

## 6. LA GOVERNANCE

---

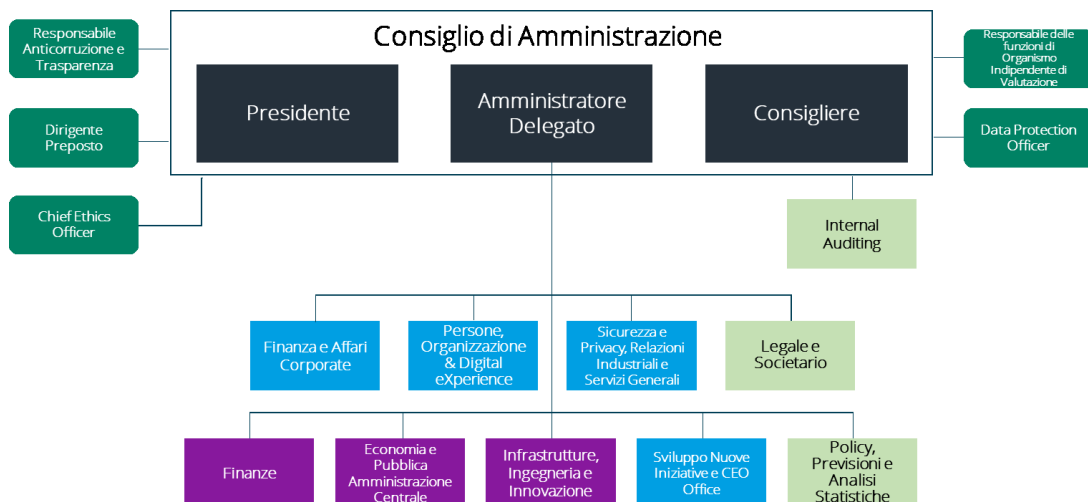
Gli interventi organizzativi del 2021 hanno perseguito l'obiettivo comune di consolidare il presidio sui Clienti e rafforzare il ruolo aziendale quale partner tecnologico della PA anche in ottica di eventuale sviluppo prospettico del ruolo di Polo Strategico Nazionale.

In particolare, nell'area *Business e Technology*, le Direzioni di Business hanno visto completarsi e affinarsi il percorso intrapreso nel 2020 finalizzato ad una più efficace interlocuzione con i Clienti, ad una maggiore semplificazione dei flussi informativi e ad un più puntuale presidio delle nuove opportunità di business nate nel corso del biennio, tra le quali risulta sicuramente degno di nota il contributo diretto di Sogei al Piano Nazionale di Ripresa e Resilienza (PNRR). I cambiamenti organizzativi sono stati coadiuvati da inserimenti da mercato funzionali, tra le altre cose, all'adozione del modello operativo Sogei in mercati storicamente presidiati attraverso il governo di alto livello, piuttosto che di specifiche professionalità a supporto del funzionamento del PNRR.

La Direzione *Service & Technology Innovation Hub* è stata profondamente rivisitata con l'obiettivo di un più efficace presidio delle tematiche gestite, coerentemente con il processo di Trasformazione Digitale della PA attraverso l'utilizzo di architetture *cloud*. La Direzione, completando operativamente il percorso intrapreso nel 2020, è stata pertanto ridisegnata per perimetrare e segregare l'ambito di presidio e resilienza tradizionale del *Cloud Data Center* infrastrutturale, all'interno del quale si colloca anche uno specifico ambito di responsabilità in materia di *Cyber Defence* e le attività di produzione di servizi e soluzioni trasversali a più Clienti, garantendo così l'ingegnerizzazione dell'innovazione e il governo e presidio del ciclo produttivo del *software*.

Nell'area *Corporate*, sono stati attuati interventi organizzativi tesi all'affinamento e consolidamento del modello, completando l'individuazione di responsabilità specifiche ed operando marginali interventi di razionalizzazione delle competenze organizzative.

