Informazioni ESG integrative

Indice

Informazioni integrative relative all'area risorse umane **2**

Programmi di gestione delle condizioni di lavoro 2

Supporto dei dipendenti 2

Approccio ai processi di riorganizzazione 3

Lavoro da remoto e lavoro flessibile 3

Salute mentale 3

Sistema di sviluppo e di valutazione delle performance 3

Modalità di valutazione e gestione dei rischi per la salute e sicurezza 4

Gestione e sensibilizzazione in tema Salute e Sicurezza per gli appaltatori 5

Informazioni integrative relative all'area di business **5**

Asset Management System 5

Business Continuity Management System 6

Programma di risposta alle emergenze 7

Information Security 7

Information Security Governance 7

Information Security Policy 8

Information Security management programs 10

Responsible Artificial Intelligence 10

Artificial Intelligence Policy 10

Responsible Artificial Intelligence Programs 12

Processo di gestione e risoluzione dei reclami 12

Risk management reporting 13

I rischi climatici fisici per il Gruppo A2A 14

Informazioni integrative relative all'area risorse umane

Programmi di gestione delle condizioni di lavoro

In tutti i settori di business in cui opera, A2A siede ai tavoli di trattativa dei contratti collettivi nazionali, (CCNL che figurano quali contrattazione uniche di riferimento per ciascun settore) concorrendo alla definizione dei trattamenti di primo livello periodicamente aggiornati all'andamento dei valori inflazionistici registrati a consuntivo e previsti per gli anni a venire. Le logiche retributive di Gruppo hanno peraltro costituito oggetto di analisi e validazione da parte di enti certificatori esterni.
Nella contrattazione collettiva di Gruppo, la prestazione straordinaria è individuata quale strumento residuale ed eccezionale, sottoposto a limiti quantitativi fissati dal ccnl e dalla contrattazione aziendale.
Le policy retributive trovano applicazione senza riguardo alcuno al genere del lavoratore/lavoratrice, adottando il Gruppo misure per il coinvolgimento delle rappresentanze dei lavoratori sui sistemi di monitoraggio di eventuali salary gap totalmente rispettose delle previsioni normative.
Le ferie annuali sono periodi di assenza retribuita e si segnalano, all'interno della contrattazione di Gruppo, intese atte a favorire lo smaltimento degli istituti feriali attribuiti a ciascun lavoratore (ferie – in misura superiore al minimo fissato dalla legge - permessi ed altre forme di tempo "pagato" dall'azienda).
I licenziamenti collettivi sono gestiti con tempistiche di preavviso amplificate rispetto a quelle stabilite dalla legge 223/91 al fine di gestire con i tempi necessari la co-costruzione di eventuali percorsi di accompagnamento, primariamente rivolti al personale più prossimo al pensionamento.
Esistono sistemi per la verifica del rispetto dell'orario di lavoro da parte della popolazione aziendale, argomento sul quale è costante il confronto con le rappresentanze dei lavoratori anche al fine di individuare le migliori soluzioni di flessibilizzazione.
La protezione sociale si estende oltre quella nazionale, prevedendo coperture sanitarie, assicurative e sussidi ulteriori rispetto a quelle di legge.
Costante è anche il confronto sui fabbisogni formativi dell'organico aziendale, anche in logica di costante adeguamento delle skills all'evoluzione delle modalità di lavoro e delle tecnologie.

Supporto dei dipendenti

A2A Life Caring è un piano a supporto della genitorialità dei dipendenti, un programma ampio, completo e trasversale che testimonia l'impegno concreto del Gruppo nel sostegno alla natalità in una fase storica caratterizzata dal continuo calo demografico del Paese.
I principali contenuti dell'iniziativa:

- Tempo/Congedo di maternità e paternità: in aggiunta a quanto previsto per legge, si ha la possibilità di fruire di un ulteriore mese di congedo retribuito al 100% o, in alternativa di optare per la liquidazione a cedolino stipendio di un importo una tantum equivalente.
- Supporto economico: previsione di contributi a supporto dell'educazione e della conciliazione, con possibilità di ottenere il rimborso di spese sostenute per servizi di educazione ed istruzione (quali libri, tasse scolastiche, asili nido) differenziate per fasce di età, per ogni figlio fino ai 18 anni di età.
- Cultura: percorsi di sensibilizzazione per i neogenitori con figli/e da 0 a 3 anni e per la/il loro manager. I percorsi sostengono e accompagnano i neogenitori alla scoperta e al potenziamento delle loro capacità, aiutandoli a metterle in pratica nella vita privata e lavorativa. Anche i manager partecipano a tale iniziativa con l'obiettivo di rafforzare modelli culturali manageriali positivi e offrire suggerimenti utili ad accogliere e valorizzare sempre più le esigenze dei propri collaboratori "neogenitori".
- Cultura: attività di divulgazione e sensibilizzazione grazie a webinar dedicati alla genitorialità, oltre che attività di divulgazione interna su fertilità e procreazione, inclusa la Procreazione Medico Assistita.

Sono inoltre a disposizione:

- la rete di asili del progetto “Cresciamo il Futuro” (in collaborazione con il Ministero del Lavoro e delle Politiche Sociali, l’iniziativa coinvolge 8 grandi imprese italiane e mette a disposizione un network di asili nido aziendali e privati a cui possono accedere tutte le persone delle aziende aderenti)
- l’asilo nido e la scuola d’infanzia Crescere Assieme sita presso la sede A2A di Brescia.

Il Gruppo fornisce anche diversi canali di Supporto alle/ai caregiver: da incontri info formativi alla possibilità di richiedere una presa in carico personalizzata, con accompagnamento fino all’attivazione dei servizi necessari alla cura del/della proprio/a caro/a.
Vi è infine la possibilità di accedere a un Portale che consente di consultare tutte le opportunità messe a disposizione dal Welfare Pubblico.

Approccio ai processi di riorganizzazione

In parallelo all’ascolto e al supporto delle persone, A2A adotta un approccio responsabile anche nella gestione dei processi di riorganizzazione, garantendo attenzione alla sostenibilità sociale delle proprie scelte e promuovendo il dialogo con le parti sociali. Nel 2024 alcune società del Gruppo hanno concordato con le organizzazioni sindacali l'attivazione di procedure di licenziamento collettivo (destinate ad interessare il 2025 e anche parte del corrente 2026) atte a favorire processi di riorganizzazione e ricambio generazionale, tramite meccanismi di incentivazione economica a beneficio di persone prossime al trattamento pensionistico.
Con riguardo alle procedure di trasferimento d’azienda, ogni operazione straordinaria del Gruppo viene accompagnata con percorsi di confronto sindacale, utili alla individuazione congiunta (tra azienda ed organizzazioni sindacali) delle migliori soluzioni di salvaguardia occupazionale e continuità dei trattamenti.

Lavoro da remoto e lavoro flessibile

A2A adotta un modello di smartworking connotato da un elevato grado di flessibilità ed adattabilità, costruito tenendo conto dei ruoli, delle attività e delle esigenze individuali; il risultato è uno strumento che bilancia lavoro da remoto ed in presenza tenendo conto delle esigenze operative e di team con l’obiettivo di favorire collaborazione, produttività e benessere. È un modello che consente di lavorare da remoto tra il 20% e il 60% del tempo su base mensile o bimestrale, anche a mezze giornate, considerando il ruolo e le attività.
Ed ugualmente avanzata è la gamma di strumenti di flessibilità (giornaliera, ultragiornaliera, orario “fiduciario”) che consentono ad una porzione significativa del perimetro aziendale di superare le difficoltà del classico “orario rigido”.
La contrattazione offre anche strumenti di banca delle ore, per l’accantonamento del maggior lavoro e suo utilizzo secondo le necessità del lavoratore, oltre che soluzioni di costruzione dell’orario settimanale secondo la modalità del cd venerdì corto
Il lavoro a tempo parziale è uno strumento che trova applicazione in tutte le Business Unit, con un grado di estensione coerente con la tipologia di attività e l’organizzazione del lavoro.

