sicurezza controlla periodicamente, almeno una volta all'anno, la 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 viene attuata qualora decadano le caratteristiche di abilitazione di un utente.

Caratteristiche e gestione delle password

AGREA considera la password, conformemente alle norme di sicurezza informatica, 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.

AGREA genera ed assegna password individuali e l'utente è responsabile della sua riservatezza.

La struttura delle password generate dai sistemi di AGREA presenta 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.

12. GESTIONE SOFTWARE SU LICENZA

AGREA acquisisce del software tramite pagamento delle relative licenze ed autorizza i collaboratori, utenti e amministratori, al loro uso.

AGREA, in coerenza con le policy regionali, consente l'uso solo di software autorizzato installato sui sistemi all'atto della consegna. La Regione Emilia - Romagna richiede che sui sistemi dati in dotazione ai collaboratori sia installato software autorizzato e considera 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.

13. SVILUPPO DI APPLICAZIONI SOFTWARE

Lo sviluppo delle applicazioni software (fuori ambito SGSI) avviene in coerenza con la strategia dell'Agenzia ed 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, si svolge secondo i seguenti criteri:

- 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";

- pianificazione e controllo delle varie fasi: analisi, disegno, sviluppo, deployment, test;
- conformità alle direttive comunitarie e nazionali sulla sicurezza delle informazioni.

14. BACKUP DEI DATI ED USO DEI DISPOSITIVI DI MEMORIZZAZIONE

Eventi dannosi dovuti ad errori accidentali possono comportare perdita di dati conservati sul computer personale con ripercussioni anche gravi sull'attività lavorativa e sull'erogazione dei servizi.

Al fine di evitare il rischio di perdita di dati importanti, i collaboratori sono invitati a salvare periodicamente i dati residenti sul personal computer, nelle cartelle di rete esistenti.

La Regione ha acquisito e incentiva l'utilizzo di spazio in modalità "cloud" per la memorizzazione dei dati personali degli utenti.

AGREA limita la possibilità di utilizzare i supporti removibili.

15. SICUREZZA DELLE RETI E DELLE COMUNICAZIONI

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.

16. GESTIONE DEGLI INCIDENTI

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 Incidenti di sicurezza e Data breach".*

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.