Nel 2021 si è inoltre proceduto a definire importanti riorganizzazioni, poste in essere a febbraio 2022, che hanno ridefinito la macrostruttura organizzativa nel seguente modo.



La riorganizzazione delle Direzioni di *Business* in Divisioni ha lo scopo di consolidare il modello di presidio diretto dei Clienti strategici e facilitare lo sviluppo di nuove collaborazioni. È stata inoltre istituita la Direzione Sviluppo Nuove Iniziative e *CEO Office* per individuare nuove opportunità e coadiuvare le Divisioni di *Business* nel cogliere le evoluzioni del mercato, garantendo un approccio strutturato all'industrializzazione dei nuovi servizi/prodotti offerti. La nuova Direzione presidia direttamente l'offerta legata ai nuovi servizi di consulenza e al *business* derivante dal Polo Strategico Nazionale.

Gli interventi organizzativi del 2022 sono inoltre supportati dall'introduzione di un nuovo modello di *Governance* Aziendale, con l'istituzione di una serie di comitati aziendali interfuzionali che, attraverso la facilitazione della comunicazione, dell'esame e delle decisioni congiunte fra le diverse responsabilità aziendali, portino ad un rafforzamento del presidio delle attività strategiche. L'organizzazione dei Comitati, ispirata alla norma ISO 37000, si integra con quella formalizzata dall'organigramma con lo scopo di creare Valore, rispetto ad un obiettivo strategico o tattico, ottimizzando le professionalità trasversali all'Azienda e facendo leva sui principi di *Accountability* e di *Leadership*.

## 6.1 CORPORATE GOVERNANCE

I diritti dell'Azionista di Sogei sono esercitati dal Ministero dell'Economia e delle Finanze - Dipartimento del Tesoro-Direzione VII-Finanza e Privatizzazioni, in virtù di quanto previsto dall'art. 5, comma 7, del DPCM 26 giugno 2019, n. 103, così come modificato dal DPCM 30 settembre 2020, n. 161, che provvede agli atti conseguenti in base alla legislazione vigente.

Secondo quanto previsto all'art. 20 dello Statuto sociale, il Dipartimento del Tesoro e il Dipartimento delle Finanze, quest'ultimo per l'esercizio del "Controllo analogo" ad esso spettante in relazione alla natura *in house* della Società, hanno il diritto di avere dagli Amministratori notizie e informazioni sulla gestione e amministrazione della Società. L'Azionista e il Dipartimento delle Finanze verificano la rispondenza dell'azione sociale alle direttive impartite e al Piano generale annuale di cui all'art. 26 dello Statuto. In particolare, tali Dipartimenti devono essere periodicamente informati sul budget comprensivo della relazione previsionale e programmatica contenente i programmi di investimento e il piano annuale. Inoltre, gli Amministratori devono trasmettere mensilmente al Dipartimento delle Finanze i verbali delle riunioni del Consiglio di Amministrazione e del Collegio Sindacale e l'ordine del giorno delle adunanze del medesimo Consiglio di Amministrazione.

Inoltre, ai sensi dell'art. 26 dello Statuto sociale, la gestione della Società spetta agli Amministratori, i quali compiono le operazioni necessarie per l'attuazione dell'oggetto sociale, tenuto conto degli indirizzi ricevuti dal Dipartimento delle Finanze e in conformità alle previsioni del Contratto di Servizi Quadro e della Convenzione stipulata con il Dipartimento dell'Amministrazione Generale, del Personale e dei Servizi, ai sensi del Decreto Legislativo n. 414 del 1997.

Il Dipartimento delle Finanze, sentite per i profili di competenza le altre Amministrazioni affidanti, impartisce le Direttive generali concernenti le strategie, l'organizzazione, le politiche economiche, finanziarie e di sviluppo della Società.

La *governance* aziendale dispone di un sistema composito di prevenzione e mitigazione di rischi di non conformità.