Salute mentale

Uno dei servizi storici che il Gruppo mette a disposizione delle proprie persone è il Counseling Psicologico: uno spazio per prendersi cura di sé e del proprio benessere, un supporto per affrontare momenti di difficoltà o di cambiamento, acquisire consapevolezza di vissuti ed emozioni e potenziare risorse e punti di forza, in ogni fase della propria vita.
Gli incontri possono essere in presenza nelle principali sedi del Gruppo, o da remoto, senza alcuna limitazione al numero di sedute di cui si può beneficiare

Sistema di sviluppo e di valutazione delle performance

Nelle società del Gruppo A2A (inclusa Acinque) è presente un processo specifico di Performance Management che coinvolge tutta la popolazione dei dirigenti, quadri e impiegati, complessivamente circa 7.500 persone. Questo processo prevede, con scadenza annuale, una valutazione complessiva sul contributo individuale e una sui comportamenti agiti rispetto alle competenze chiave del modello di competenze comportamentali. Nella prima fase del processo è prevista la definizione del proprio contributo individuale attraverso la descrizione delle proprie attività condivise tra persona e manager, che possono essere aggiornate. Nella successiva fase di valutazione, per

ogni persona è previsto uno step di autovalutazione, finalizzato a stimolare la consapevolezza e il confronto con i manager, nonché la possibilità di coinvolgere uno o più "valutatori aggiuntivi", oltre ai manager diretti, per raccogliere più punti di vista ed arricchire il feedback nel rapporto manager-persona. L'avvio del processo di Performance Management, dal 2026, sarà esteso anche ad un perimetro pilota del personale con qualifica operaio delle società delle BU Smart infrastructures, BU Generazione e Trading e di AEB (Reti più e Illuminazione Pubblica) per un totale di circa 850 persone.
Il performance management annuale, sopra descritto, è supportato (società del Gruppo A2A, esclusa Acinque) anche dalla presenza della sessione "Anytime Feedback", nell'applicativo Smart People, che consente di scambiare feedback tra responsabili e collaboratori, e tra colleghe e colleghi. L'obiettivo è quello di alimentare la cultura del feedback all'interno del Gruppo e facilitare il dialogo tra le persone in un'ottica di miglioramento continuo.
Sempre per le società del Gruppo A2A (non Acinque) è previsto un processo di MBO in bonus pool per dirigenti e un processo di MBO in bonus pool per un perimetro del personale non dirigente.
Il processo di MBO prevede due tipologie di obiettivi: obiettivi Centrali e obiettivi Individuali identificati dal Manager, anche su proposta della Persona Assegnataria MBO.
Il meccanismo di calcolo del sistema incentivante prevede l'incidenza incrementale o decrementale del fattore correttivo di natura economico- finanziaria del Gruppo
A2A al 31/12 dell'anno di competenza, della fascia di risultato determinata sulla base della valutazione di raggiungimento degli obiettivi assegnati effettuata tramite auto-consuntivazione (opzionale) da parte dell'assegnatario MBO, approvazione da parte della/del propria/o Manager e validazione a carico del Referente MBO di BU / staff Unit.
La valutazione delle competenze influisce solo dimezzando il payout dell'MBO in caso di risultato non adeguato nell'ambito del Performance Management sopra riportato.
Invece il sistema MBO Acinque, che si applica a tutta la popolazione Dirigenziale e ad alcuni figure quadro con impatto più diretto sui risultati di Business, prevede una componente variabile correlata alla performance nel breve periodo, sia con riferimento alla performance individuale e alle competenze agite, che ai risultati della Società e di Gruppo, tenendo conto degli obiettivi definiti nel piano strategico. La componente variabile prevede un limite massimo con obiettivi di performance predeterminati, misurabili e collegati alla creazione di valore per gli azionisti in un orizzonte annuale. Il processo prevede una fase iniziale di definizione degli obiettivi, entro il mese di marzo, una fase di mid-year review, a metà anno, e una fase di consuntivazione all'inizio dell'anno successivo. La valutazione degli obiettivi individuali è in capo al Manager, supportato da idonea certificazione, mentre la consuntivazione degli obiettivi finanziari è in capo ad AFC e HR.

Modalità di valutazione e gestione dei rischi per la salute e sicurezza

Il Gruppo A2A gestisce i rischi per la salute e sicurezza con un processo integrato che unisce DVR, piani di miglioramento, sorveglianza sanitaria e gestione degli eventi incidentali, con tracciabilità su ARIAL.
La valutazione dei rischi OHS è svolta in coerenza con il D.Lgs. 81/2008 e si formalizza nel DVR, elaborato con il coinvolgimento della linea e delle figure previste (RSPP, Medico Competente, RLS, dirigenti e preposti). In ARIAL la valutazione è organizzata per mansioni/gruppi omogenei (GOP/GOS) e scenari di esposizione, con definizione di gravità e probabilità, misure di prevenzione e protezione e rischio residuo; gli esiti alimentano i protocolli e la sorveglianza sanitaria. Le priorità sono definite in funzione del rischio residuo e tradotte in Piani di Azione tracciati in ARIAL (obiettivi, responsabilità, risorse e tempi), includendo il monitoraggio nel tempo dei casi da attenzionare.
La preparazione e risposta alle emergenze è integrata nel sistema: in caso di evento si attivano azioni immediate di tutela e contenimento e, se necessario, i Piani di Emergenza e i presidi di crisis management, con le comunicazioni previste e il coinvolgimento delle strutture HSEQ competenti.
I progressi sono verificati attraverso il monitoraggio dell'avanzamento e dell'efficacia delle azioni (anche con esiti di audit/monitoraggi e gestione di eventuali non conformità) e tramite reporting periodico su trend e indicatori (es. indici infortunistici, segnalazioni/near miss e stato di chiusura delle azioni). Le ispezioni e i sopralluoghi supportano l'identificazione dei pericoli e l'aggiornamento del DVR; il Medico Competente effettua sopralluoghi negli ambienti di lavoro almeno annualmente (salvo diverse indicazioni nel DVR), con verbalizzazione e follow-up delle azioni.
L'investigazione degli eventi incidentali segue un flusso strutturato (segnalazione, azioni immediate, registrazione/classificazione, analisi e azioni di miglioramento): gli eventi infortunistici sono registrati in ARIAL entro 48 ore (entro 24 ore per gli infortuni dei lavoratori del Gruppo), con gestione degli adempimenti verso INAIL in

funzione della prognosi; la classificazione considera conseguenze reali e potenziali e l'analisi genera azioni monitorate in ARIAL fino alla verifica di efficacia e all'eventuale aggiornamento del DVR.

Gestione e sensibilizzazione in tema Salute e Sicurezza per gli appaltatori

A2A presidia la salute e sicurezza degli appaltatori con un percorso che accompagna l'impresa dall'ingresso nell'Albo Fornitori fino alla chiusura delle attività in sito. L'approccio combina pre-qualifica HSE, verifica dei requisiti prima dell'avvio, induction operativa e monitoraggio costante delle performance, così da prevenire infortuni e promuovere comportamenti sicuri lungo tutta la catena di fornitura.

Formazione in materia di salute e sicurezza sul lavoro per gli appaltatori

La competenza in materia HSE è un prerequisito: già in qualifica A2A raccoglie evidenze, questionari e, ove applicabile, certificazioni, così da verificare che l'impresa disponga di organizzazione e competenze adeguate. Prima dell'avvio operativo, la formazione è completata dall'informazione e dall'addestramento specifici di sito, coerenti con i rischi e con le misure definite nei documenti di sicurezza (ad es. DUVRI/PSC/DIC).

Criteri di pre-qualificazione in materia di salute e sicurezza per gli appaltatori

La selezione privilegia fornitori qualificati, valutati anche per solidità, reputazione e sostenibilità, includendo aspetti HSE. In funzione della criticità delle attività, la qualifica può essere più snella o più approfondita, con verifiche aggiuntive su requisiti e documentazione. Quando opportuno, il percorso è completato da audit o verifiche sul campo, utili a confermare l'effettiva applicazione degli standard richiesti.

Induction su salute e sicurezza in cantiere per gli appaltatori

Prima dell'accesso al sito all'appaltatore vengono esposte regole operative, rischi specifici e modalità di cooperazione e coordinamento con il committente. L'avvio è supportato dalla documentazione di sicurezza pertinente (ad es. DUVRI/PSC/DIC) e dalle verifiche necessarie al perfezionamento dell'ordine; per lavori e servizi soggetti all'art. 26 e/o al Titolo IV del D.Lgs. 81/08 è prevista anche una verifica di conformità, con eventuale richiesta di integrazioni.

Processi di valutazione continua della salute e sicurezza per gli appaltatori presenti in sito

Durante l'esecuzione, A2A monitora l'andamento HSE degli appaltatori attraverso strumenti di valutazione del rischio e della performance, così da intercettare tempestivamente eventuali segnali di criticità. Se emergono scostamenti o non conformità, vengono attivati approfondimenti, azioni correttive e – se necessario – verifiche sul campo; nei casi più gravi si applicano misure di gestione conseguenti, in coerenza con le regole di Gruppo.

Nel complesso, questi presidi rafforzano l'approccio di Responsible Procurement del Gruppo e favoriscono la diffusione di una cultura della prevenzione anche presso le imprese appaltatrici.

Informazioni integrative relative all'area di business

Asset Management System

Con riferimento alla Business Unit Smart Infrastructures e alle società Unareti e Duereti, A2A adotta un approccio strutturato di Asset Management lungo l'intero ciclo di vita degli asset.

L'Asset Owner di BU definisce e aggiorna la Policy di Asset Management, che traduce la mission e i pilastri del Piano Industriale A2A in obiettivi operativi di Asset Management, chiarendo i principi di gestione, le priorità e i criteri decisionali.

La Policy è parte integrante dello Strategic Asset Management Plan (SAMP), predisposto dall'Asset Manager, che dettaglia l'asset management framework, i processi di pianificazione e controllo e le responsabilità manageriali secondo il modello Asset Owner - Asset Manager - Service Provider.

Il SAMP contiene tutti gli elementi necessari affinché la strategia aziendale delle società Unareti e Duereti, sia opportunamente convertita in strategia di gestione degli asset. Di fatto rappresenta la linea guida strategica che contiene e allinea la policy di asset management, gli obiettivi strategico aziendali, le strategie e gli approcci per lo sviluppo e la gestione del portfolio di asset e del sistema di asset management nel suo complesso.

In tale ambito sono definiti anche i KPI per il monitoraggio delle performance degli asset e la gestione dei rischi e delle opportunità, integrata nei processi di asset management attraverso specifiche procedure e valutazioni periodiche. Inoltre, è attivo un costante allineamento con le strutture di Gruppo di Enterprise Risk Management e con le funzioni competenti in materia di Salute e Sicurezza, Ambiente e Qualità, Procurement, Comunicazione, Stakeholder Engagement, Organizzazione, HR, al fine di assicurare un presidio coordinato dei principali fattori di rischio e l'attuazione delle relative misure di mitigazione.

Recependo le indicazioni del SAMP, Unareti e Duereti definiscono e implementano un Piano di Asset Management formale, coincidente con il Piano di Sviluppo delle società e con gli obiettivi di continuità del servizio, sicurezza, resilienza e affidabilità delle infrastrutture. Il Piano include priorità di intervento, programmi manutentivi e di rinnovo, criteri di investimento. La sensibilizzazione e formazione sul tema asset management è continuativa e si basa su percorsi disponibili su Academy A2A, oltre a iniziative specialistiche incluse nei piani di sviluppo delle competenze (es. master e dottorati di ricerca). A supporto del miglioramento continuo, la BU e le società possono avvalersi di consulenze specialistiche per rafforzare metodologie, processi e strumenti di gestione del ciclo di vita degli asset.

In tema di assurance, il sistema di asset management è sottoposto a verifiche periodiche tramite audit interni ed esterni secondo quanto previsto dallo standard ISO55000. Si evidenzia infine che Unareti ha conseguito nel 2025, come primo DSO di energia elettrica e gas in Italia, la certificazione ISO 55001 Asset Management Systems con organismo accreditato.

Business Continuity Management System

Nel 2019 è stato avviato il progetto per l'implementazione di un Sistema di Gestione della Continuità Operativa che, nel 2022, è arrivato alla prima certificazione (in aderenza allo standard ISO22301).

Da allora il perimetro dei processi certificati è andato ampliandosi anno dopo anno, fino a comprendere oggi i seguenti processi:

- Energy Management
- Finanza
- Distribuzione Elettrica
- Ciclo Idrico Integrato
- Generazione Idroelettrica
- IT Incident Management & Disaster Recovery
- CyberSecurity Incident Handling & Monitoring

Nell'anno 2026 è in programma l'estensione del perimetro certificato anche ai processi di Teleriscaldamento, Termovalorizzazione, Security Control Room.

Le attività afferenti al sistema di gestione, così come da Standard ISO22301, sono le seguenti:

- aggiornamento periodico dell'analisi di BIA (Business Impact Analysis), su tutti i processi del Gruppo A2A. Vengono valutati gli impatti economico, operativo, compliance, verso il mercato e verso i dipendenti, per potenziali interruzioni su 6 intervalli di tempo (da 24h a più di un mese). Nelle BIA vengono mappate anche le risorse critiche per il processo, compresi gli applicativi su cui poi verrà costruito il Disaster Recovery sia applicativo che infrastrutturale;
- aggiornamento periodico del Risk Assessment (specifico di Business Continuity), su tutti i processi del Gruppo A2A. E' un'analisi strutturata secondo quanto indicato nello standard ISO31000, in cui viene valutata la probabilità di accadimento di una minaccia (sia teorica, secondo statistiche pubbliche, sia puntuale, secondo quanto occorso nel Gruppo A2A), l'impatto (ereditato dalla BIA) e le contromisure in essere a mitigazione del rischio inerente (essendo un rischio su cui agire operativamente alla mitigazione, si valuta il rischio residuo).

Sia le metriche di base (matrice degli impatti ed indici di probabilità) sia i risultati delle analisi di BIA ed RA vengono condivise con la struttura di Enterprise Risk Management.

Formazione ed Awareness: sia tramite piattaforme online che con lezioni frontali (in presenza o virtuali);

Test: ogni anno vengono organizzati test di diverse nature (tecnologici, di processo, ibridi tecnologia/processo, table top);

Revisione documentale: il sistema di gestione è imperniato su un framework documentale che necessita di aggiornamento annuo, a valle dell'evoluzione delle analisi, del contesto e dei risultati di test ed eventi reali. Oltre a

Policy e Documenti Tecnici, vengono aggiornate anche le schede di Recovery, che sono quei file in cui sono elencati i possibili scenari di indisponibilità e le strategie di continuità che è necessario avviare per mitigarli/risolverli (con tutte le caratteristiche in termini di tempi di ripristino e persone coinvolte);

Plant Service Continuity Assessment: sugli impianti critici per il Gruppo A2A viene svolta un'analisi sul livello di mitigazione del livello di rischio operativo indiretto;

Supply Chain Continuity: è stato strutturato un processo di valutazione della capacità di continuità operativa dei fornitori critici per il Gruppo A2A (sia in fase di gara che ex-post), in aderenza sia allo standard ISO22301 di riferimento, sia alle necessità in termini di continuità operativa del Gruppo A2A

Nell'alveo delle attività di Crisis Management, la struttura di Business Continuity & Resilience supporta sia nella fase di triage dell'evento che nel coordinamento e nelle comunicazioni necessarie, fino alla risoluzione dell'evento avverso e del ritorno alla normale operatività. In conseguenza di eventi di livello rilevante, vengono poi svolte le necessarie analisi ex-post e valutate eventuali iniziative di remediation.

Programma di risposta alle emergenze

Nel Gruppo A2A la gestione delle emergenze è affidata a diverse strutture: HSE, Group Security, Digital Technology & Innovation e Impianti industriali.