Nel corso del 2021 non sono state emesse a carico di Sogei sanzioni, anche non monetarie, per non conformità a leggi e regolamenti, così come non sono state avanzate azioni legali riferite a concorrenza sleale, antitrust e pratiche monopolistiche. Non si rilevano inoltre sanzioni di carattere amministrativo, fiscale o tributario.

Oltre alla sede principale di via Mario Carucci, 99 - 00143 Roma, Sogei ha le seguenti sedi secondarie:

- via Mario Carucci, 85 - 00143 Roma;
- via Atanasio Soldati, 80 - 00155 Roma.

Personale Sogei è anche dislocato presso le sedi dei Clienti.

#### **Altri contatti:**



+39 06 5025 1 (centralino)



[protocolloSogei@pec.Sogei.it](mailto:protocolloSogei@pec.Sogei.it) (casella di posta certificata del Protocollo)



[ufficiostampa@Sogei.it](mailto:ufficiostampa@Sogei.it) (casella e-mail dell'ufficio stampa)



[www.Sogei.it](http://www.Sogei.it)



[https://twitter.com/@Sogei\\_SpA](https://twitter.com/@Sogei_SpA)



<https://goo.gl/jp9L6L>



[www.linkedin.com/company/Sogei](http://www.linkedin.com/company/Sogei)



[https://www.instagram.com/Sogei\\_spa/?hl=it](https://www.instagram.com/Sogei_spa/?hl=it)

#### **6.1.1 CONSIGLIO DI AMMINISTRAZIONE**

L'art. 21 dello Statuto prevede che la Società sia amministrata da un Consiglio di Amministrazione, composto da un numero di tre membri, di cui due dipendenti dell'Amministrazione economico-finanziaria e il terzo con funzioni di Amministratore Delegato, secondo quanto previsto dall'art. 23 quinquies del D.L. 6 luglio 2012, n. 95, convertito dalla legge 7 agosto 2012, n. 135. Lo Statuto prevede, altresì, che la composizione del Consiglio di Amministrazione debba assicurare il rispetto delle disposizioni di legge e regolamentari vigenti in materia di equilibrio tra i generi.

Inoltre, sempre all'art. 21, è previsto il divieto di corrispondere gettoni di presenza, premi di risultato deliberati dopo lo svolgimento dell'attività e trattamenti di fine mandato.

L'art. 27 dello Statuto, relativamente alle Deleghe, prevede la possibilità che il Consiglio di Amministrazione, previa delibera dell'Assemblea degli Azionisti, attribuisca deleghe gestionali al Presidente sulle materie indicate dall'Assemblea, determinandone in concreto il contenuto.

#### **6.1.2 DELEGHE E POTERI CONFERITI**

Il Presidente e l'Amministratore Delegato hanno la Rappresentanza legale stabilita ai sensi dell'art. 29, commi 1 e 2 dello Statuto. Con delibera del Consiglio di Amministrazione del 13 luglio 2021 sono state conferite all'Amministratore Delegato le più ampie deleghe di gestione e di esercizio della firma sociale. Il Consiglio di Amministrazione del 13 luglio 2021 è stato informato che sono presenti, fino a eventuale revoca, le procure già conferite ai Direttori e le deleghe e le procure nei seguenti ambiti, quali ad esempio:

GRI 102-22  
GRI 102-23  
GRI 102-24

GRI 102-26

- la designazione a Responsabile del servizio di Prevenzione e Protezione Aziendale, sempre in conformità al D.Lgs. n. 81/2008;
- la delega a Funzionario alla Sicurezza, così come previsto dal DPCM n. 22/2011;
- la delega per il settore Privacy, in conformità al Regolamento Europeo in materia di protezione dei dati personali (UE) 2016/679;
- la delega a fornire all'Autorità Giudiziaria, e ai soggetti dalla stessa delegati, nell'ambito delle indagini di Polizia Giudiziaria, nonché alle Strutture Organizzative dell'Amministrazione finanziaria all'uopo accreditate, le risultanze, i dati e le informazioni oggetto dell'attività di verifica richiesta, così come effettuata dalle competenti strutture di Sogei;
- la procura a Responsabile della gestione documentale e della conservazione dei documenti trattati da Sogei sul sistema di conservazione digitale.