Nella Direzione di Group Security sono stati sviluppati i seguenti strumenti tecnologici ed organizzativi:

- Security Control Room: una sala controllo operativa h24 in cui degli operatori monitorano tramite uno PSIM segnali inviati da impianti antincendio, antintrusione e controllo accessi, oltre alle immagini di più di 5.000 telecamere installate nei diversi asset aziendali. Questa struttura ha in carico anche la gestione delle chiamate d'emergenza del personale in viaggio e svolge un ruolo centrale nel processo di Crisis Management, ricevendo le segnalazioni e effettuando il primo triage, per poi avviare il processo di comunicazione verso distribution list predefinite, in relazione alla gravità dell'evento. È in corso un progetto di aggiornamento e re-design del processo di Crisis Management, in linea con lo standard ISO22361.
- Security Operations Center: una sala controllo operativa h24 in cui degli operatori monitorano gli asset tecnologici (applicativi, rete, siti) del Gruppo A2A. (La descrizione completa nella sezione di Cyber Defence).

Nella Direzione Group Security & Cyber Defence vengono svolte periodicamente diverse analisi del rischio, tutte ISO31000 based, una per ogni natura di minacce (physical, people, cyber). Tutte le attività, ruoli e responsabilità, flussi e processi sono normati in procedure dedicate.

Il processo di Comunicazione, Awareness & Learning di Direzione permette di diffondere informazioni, buone pratiche e conoscenza delle Procedure e Policy afferenti alle attività di gestione di incidenti/emergenze.

Information Security

Information Security Governance

Il Gruppo A2A ha implementato un modello strutturato e formalizzato di governance della Information Security, integrato nel Sistema di Controllo Interno e di Gestione dei Rischi, con l'obiettivo di garantire la protezione degli asset informativi, la resilienza dei sistemi IT e OT, la continuità operativa dei servizi e la resilienza complessiva del business.

Dal 2017, il Gruppo si è strutturato con la Direzione Group Security & Cyber Defence, dedicata alla Security sia fisica che digitale di Gruppo, con responsabilità trasversali a livello di Gruppo. Al suo interno, la Funzione Cyber Defence definisce politiche, processi e standard di sicurezza informatica da applicare nelle fasi di progettazione ed erogazione dei servizi, secondo i principi di security by design e vulnerability management.

In coordinamento con la struttura di Risk Prevention and Security Resilience, la struttura Cyber Defence:

- definisce e implementa il framework di gestione del rischio cyber;
- garantisce il monitoraggio continuo dei rischi IT e OT;

- assicura attività di reporting periodico a livello esecutivo e operativo;
- individua le iniziative di mitigazione e ne monitora l'attuazione;
- coordina la risposta agli incidenti e alle minacce cyber, anche tramite il costante scambio informativo con l'Agenzia per la Cybersicurezza Nazionale.

La supervisione delle tematiche di Information Security è assicurata a livello di Consiglio di Amministrazione tramite periodiche informative al CdA della Capogruppo e ai CdA delle Società Controllate, oltre che il trimestrale reporting verso il Comitato Controllo e Rischi, nell'ambito dei processi di Enterprise Risk Management. Attraverso flussi informativi strutturati, le funzioni competenti forniscono aggiornamenti periodici sul profilo di rischio cyber, sulle principali minacce e sulle iniziative di mitigazione adottate. Il CdA riceve pertanto report formali e strutturati in materia di cybersecurity e sicurezza delle informazioni.

Le comunicazioni in ambito Information Security sono pubblicate sulla intranet aziendale e costituiscono un presidio fondamentale del sistema di governance e del processo di diffusione del framework normativo interno. In tale ambito, le policy e i principali documenti di sicurezza, approvati dagli organi competenti del Gruppo A2A, incluso il Consiglio di Amministrazione per i temi a maggiore rilevanza, vengono formalmente comunicati a tutti i destinatari al fine di garantirne la piena conoscenza e applicazione da parte delle strutture organizzative coinvolte. Le comunicazioni intranet rendono disponibili i documenti normativi, ne formalizzano la decorrenza operativa ed evidenziano gli aggiornamenti introdotti, assicurando coerenza con i requisiti normativi e gli standard di riferimento (es. ISO/IEC 27001, Direttiva NIS2). Esse rappresentano inoltre evidenza delle attività di informazione e sensibilizzazione interna e contribuiscono ad assicurare l'allineamento continuo dell'organizzazione rispetto all'evoluzione dei rischi cyber, dei relativi modelli di gestione e delle misure di sicurezza adottate dal Gruppo, a tutela del patrimonio informativo e tecnologico.

La responsabilità complessiva della governance della sicurezza è attribuita alla Direzione Group Security & Cyber Defence, guidata da Alessandro Manfredini, Responsabile Group Security & Cyber Defence. In ambito operativo e specialistico, la funzione di Head of Cyber Defence è ricoperta da Simonetta Sabatino, con responsabilità sul presidio delle tematiche di cybersecurity, sulla gestione del rischio cyber e sul coordinamento delle iniziative tecniche e organizzative.

La governance della sicurezza si fonda su un modello organizzativo dedicato, articolato in diverse strutture specializzate che presidiano la gestione della cybersecurity sia in ambito Digital sia Industrial.

La funzione Cyber Defence detiene la responsabilità complessiva del sistema di sicurezza informatica, definendo politiche, processi e standard di cybersecurity, implementando il framework di gestione del rischio cyber in coerenza con il modello di Enterprise Risk Management e monitorando il livello di sicurezza e la maturità dei controlli. La funzione assicura inoltre lo svolgimento delle attività di audit, il coordinamento della gestione delle minacce e degli incidenti cyber e l'interazione con le autorità competenti e gli stakeholder esterni.

All'interno di tale assetto, la struttura Cyber Security Governance, Risk & Reporting presidia la valutazione e il monitoraggio dei rischi, la definizione dei piani di mitigazione, la gestione del framework normativo e dei controlli interni, nonché le attività di compliance e reporting.

La struttura Cyber Security Engineering & Delivery è responsabile della definizione degli standard tecnologici, della progettazione e dell'implementazione delle soluzioni di sicurezza e del presidio del processo di security by design.

La struttura del Security Operations Center (SOC), infine, garantisce il monitoraggio continuo delle minacce, la gestione operativa degli incidenti di sicurezza e le attività di threat intelligence.

Il modello complessivo si caratterizza per il forte coordinamento con le strutture di Digital Technology & Innovation e con le Business Unit, adottando un approccio integrato e risk-based che copre l'intero ciclo di gestione della cybersecurity: dalla definizione delle politiche e dei requisiti di sicurezza, alla progettazione e implementazione dei controlli, fino al monitoraggio continuo e alla risposta agli incidenti.

Information Security Policy

Il Gruppo A2A ha adottato una Policy di Information Security, inserita in un sistema integrato di politiche e procedure aziendali, accessibili a tutto il personale tramite Intranet e costantemente aggiornate sulla base delle necessità interne ed esterne. Tali documenti stabiliscono obblighi di comportamento, principi di protezione delle informazioni, regole di utilizzo dei sistemi e delle credenziali e prevedono processi di escalation formalizzati che consentono a tutti i dipendenti e collaboratori di segnalare tempestivamente incidenti di sicurezza, vulnerabilità o attività sospette.

Questo assetto è rafforzato da programmi strutturati di formazione e awareness sulla sicurezza delle informazioni, inclusi percorsi formativi periodici e simulazioni (ad esempio campagne di phishing), finalizzati a diffondere una cultura della sicurezza a tutti i livelli organizzativi e a garantire che ciascun individuo contribuisca attivamente al presidio del rischio cyber.

Il sistema è conforme agli standard internazionali di riferimento ed è certificato ISO/IEC 27001 per il Sistema di Gestione della Sicurezza delle Informazioni. La Corporate Security Policy è pubblica mentre gli altri documenti sono disponibili internamente ai suoi dipendenti.

Ad esempio, A2A attraverso le varie strutture aziendali, ha emanato:

- Policy, quali la Cyber Security Management Policy, la Enterprise Risk Management Policy, il Group Crisis Plan, il Business Continuity Plan, la Cyber Vulnerability Management Policy e la Protezione dei dati ai fini privacy.
- Procedure, quali la Security by Design Procedure, la Cyber Security Incident Handling Procedure, la Cyber Threat Intelligence Procedure e la Access & Identity Management Procedure, Procedura per la gestione e notifica degli incidenti in ambito NIS2.