In data 29 gennaio 2020 e, successivamente il 3 maggio 2021 sono state conferite le deleghe di Funzioni in materia di tutela della salute e della sicurezza nei luoghi di lavoro e in materia di tutela ambientale e di prevenzione incendi ai sensi del D.Lgs. n. 81/2008, per le diverse sedi aziendali.

Da ultimo si rileva che, nel corso del 2021, le procure conferite nel corso del 2020 non sono state oggetto di modifica e/o integrazione.

### **6.1.3 INFORMATIVA AL CONSIGLIO DI AMMINISTRAZIONE**

L'art. 27 dello Statuto sociale prevede che gli organi delegati riferiscano sul generale andamento della gestione e sulla sua prevedibile evoluzione, nonché sulle operazioni di maggior rilievo, per dimensioni e caratteristiche, effettuate da Sogei e dalle sue controllate. Il Responsabile dell'Internal Auditing riferisce almeno una volta l'anno al Consiglio di Amministrazione, ovvero ad apposito Comitato eventualmente costituito all'interno dello stesso.

Il Responsabile della Prevenzione della Corruzione e della Trasparenza trasmette al Consiglio di Amministrazione, su base annuale, una specifica informativa sull'adeguatezza e sull'osservanza del piano di prevenzione della corruzione.

Al Consiglio di Amministrazione riferiscono, altresì, in funzione delle specifiche disposizioni normative o organizzative, l'Organismo di Vigilanza, il Dirigente Preposto, il Responsabile della Prevenzione della Corruzione e della Trasparenza, il Responsabile delle Funzioni analoghe all'Organismo Indipendente di Valutazione, il *Data Protection Officer* (DPO) e il *Chief Ethics Officer*.

L'incarico a Responsabile della Prevenzione della Corruzione e della Trasparenza (RCPT) è stato rinnovato dal Consiglio di Amministrazione in data 18 novembre 2021; il *Data Protection Officer* è stato nominato, dal Consiglio di Amministrazione, in data 19 marzo 2018, il Responsabile delle Funzioni analoghe all'Organismo Indipendente di Valutazione è stato nominato, dal Consiglio di

Amministrazione, in data 09 settembre 2021, mentre il *Chief Ethics Officer* è stato nominato con Ordine di Servizio n. 4/2021.

#### **6.1.4 ORGANI DI CONTROLLO**

##### **6.1.4.1 *Controllo Analogico***

Sogei si pone, nei rapporti con il MEF, su due “binari” istituzionali: con il Dipartimento del Tesoro per quanto attiene al quadro dei diritti dell’Azionista, e con il Dipartimento delle Finanze per gli atti di natura negoziale, declinati attraverso un affidamento *in house*.

La giurisprudenza, sia comunitaria che nazionale, ha precisato che tale affidamento è configurabile solamente nel caso in cui l’ente committente eserciti sul soggetto affidatario un “controllo analogo” a quello che esercita sui propri servizi, stabilendo così una relazione di vera e propria subordinazione gerarchica e funzionale, assimilabile a quella che sussiste nei confronti delle articolazioni organizzative interne all’ente stesso.

Per tale motivo, ad aprile 2008, l’azionista ha provveduto ad adeguare lo Statuto della Società, limitando i poteri degli Amministratori, i quali compiono le operazioni necessarie per l’attuazione dell’oggetto sociale tenuto conto degli indirizzi ricevuti dall’Assemblea e dal Contratto di Servizi Quadro e riconoscendo allo stesso DF, in quanto ente committente, un potere di approvazione degli indirizzi generali concernenti le strategie, l’organizzazione, nonché le politiche economiche, finanziarie e di sviluppo della Società.

A partire da maggio 2010 - attraverso una serie di incontri tra il Vertice aziendale e la Direzione Sistema Informativo della Fiscalità del Dipartimento delle Finanze - sono state definite le regole e le modalità operative attraverso cui attuare il controllo analogo, secondo quattro linee di intervento: potere di approvazione in materia di indirizzi generali (piano triennale, piani industriali, organigramma, budget, piano degli investimenti), potere di indirizzo, controllo di gestione, controllo sulla qualità del servizio reso.

A partire dal 1° luglio 2013, a seguito dell’incorporazione del ramo IT Consip, per le direttive riguardanti le attività svolte dall’ex ramo Consip, il DF opera d’intesa con il DAG, che a sua volta raccoglie le istanze degli altri Dipartimenti del Ministero interessati.

La definitiva attuazione dell’istituto del Controllo analogo in Sogei presenta vantaggi sia per il committente che per la Società, in quanto garantisce e dà certezza al rapporto *in house*, presupposto di una condivisione nella definizione e nel raggiungimento di obiettivi di business tra Sogei e Amministrazione, in attuazione delle direttive di governo.

Da ultimo, si segnala che con comunicazione del 30 luglio 2019 il Dipartimento delle Finanze ha integrato la Direttiva sull’esercizio del Controllo analogo. Tale integrazione è volta alla

determinazione di direttrici per la definizione di linee di azione industriale e per l'implementazione del piano generale annuale concernente le attività, gli investimenti e l'organizzazione.

#### **6.1.4.2 Collegio Sindacale**

L'art. 30 dello Statuto sociale prevede che il Collegio Sindacale sia costituito da tre componenti effettivi e due supplenti e che essi restino in carica per tre esercizi e siano rieleggibili.

Prevede, inoltre, che la composizione del Collegio Sindacale debba assicurare il rispetto delle disposizioni di legge e regolamentari vigenti in materia di equilibrio tra i generi e che, se nel corso del mandato vengono a mancare uno o più sindaci effettivi, subentrino i sindaci supplenti nell'ordine atto a garantire il rispetto delle suddette disposizioni di legge e regolamentari in materia di equilibrio tra i generi.

Prevede anche che, oltre a quanto previsto dall'art. 2399 c.c., non possano essere nominati sindaci i soci che detengano partecipazioni qualificate o di controllo in società produttrici e fornitrici di apparecchiature elettroniche, di programmi e di servizi IT, nonché coloro che sono legati a dette società, o alle società da queste controllate o alle società che le controllano o a quelle sottoposte a comune controllo, da un rapporto di lavoro o da un rapporto continuativo di consulenza o di prestazione di opera retribuita ovvero da altri rapporti di natura patrimoniale che ne compromettano l'indipendenza.

#### **6.1.4.3 Società di revisione**

Ai sensi dell'art. 32 dello Statuto, il controllo contabile è demandato a un revisore contabile o a una società di revisione legale iscritti nell'apposito registro, secondo quanto previsto dall'art. 2409-bis c.c.

L'incarico di revisore legale dei conti, ai sensi dell'art. 13 del D.Lgs. 27 gennaio 2010, n. 39, è attualmente affidato alla Società TREVOR S.r.l. nominata dall'Assemblea degli Azionisti dell'8 giugno 2020, per la revisione legale dei conti degli esercizi riguardanti il triennio 2020-2022.

#### **6.1.4.4 Magistrato della Corte dei conti**

La Società è soggetta al controllo della Corte dei conti - Sezione controllo enti - che lo esercita ai sensi dell'art. 100, comma 2, della Costituzione, secondo le modalità dettate dall'art. 12 della Legge 21 marzo 1958, n. 259, per il tramite del Magistrato Delegato, che a tal fine assiste alle sedute del Consiglio di Amministrazione e del Collegio Sindacale. Il controllo ha per oggetto la

gestione finanziaria della Società, nell'ottica della tutela del pubblico Erario. L'esito del risultato del controllo eseguito sulla gestione finanziaria della Società è annualmente sintetizzato in una deliberazione, approvata dalla competente Sezione della Corte dei conti, inviata alle Camere e al Governo.