Attraverso la propria policy e la documentazione correlata, A2A si impegna esplicitamente a:

- Migliorare continuamente i sistemi di sicurezza delle informazioni, secondo il principio del miglioramento continuo;
- Garantire la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni trattate;
- Monitorare e rispondere alle minacce alla sicurezza delle informazioni, attraverso strutture dedicate di Security Operations e Cyber Defence;
- Definire responsabilità individuali in materia di Information Security per l'intera forza lavoro;
- Stabilire requisiti di sicurezza delle informazioni per le terze parti, applicati lungo l'intero ciclo di vita della fornitura;
- Garantire i diritti degli interessati in materia di protezione dei dati personali (accesso, rettifica, cancellazione), in coerenza con la normativa privacy;
- Implementare misure tecniche e organizzative adeguate alla protezione dei dati personali e aziendali.

Il Gruppo A2A ha inoltre definito specifici requisiti di Information Security applicabili alle terze parti, inclusi fornitori e partner, con l'obiettivo di mitigare i rischi derivanti dalla catena di fornitura.

In particolare, tali requisiti sono formalizzati mediante l'inserimento di specifiche clausole contrattuali di sicurezza nei contratti e negli accordi con le controparti, nonché definiti all'interno delle policy e dei documenti normativi di Gruppo resi disponibili anche tramite gli strumenti aziendali. Contestualmente, A2A prevede processi di due diligence e valutazione del rischio volti a identificare, analizzare e monitorare i rischi cyber associati ai fornitori lungo l'intero ciclo di vita della relazione contrattuale. Le attività di qualificazione e monitoraggio delle terze parti sono basate su criteri di cybersecurity e includono, ove applicabile, audit periodici e verifiche di conformità sui fornitori più critici, al fine di valutare l'efficacia dei presidi adottati e il rispetto degli obblighi definiti. Inoltre, il Gruppo stabilisce standard minimi di sicurezza per tutte le terze parti che accedono a sistemi, dati o servizi aziendali, assicurando che i rischi derivanti da fornitori, prodotti e servizi siano compresi, registrati, prioritizzati, trattati e monitorati nel tempo, in coerenza con i processi di gestione del rischio cyber adottati a livello aziendale. Questo approccio consente di estendere il presidio della sicurezza delle informazioni anche a soggetti terzi che trattano dati o accedono ai sistemi del Gruppo.

Dalla documentazione del Gruppo A2A le policy e procedure aziendali descrivono:

- le tipologie di dati trattati (dati personali, dati di clienti, fornitori e dipendenti, informazioni aziendali e proprietà intellettuale);
- le finalità e modalità di utilizzo dei dati, nel rispetto dei requisiti normativi;
- le modalità di comunicazione e divulgazione dei dati, incluse le regole per la gestione delle informazioni attraverso etichette di classificazione (pubblico, divulgazione controllata, confidenziale, strettamente confidenziale);
- meccanismi strutturati di segnalazione di problematiche relative alla protezione dei dati e alla sicurezza (canali di escalation e procedure dedicate);
- le pratiche di conservazione dei dati (data retention);
- le procedure di gestione e notifica degli incidenti di sicurezza con anche riferimento a temi di compliance quali NIS2, PSNC, e data breach.

Information Security management programs

Il Gruppo A2A ha definito e implementato un Information Security Management Program strutturato, finalizzato alla gestione dei rischi cyber e alla garanzia della resilienza dei servizi IT e OT, coerente con il NIST Cyber Security Framework e basato sui requisiti dello standard ISO/IEC 27001. Tale programma è orientato a mantenere il livello di rischio cyber entro soglie accettabili e ad assicurare la continuità operativa dei servizi essenziali per il business, che rappresenta un obiettivo prioritario per il Gruppo.

La resilienza dei servizi è presidiata attraverso l'adozione di piani di Business Continuity e Disaster Recovery regolarmente aggiornati e testati, supportati dalla presenza di due Data Center (primario e di backup) e dalla definizione di obiettivi di recupero (RTO), nonché dall'integrazione della componente cyber nel programma di risposta alle emergenze (ERP) e nei piani di gestione delle crisi aziendali. Il modello di controllo include inoltre attività strutturate di analisi delle vulnerabilità, valutazione dei rischi cyber in ambito IT e OT, analisi privacy e valutazioni di impatto (PIA/DPIA), accompagnate da audit interni sull'infrastruttura IT e sui sistemi di gestione della sicurezza delle informazioni.

A presidio continuo degli ambienti tecnologici, il Gruppo si avvale di una struttura dedicata di Security Operations, responsabile del monitoraggio continuativo degli ambienti IT e OT, delle attività di cyber threat intelligence, dell'analisi delle vulnerabilità e della gestione degli incidenti di sicurezza. Tali attività sono supportate da esercitazioni e test periodici delle procedure di risposta agli incidenti e da processi formalizzati di notifica e gestione dei Data Breach, in coerenza con la normativa applicabile.

Le politiche aziendali in materia di sicurezza delle informazioni, accessibili tramite i canali di comunicazione interna, definiscono in modo chiaro i processi di escalation che consentono a dipendenti e collaboratori di segnalare tempestivamente incidenti, vulnerabilità o attività sospette, garantendo l'accesso a un supporto specialistico attivo 24 ore su 24, 7 giorni su 7 mediante canali di segnalazione ufficiali e procedure dedicate (per maggiori informazioni: A2A CERT). In particolare, per le segnalazioni di carattere riservato trova applicazione la procedura di Whistleblowing, mentre per le segnalazioni generiche sulla sicurezza delle informazioni si applicano le disposizioni della policy di Gruppo.

Il processo di valutazione e gestione del rischio cyber è formalizzato nella policy interna Cyber Security Risk Management, che descrive il modello adottato dal Gruppo per l'identificazione, l'analisi e il trattamento dei rischi per la sicurezza delle informazioni. A supporto di tale processo vengono svolti annualmente specifici risk assessment, i cui risultati sono di natura riservata. Analogamente, le attività di audit interne ed esterne sul Sistema di Gestione della Sicurezza delle Informazioni e sui relativi controlli producono evidenze documentali non divulgabili, a tutela della sicurezza del Gruppo.

A completamento del presidio tecnico e organizzativo, il Gruppo promuove costantemente la cultura della sicurezza attraverso iniziative di comunicazione, programmi di formazione obbligatoria per le figure con ruoli critici e campagne periodiche di sensibilizzazione, incluse simulazioni di phishing, rivolte a tutto il personale interno ed esterno che opera sui sistemi aziendali.

Il presidio della sicurezza delle informazioni si estende anche alla catena di fornitura attraverso un programma di due diligence sulla cybersecurity dei terzi, che comprende checklist di qualifica cyber sul portale fornitori, valutazioni nelle fasi di sourcing e attività di audit dedicati.

Il Gruppo A2A ad ulteriore garanzia del raggiungimento degli obiettivi aziendali di sostenibilità, strategia, security e resilienza, attraverso le diverse strutture aziendali, nel corso del 2025:

- ha mantenuto la certificazione ISO 27001 relativa al Sistema di Gestione della Sicurezza delle Informazioni.
- ha mantenuto la certificazione ISO 22301 relativa al Sistema di Gestione della Continuità Operativa.

Inoltre, ha ottenuto la certificazione ISO 28000:2022 – Security & Resilience per il Sistema di Gestione dei Processi di Physical Security Governance, nonché la certificazione IEC 62443 con riferimento ai contesti industriali in perimetro di compliance PSNC.