#### **6.1.4.5 Commissione Parlamentare di Vigilanza sull'Anagrafe Tributaria**

La Commissione Parlamentare di Vigilanza sull'Anagrafe Tributaria, in base a specifica previsione di legge, ha il compito di esercitare la sorveglianza sull'operato della stessa Anagrafe e di effettuare indagini conoscitive e ricerche sulla gestione dei servizi di accertamento e riscossione dei tributi locali, vigilando altresì sui sistemi informativi a questi riferibili.

#### **6.1.4.6 Organismo di Vigilanza**

L'Organismo di Vigilanza della Società, previsto nel Codice Etico e nel Modello 231, ha il compito di vigilare sull'adeguatezza in termini di efficacia ed efficienza e sull'osservanza dei due documenti. L'Organismo opera sulla base di un apposito regolamento interno ed è dotato di autonomi poteri di iniziativa e di controllo. È composto da tre membri, un professionista esterno con funzioni di Presidente, il responsabile dell'Internal Auditing e un professionista esterno con profilo di alta esperienza legale nelle problematiche di specifica attinenza dell'Organismo stesso. L'Organismo di Vigilanza riferisce al Consiglio di Amministrazione e al Collegio Sindacale tramite la predisposizione di un reporting periodico e, ogni qualvolta lo ritenga opportuno, riporta al Consiglio di Amministrazione, per il tramite del Presidente, su circostanze e fatti significativi del proprio ufficio o al verificarsi di situazioni straordinarie.

#### **6.1.4.7 Dirigente Preposto**

Nell'ambito del sistema di controllo interno, il Dirigente Preposto opera con gli altri organi di controllo e vigilanza, con gli organi sociali e con le strutture aziendali interessate secondo le interrelazioni, gli ambiti di operatività e i flussi di reporting definiti nel "Regolamento interno del Dirigente Preposto". Con deliberazione del Consiglio di Amministrazione del 27 marzo 2019, la



posizione di Dirigente Preposto è stata affidata al Responsabile della Funzione Administration, Finance & Control, dott.ssa Cristina Barbaranelli, fino all'approvazione del Bilancio di esercizio 2021.

#### **6.1.4.8 Internal Auditing**

La Funzione opera in base al "Mandato di Internal Auditing", approvato dal Consiglio di Amministrazione della Società il 14 settembre 2020. Così come stabilito dallo Standard internazionale 1000 "Finalità, Poteri e Responsabilità" per la pratica professionale emanato dall'Institute of Internal Auditors, il Mandato è un documento formale che, tra l'altro:

- definisce finalità, poteri e responsabilità dell'attività di internal audit;
- stabilisce la posizione dell'attività nell'organizzazione;
- autorizza l'accesso ai dati, alle persone e ai beni aziendali che sono necessari per lo svolgimento degli incarichi;
- definisce l'ambito di copertura delle attività di internal audit.

La principale missione assegnata all'Internal Auditing, coerentemente con gli standard internazionali, è quella di proteggere e accrescere il valore dell'organizzazione, fornendo *assurance* obiettiva e *risk based*, consulenza e competenza - anche in relazione a quanto previsto dal MOG Sogei - attraverso un continuo processo di monitoraggio, valutazione e miglioramento del sistema di controllo interno e di gestione dei rischi.

#### **6.1.5 MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.Lgs. 231/2001 – MOG**

In assenza di novità normative sull'ampliamento del catalogo dei reati, l'attività di aggiornamento del MOG ha riguardato l'allineamento alle variazioni organizzative e il recepimento delle modifiche alle attività sensibili e al sistema di controllo interno, nonché la relativa associazione alle diverse famiglie di reato, conseguenti all'esecuzione dell'*integrated risk assessment* ex D.Lgs. 231/2001 e L.190/2012. Inoltre, si è provveduto alla formalizzazione di una tabella univoca di raccordo tra aree a rischio, reati associati, attività sensibili e procedure di riferimento, comune sia al Modello 231 che al Piano Triennale di Prevenzione della Corruzione e della Trasparenza.

Un'iniziativa formativa in modalità e-learning su MOG e PTPCT indirizzata a tutto il personale dipendente è stata fruita, a fine dicembre 2021 da circa il 97% del personale. È stata inoltre rivolta formazione al personale direttamente coinvolto sull'applicazione di normative di rilevanza 231 (*cybersecurity*, GDPR, D.Lgs. 81/2008 etc.).

### **6.1.6** PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE E DELLA TRASPARENZA - PTPCT

Il PTPCT è stato aggiornato al triennio 2022-2024. Il Piano integra e completa l'applicazione della metodologia di gestione del rischio corruttivo introdotta dal Piano Nazionale Anticorruzione 2019, su tutti i processi aziendali. In tal senso perfeziona il metodo di computo, mantenendo inalterato l'approccio valutativo, e termina la mappatura del contesto interno, già avviata nel 2020, procedendo a verticalizzare sui singoli processi l'articolazione dei principi strategici, metodologici e finalistici. Ciascun processo dell'*Enterprise Architecture* (EA) è stato descritto nel suo funzionamento identificandone eventuali attività sensibili, a rischio corruzione associandole alle corrispondenti aree di rischio. In particolare, il processo di gestione del rischio corruttivo ha avuto ad oggetto complessivamente l'analisi di 68 processi e di 136 attività sensibili potenzialmente esposte a tale rischio.

È stato dato particolare rilievo alla definizione e alla pianificazione delle misure generali di prevenzione della corruzione, con particolare riguardo alle modalità attuative degli obblighi di trasparenza.

Sempre in linea con quanto richiesto dal Controllo analogo è stata verificata, tramite accesso al casellario giudiziale e alla Camera di Commercio, la veridicità delle dichiarazioni di inconferibilità/incompatibilità rese dai dirigenti, ai sensi della Delibera ANAC n.833/2016.

Nell'anno sono, poi, proseguite le attività finalizzate all'attuazione della normativa in materia di obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni e delle società in controllo pubblico, prevista dal D.Lgs. 14 marzo 2013, n. 33. In tale ambito, è stato effettuato il costante aggiornamento della sezione del sito web "Società trasparente".

Nell'anno la formazione in tema di prevenzione della corruzione e di trasparenza è stata erogata interamente a distanza (*e-learning* o aula virtuale); è stato predisposto un corso *e-learning* di aggiornamento su MOG e PTCPT, destinato a tutto il personale. Il corso è stato fruito da circa il 97% dei dipendenti. Altra formazione è stata erogata in tema di conflitto di interessi, incompatibilità, inconferibilità, pantouflage, *compliance* integrata 231 e anticorruzione nelle società pubbliche, *whistleblowing* e trasparenza.

Nel 2021 non ci sono stati episodi di corruzione accertati.

### **6.1.7** ETICA

#### **6.1.7.1** *Codice Etico*

L'orientamento all'etica è, per noi di Sogei, un approccio indispensabile per l'affidabilità nei rapporti con gli azionisti, con i clienti e, più in generale, con l'intero contesto civile ed economico

in cui operiamo. L'etica esprime l'insieme di norme di condotta seguite da una persona. Il suo ambito d'azione, pur rinviando a un universo astratto, fatto di principi e valori, è tutt'altro che teorico: riguarda il quotidiano e si traduce in norme di comportamento.

Per tale motivo, nel 2021, è stata effettuata una revisione profonda del Codice Etico aziendale, che di fatto regola l'insieme dei diritti, dei doveri e delle responsabilità che tutti noi assumiamo espressamente nei confronti degli *stakeholder* con i quali interagiamo nell'ambito dello svolgimento delle nostre attività.