Responsible Artificial Intelligence

Artificial Intelligence Policy

A2A ha adottato una policy sull'utilizzo responsabile dell'AI, articolata in due documenti normativi complementari applicabili a tutto il Gruppo A2A. I principali contenuti, mappati sui temi richiesti, sono i seguenti:

- Data privacy. La policy disciplina il rispetto della data privacy nell'uso e nello sviluppo dell'AI: vieta l'inserimento negli strumenti di IA di Dati Personali, Dati Particolari e Dati Giudiziari senza preventiva verifica e autorizzazione, richiama il GDPR (Reg. UE 2016/679) – in particolare i principi dell'art. 5 (liceità, correttezza, trasparenza, minimizzazione dei dati) e l'art. 22 sul processo decisionale automatizzato – e il Codice Privacy. È previsto il coinvolgimento della struttura Compliance Privacy (COMPRI) per gli aspetti di data protection. Gli strumenti autorizzati devono garantire la segregazione dei dati su server dedicati al Gruppo ed esclusivamente dislocati in Europa (EU Data Boundary), senza che i dati siano accessibili a terzi o utilizzati per addestrare sistemi di terze parti.
- Cybersecurity. La policy tutela la cybersecurity dei sistemi nell'uso e nello sviluppo dell'AI: la struttura Cyber Defence è responsabile della valutazione del rischio cyber con approccio Security by Design e Vulnerability Assessment, in coerenza con la Information Security Management Policy, l'Access & Identity Management Policy e la Security Policy di Gruppo. È ammesso solo l'uso di strumenti di IA autorizzati e installati su dispositivi aziendali; per i sistemi AI sono definite procedure e misure di sicurezza dedicate e la segnalazione degli incidenti gravi alle autorità.
- Bias. La policy mira a evitare il potenziale bias (bias algoritmico) nell'uso e sviluppo dell'AI: definisce il bias algoritmico come pregiudizio/distorsione che può portare a risultati iniqui o discriminatori, evidenzia la natura statistica e potenzialmente imprecisa degli Output e impone una verifica umana critica per mitigare bias ed errori.
- Human in the loop. La policy mantiene l'uomo "in the loop" (human-in-the-loop) per le decisioni critiche e prevede sempre l'intervento umano: impone il coinvolgimento del controllo umano e vieta un utilizzo privo di supervisione. È obbligatoria la "Verifica" umana di ogni Output prima del suo utilizzo (logicità, coerenza, correttezza dei dati, attendibilità delle fonti, individuazione degli errori); in nessun caso un Output può essere usato senza Verifica.
- Transparency & explainability. La policy assicura la transparency dei sistemi AI e supporta l'explainability dei risultati: ogni Output deve riportare la dicitura "Generato tramite l'ausilio di Intelligenza Artificiale Generativa" e, ove possibile, i documenti/fonti che lo hanno generato; per i sistemi a rischio limitato è richiesto che gli utenti siano informati dell'interazione con l'AI e che i contenuti sintetici (testi, immagini, audio, video) siano marcati in formato leggibile e rilevabile.
- Accountability. La policy stabilisce una chiara accountability per gli esiti prodotti da modelli/strumenti AI: gli strumenti supportano ma non sostituiscono l'utilizzatore, che resta integralmente responsabile di quanto prodotto, e l'uso dell'AI non costituisce scriminante per errori o inesattezze. Ruoli e responsabilità sono definiti (Business, Digital & Innovation / Group Data Office, Cyber Defence, Affari Legali e Compliance, COMPRI, Project Owner). Le violazioni comportano conseguenze disciplinari ed eventuale responsabilità penale, anche ai sensi del D.lgs. 231/2001.
- Clear boundaries. La policy definisce confini chiari (clear boundaries) su ciò che l'AI può e non può fare: individua casi d'uso consentiti, casi che richiedono autorizzazione del Direttore di Struttura (es. gare d'appalto, documenti finanziari ufficiali, comunicazioni regolamentari, documenti strategici) e casi non consentiti (es. registrazione di riunioni con ALC, Cyber Defence o Segreteria Societaria, o su temi sensibili). È ammesso solo l'uso di strumenti di IA autorizzati e inseriti nel Registro di IA Generativa.
- Low ecological footprint. A2A presidia l'impronta ecologica (low ecological footprint) dei data center e dei modelli AI: utilizza data center di fornitori cloud di prossimità (in EU) alimentati possibilmente da fonti rinnovabili, monitora le emissioni di CO_2 dei propri sistemi e sperimenta modelli proprietari e open eseguiti localmente – in ottica di sovranità dell'AI – su macchine proprietarie, con il supporto di Life Ventures (AI Strategy & Development).
- Prohibited systems (EU AI Act). La policy non utilizza/distribuisce i sistemi vietati dall'AI Act: sono esclusi i sistemi di AI che adottano comportamenti manipolativi o subliminali (manipulative behavior), sfruttano vulnerabilità individuali (exploitation of vulnerabilities) legate a età/disabilità/condizione sociale, implementano il social scoring, effettuano sorveglianza biometrica non autorizzata (unauthorized biometric surveillance), creano banche dati di riconoscimento facciale, inferiscono emozioni in ambito lavorativo/scolastico o classificano le persone tramite dati biometrici. Gli applicativi a rischio non accettabile non possono essere acquistati e, se preesistenti, devono essere dismessi o modificati.

Le policy sono redatte, verificate e approvate a livello di Management: la responsabilità è in capo alla Direzione Digital Technology & Innovation – responsabile della governance degli applicativi enterprise, tramite il Group Data Office – con il supporto di Affari Legali e Compliance e di Group Security & Cyber Defence.

Responsible Artificial Intelligence Programs

Le attività di A2A per l'utilizzo responsabile dell'AI derivano dall'attuazione delle policy 101.0008 e 101.0044 e dal progetto "AI Act Project", che ha istituito un Gruppo di Lavoro dedicato e un catalogo dei sistemi di AI. Rispetto ai punti richiesti:

- Limiting access to sensitive AI capabilities. L'accesso alle capability AI sensibili è limitato: il riconoscimento facciale tramite scraping indiscriminato e l'identificazione biometrica remota in tempo reale (facial recognition, surveillance) rientrano tra le pratiche vietate e non possono essere acquistati/utilizzati; l'accesso completo agli strumenti AI autorizzati è subordinato a formazione obbligatoria e all'approvazione del responsabile diretto, di Digital & Innovation e di Cyber Defence, con controllo degli accessi (Access & Identity Management).
- Distinct labeling of AI-generated content. È prevista l'etichettatura distinta (distinct labeling) dei contenuti generati dall'AI e degli esiti delle decisioni AI: obbligo della dicitura "Generato tramite l'ausilio di Intelligenza Artificiale Generativa" su ogni Output e marcatura dei contenuti sintetici in formato leggibile e rilevabile ai sensi dell'AI Act.
- Mechanisms to detect/correct drift or degradation. Sono attivi sistemi di controllo che monitorano le performance dei modelli e generano alert automatici in caso di deterioramento (drift/degradation) del modello. A supporto, il catalogo dei sistemi AI è mantenuto continuamente aggiornato con monitoraggio del livello di rischio tramite un'interfaccia Power BI dedicata e, al rilascio in produzione, si verifica la coerenza tra questionario e sistema, attivando misure correttive in caso di variazione della classe di rischio.
- Regular assessments for fairness/bias. I modelli in produzione sono sottoposti a valutazioni ricorrenti tramite gli stessi sistemi di monitoraggio delle performance con alert automatici; inoltre il Group Risk Management integra i rischi AI nel framework di gestione del rischio ed esegue risk assessment aggiornati.
- Initiatives to lower the ecological footprint. A2A adotta iniziative per ridurre l'ecological footprint dei data center e dei modelli AI: ricorso a data center di prossimità alimentati possibilmente da fonti rinnovabili, monitoraggio delle emissioni di CO2 dei propri sistemi e sperimentazione di modelli proprietari/open eseguiti localmente su macchine proprietarie (sovranità dell'AI), con il supporto di Life Ventures (AI Strategy & Development).
- Appeals process. I sistemi AI sono censiti come tutti i sistemi aziendali ed è possibile aprire ticket specifici sull'applicazione di riferimento per segnalazioni e contestazioni.
- Quantification of impact on sustainability. Alcune iniziative basate sull'AI hanno un impatto diretto sugli outcome di sostenibilità, in particolare sulla gestione degli sprechi e sul riciclo.
- Training of employees. È prevista la formazione obbligatoria e continua dei dipendenti (training of employees) sull'uso etico e sulla sicurezza dell'AI: corso introduttivo sui fondamenti dell'IA Generativa con questionari di verifica, corso specialistico per ogni strumento autorizzato e corso di aggiornamento annuale obbligatorio; l'accesso completo agli strumenti è subordinato al completamento della formazione.

Processo di gestione e risoluzione dei reclami

A2A Energia dispone di un processo strutturato per la gestione e la risoluzione dei reclami, che prevede la conferma della ricezione della segnalazione e la piena trasparenza sulle tempistiche di gestione. In caso di reclamo inviato tramite il sito web, il cliente riceve automaticamente un'e-mail di conferma dell'avvenuta ricezione, in conformità alla normativa vigente, con l'indicazione dei tempi massimi di risposta (30 giorni). Per le segnalazioni trasmesse tramite PEC, attualmente viene fornita la sola conferma di avvenuta consegna prevista dal canale stesso; è tuttavia previsto per il 2026 un ulteriore sviluppo che introdurrà anche l'invio della comunicazione di presa in carico. I clienti possono monitorare in ogni momento lo stato di avanzamento della pratica attraverso l'area riservata del sito, dalla presa in carico fino alla chiusura del reclamo. Il processo prevede inoltre, ove necessario, un contatto telefonico per approfondire e chiarire la problematica segnalata. Qualora il reclamo venga evaso oltre i tempi standard definiti dall'Autorità di Regolazione per Energia Reti e Ambiente (ARERA), è previsto l'accredito automatico di un indennizzo nella prima bolletta utile, comunicato direttamente al cliente nella risposta al reclamo. Infine, nella sezione "Tutela del cliente – Standard di qualità" del sito web sono pubblicati sia gli standard di risposta previsti da ARERA (30 giorni solari) sia i tempi medi di risposta registrati da A2A Energia.

Risk management reporting

Il framework di Enterprise Risk Management (ERM) di A2A garantisce l'identificazione, la valutazione, il monitoraggio e la rendicontazione dei rischi strategici, operativi ed emergenti.
Di seguito è riportata la descrizione del rischio emergente "Perdita strutturale di competitività delle plastiche riciclate rispetto ai polimeri vergini e conseguente interruzione delle filiere di riciclo della plastica

	Rischio emergente
Evidenze a supporto	Il rischio è inoltre menzionato nella **Relazione sulla Gestione**, nella sezione *"Rischi legati alle attività industriali e di business"* a pagina 437.
Nome del rischio emergente	Perdita strutturale di competitività delle plastiche riciclate rispetto ai polimeri vergini e conseguente interruzione delle filiere di riciclo della plastica
Categoria	Economica
Descrizione	I produttori di imballaggi e di altri prodotti in plastica potrebbero non trovare più economicamente conveniente acquistare granuli di plastica riciclata, poiché questi presentano costi superiori rispetto alla plastica vergine. Tale criticità sarebbe principalmente dovuta alla commercializzazione, a prezzi inferiori, di granuli vergini prodotti in Paesi extraeuropei. Di conseguenza, i centri di selezione della plastica in Italia, inclusi gli impianti del Gruppo A2A di Muggiano e Cavaglià, potrebbero registrare una significativa riduzione dei flussi in uscita a causa del minore utilizzo di granuli riciclati nella produzione di imballaggi e altri manufatti in plastica. In tale scenario, i centri di selezione potrebbero anche interrompere il ritiro della plastica proveniente dalla raccolta differenziata, con possibili ripercussioni sull'intera filiera a monte. Questo rischio si manifesta in una fase in cui A2A sta incrementando gli investimenti nelle attività di economia circolare e intende rafforzare la propria leadership nel trattamento dei rifiuti, nel recupero di materia e nella valorizzazione delle risorse, in coerenza con il Piano Strategico 2024-2035.
Impatto	Una riduzione prolungata della domanda di plastiche riciclate potrebbe compromettere le performance operative ed economiche degli impianti di selezione della plastica di A2A, inclusi quelli di Muggiano e Cavaglià, determinando minori ricavi dalle attività di recupero di materia e una riduzione della redditività delle operazioni di riciclo. Nel lungo periodo, nello scenario peggiore, si potrebbe arrivare alla sospensione delle attività di recupero presso gli impianti di selezione della plastica del Gruppo.

Azioni di mitigazione	A2A monitora costantemente gli sviluppi normativi e di mercato che influenzano i mercati dei materiali riciclati e collabora attivamente con associazioni di settore, consorzi per il riciclo (tra cui COREPLA) e stakeholder istituzionali. Le principali misure di mitigazione includono: • il rafforzamento della collaborazione con i consorzi nazionali e le autorità pubbliche per sostenere mercati finali stabili per i materiali riciclati; • il monitoraggio dell'evoluzione della normativa europea che promuove il contenuto riciclato e gli obiettivi di economia circolare.

I rischi climatici fisici per il Gruppo A2A

Nella figura 1 sono descritti i rischi climatici materiali di tipo fisico per il Gruppo A2A, individuate a seguito del processo di analisi della materialità finanziaria effettuata nell'ambito della Rendicontazione di sostenibilità 2025. Per ogni rischio identificato, viene indicata la linea di business interessata, l'eventuale opportunità collegata, l'orizzonte temporale su cui il rischio o l'opportunità si possono manifestare, la descrizione del rischio e dell'opportunità, il tipo di impatto sul business, la strategia di gestione e il collegamento alle risorse da cui il business dipende nonché al posizionamento lungo la catena del valore. In particolare, sono stati valutati gli impatti sulle attività aziendali e sulle vendite dei prodotti energetici per effetto dei cambiamenti climatici.
La valutazione economico- finanziaria o reputazionale dei rischi climatici fisici riguarda le criticità rilevanti emerse dalla analisi dei pericoli legati al clima e dall'analisi di materialità.
I rischi e le opportunità climatiche sono identificati in base a tre orizzonti temporali: di breve termine, corrispondente all'anno di budget; di medio termine, da due a cinque anni; di lungo temine, oltre cinque anni e fino al 2035. La scelta di tali orizzonti è stata basata sull'analisi del contesto climatico, economico, energetico e normativo di riferimento (di seguito definita come analisi di scenario). Queste definizioni degli orizzonti temporali trovano coerenza e riscontro nel Piano industriale, che abbraccia un orizzonte di dieci anni essendo esteso al periodo 2026-35, e nella metodologia dell'Enterprise Risk Management, che identifica e valuta i rischi come differenza rispetto agli obiettivi e alle previsioni del Piano industriale.

E1_1 - Business Unit Generazione & Trading	
Classificazione e orizzonti temporali	**Classificazione**: Physical; Chronic **Orizzonte temporale**: Breve periodo, Medio periodo Lungo periodo
Tema di Rischio/Opportunità	**Cambiamento nel regime delle precipitazioni (idraulicità)** Rischi legati a variazioni della disponibilità idrica per le principali aste idroelettriche del Gruppo
Impatto sul business/attività aziendale	**Rischio/opportunità economico-finanziario** Impatto: minori/maggiori volumi e marginalità della produzione idroelettrica.

Strategia di gestione e investimenti	Sviluppo di strumenti atti a migliorare le previsioni di precipitazioni e deflussi. Elaborazione di analisi e modelli ingegneristici a supporto della programmazione degli impianti idroelettrici sia di medio che di breve termine, anche con il supporto di competenze in campo meteorologico interne al Gruppo. Produzione idroelettrica ben distribuita sul territorio italiano. Il Piano industriale comprende investimenti per ottimizzare l'utilizzo della risorsa idrica derivata a scopo idroelettrico (es. aumento dell'efficienza di produzione e pompaggi).
Risorse e value chain	Rischi/opportunità legati a disponibilità della risorsa idrica, a monte della catena del valore

E1_2 - Business Unit Smart Infrastructures	
Classificazione e orizzonti temporali	**Classificazione:** Physical, Acute **Orizzonte temporale:** Breve periodo, Medio periodo, Lungo periodo **Classificazione:** Transition Technology **Orizzonte temporale:** Medio periodo, Lungo periodo
Tema di Rischio/Opportunità	**Resilienza delle reti di distribuzione dell'energia elettrica** Rischio di interruzioni del servizio di distribuzione dell'energia elettrica causate principalmente da: cause fisiche: - picchi di richiesta per il condizionamento estivo, conseguenti a ondate di calore; - allagamenti causati da piogge intense; cause transition: - maggiore domanda di energia conseguente alla l'elettrificazione di servizi (Data Center, auto elettrica, sviluppo trasporto pubblico, riscaldamento). Opportunità di effettuare investimenti remunerati finalizzati ad aumentare la resilienza e la flessibilità delle reti di distribuzione dell'energia elettrica.
Impatto sul business/attività aziendale	**Rischio reputazionale** Impatti reputazionali in caso di interruzioni frequenti o prolungate del servizio. Penali per mancato rispetto dei livelli minimi sulla continuità del servizio. Soccombenza nei contenziosi avviati da coloro che hanno subito un danno economico. **Opportunità economico-finanziaria** Remunerazione degli investimenti di gestione del rischio con tasso prestabilito nell'ambito del business regolato ARERA. Margini già compresi nelle previsioni del Piano industriale.
Strategia di gestione e investimenti	Gruppo di Lavoro, in collaborazione con il Comune di Milano, per la gestione degli effetti da precipitazioni estreme e delle ondate di calore. Il Piano industriale 2026-35 comprende un programma di investimenti per il mantenimento e lo sviluppo della rete elettrica, tali da consentire sia

	l'adattamento ai rischi climatici fisici sia la progressiva elettrificazione dei servizi energetici (riscaldamento con pompe di calore, mobilità elettrica, cucine a induzione ecc.), migliorandone l'efficienza e riducendo le emissioni di CO2. In particolare, il piano comprende interventi di potenziamento e razionalizzazione delle reti, delle cabine secondarie, delle cabine primarie ed un ampliamento dei sistemi di gestione da remoto degli asset. L'approccio risk based nella gestione degli asset ha portato all'ottenimento della certificazione ISO 55001 "Sistemi di gestione degli asset".
Risorse e value chain	Rischio legato a picchi di domanda di energia sulla rete, a valle della catena del valore, per quanto concerne problematiche legate all'aumento delle temperature e all'elettrificazione dei servizi. I fenomeni di allagamento insistono sulle operazioni proprie del gruppo. Potenziali benefici reputazionali, tecnici ed economico-finanziari in collegamento al progetto Mindflex, progetto che ha l'obiettivo di rendere la rete di distribuzione locale più flessibile per favorire il processo di transizione energetica grazie all'ottimizzazione dell'uso di energia elettrica rinnovabile generata da piccoli produttori sul territorio.

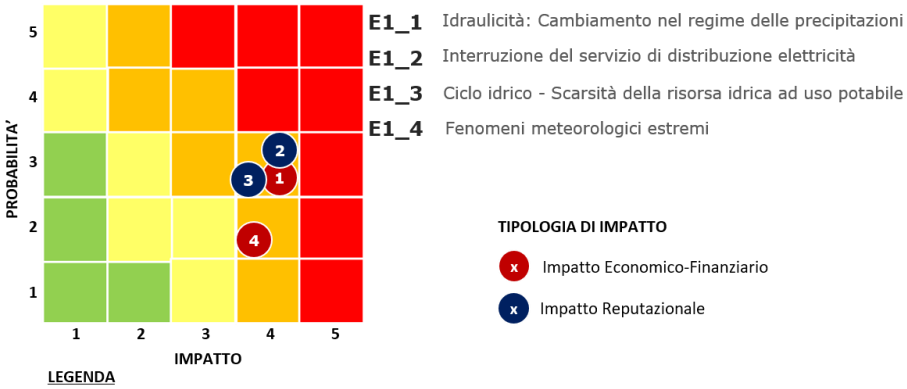
E1_3 - Business Unit Circular Economy	
Classificazione e orizzonti temporali	**Classificazione**: Physical, Chronic **Orizzonti temporali**: Breve periodo, Medio periodo, Lungo periodo
Tema di Rischio/Opportunità	**Scarsità della risorsa idrica per usi potabili** Rischio di non erogare con continuità l'acqua potabile in caso si manifestino periodi prolungati di siccità e/o cambiamenti nel regime idrologico.
Impatto sul business/attività aziendale	**Rischio reputazionale** Impatto reputazionale in caso di interruzioni del servizio di erogazione dell'acqua per periodi prolungati e/o su porzioni di territorio significative.
Strategia di gestione e investimenti	Mappatura delle perdite dagli acquedotti al fine di individuare i tratti maggiormente critici. Studi per utilizzare – in condizioni di scarsità/ emergenza le riserve d'acqua dolce (laghi) ad integrazione delle fonti di monte. Partecipazione al progetto "Water Stressed Areas": mappatura dei comuni più a rischio e affinamento del monitoraggio delle quantità di acqua trattata, erogata e persa. Monitoraggio continuo del livello delle fonti e dei serbatoi. Gestione delle emergenze con autobotti e serbatoi mobili, anche col supporto della Protezione Civile. Il Piano industriale comprende investimenti per: - ridurre le perdite dalla rete idrica - realizzare la captazione da nuove fonti di approvvigionamento

	- interconnettere gli acquedotti in modo da creare una “collaborazione” tra fonti di approvvigionamento e reti di distribuzione.
Risorse e value chain	Rischi legati a disponibilità della risorsa idrica, a monte della catena del valore.

E1_4 – Gruppo A2A	
Classificazione e orizzonti temporali	**Classificazione:** Physical, Acute **Orizzonti temporali**: Breve periodo, Medio periodo, Lungo periodo
Tema di Rischio/Opportunità	**Fenomeni meteorologici estremi** Rischi per gli asset del Gruppo e per la continuità del business in esito ai rischi derivanti dai pericoli climatici fisici di tipo acuto (alluvioni, frane, bombe d’acqua, trombe d’aria, grandine) che interessino impianti e le infrastrutture del Gruppo
Impatto sul business/attività aziendale	**Rischio economico-finanziario** Impatto: danni diretti sugli asset del Gruppo e danni indiretti dovuti alla necessità di interrompere le attività produttive. Impatti reputazionali qualora detti eventi estremi non fossero gestiti in modo ottimale ai fini della sicurezza del territorio nelle aree di competenza del Gruppo.
Strategia di gestione e investimenti	Contratti di assicurazione con copertura estesa anche a danni derivanti da fenomeni naturali. Piani di miglioramento in ottica loss prevention, condivisi con il broker assicurativo. Procedure e piani di emergenza e di business continuity per gestire in maniera tempestiva ed ottimale il sopraggiungere di eventuali fenomeni meteorologici acuti. Realizzazione di modifiche impiantistiche volte a prevenire fenomeni di inquinamento in caso di “bombe d’acqua”. Progettazione e realizzazione degli impianti (es. eolici e fotovoltaici) effettuata tenendo conto delle caratteristiche del territorio e della climatologia locale (es. stabilità dei versanti, ventosità, ecc).
Risorse e value chain	Rischio che insiste sulle operazioni proprie del gruppo con conseguenze di interruzione dei servizi essenziali anche a valle della catena del valore.

Heatmap dei rischi climatici fisici

Gli scenari di riferimento precedentemente illustrati sono considerati nelle analisi svolte dalla funzione ERM, per l'identificazione dei rischi collegati al cambiamento climatico, contribuendo a fornire insight al management per assicurare la resilienza del business model di A2A.
Nella seguente Figura 2 sono rappresentati sinteticamente sulla heatmap impatto – probabilità dei rischi descritti nella tabella di Figura 1.
I rischi sono stati quantificati in base alle assumptions riportate nella Relazione sulla Gestione 2025 (pag 154).



LEGENDA

RISCHI Livello di impatto
1 irrilevante
2 poco rilevante
3 rilevante
4 molto rilevante
5 critico

LIVELLO DI PROBABILITA'	Min	Max
1 improbabile	0	5%
2 difficilmente probabile	5%	25%
3 probabile	25%	50%
4 molto probabile	50%	75%
5 altamente probabile	75%	

Per i rischi e le opportunità economico-finanziari le scale di impatto sono riferite a impatti su EBITDA medi annui. Il livello 4 corrisponde a impatti superiori a circa 28 M€/a, il livello 5 a impatti superiori a circa 76 M €/a.