In particolare, la sua evoluzione ha perseguito i seguenti molteplici obiettivi:

- adeguare il “Tone of Voice” per renderlo coerente con altri prodotti aziendali destinati sia alle persone di Sogei sia agli interlocutori esterni;
- sintetizzare, valorizzando esclusivamente i principi, i valori e i comportamenti richiesti limitando i riferimenti normativi alle norme essenziali;
- aggiornare i riferimenti normativi alle norme attuali;
- fornire maggior chiarezza e immediatezza dei messaggi contenuti per una condivisione e un'attuazione sempre più efficace, anche mediante esempi di situazioni pratiche (cosa fare/cosa evitare);
- integrare i principi di Etica Digitale e aggiornare i comportamenti con quanto già definito a livello di Modello di Leadership;
- progettare/realizzare gradualmente un prodotto completamente digitale ed esteticamente più apprezzabile.

#### **6.1.7.2 Etica digitale**

Nel corso del periodo 2020-2021 è stato definito e avviato un progetto volto a costruire *l'Ethical eXperience* di #NoidiSogei, nell'ottica di accrescere la consapevolezza etica nella cultura organizzativa e *nell'execution* quotidiana.

Primo passo di questo percorso è stato prendere coscienza della prassi etica ed esplicitarla attraverso la Tavola dell'Etica Digitale, ovvero l'insieme di valori e principi etici che orientano il nostro agire, individuati attraverso l'ascolto del vissuto del top management e grazie all'analisi dei principali contributi internazionali sul tema.

L'approfondimento del tema etico nei sistemi algoritmici, porta alla focalizzazione su otto tendenze tematiche chiave: privacy, responsabilità, sicurezza, trasparenza e “spiegabilità”, equità e non discriminazione, controllo umano della tecnologia, responsabilità professionale e promozione dei valori umani.

Alla base di questo nucleo normativo, le analisi della letteratura indicata sopra conducono ad una serie di principi individuali su cui la PA in generale sarà chiamata a confrontarsi all'aumentare della pervasività tecnologica. Il tutto al fine di massimizzare i benefici e minimizzare i possibili danni dell'introduzione di artefatti (principalmente IA ma non solo) nell'attività produttiva.

Il progetto, dunque, prevede la disseminazione del modello etico proposto e la sua adozione concreta nel processo produttivo attraverso un approccio *bottom-up* realizzato mediante gli *Ethical Lab*, ovvero attraverso momenti di co-progettazione che hanno l'obiettivo di individuare requisiti, *best practice* ed azioni da seguire durante lo sviluppo delle soluzioni digitali per i Clienti.

Propedeutica all'adozione a regime del modello è la sua sperimentazione su un prodotto/servizio pilota.

L'utilizzo sempre più pervasivo di dati, servizi informatici, tecnologie, Intelligenza Artificiale può comportare implicazioni etiche che richiedono di essere attentamente valutate a sostegno e garanzia del *purpose* di Sogei e della responsabilità assunta verso gli *stakeholder*.

Si è voluto pertanto individuare un Modello di Etica Digitale da applicare ai servizi erogati, con particolare riferimento alle soluzioni di Intelligenza Artificiale (IA) e che utilizzano algoritmi di *Machine Learning* (ML), assegnando a Sogei il ruolo di *assurance* di uno sviluppo digitale fondato su valori e principi di eticità.

Il tema dell'etica digitale è compreso fra le priorità di Sogei che, già a partire dal 2019, ha preso parte alle diverse fasi di definizione delle linee guida per l'Intelligenza Artificiale lanciato dalla Commissione Europea e ha avviato una collaborazione con Padre Paolo Benanti, figura di riferimento nel panorama internazionale, al fine di un primo inquadramento del tema etico nel contesto Sogei. Padre Benanti è un francescano del Terzo Ordine Regolare che, ormai da diversi anni, si occupa di etica, bioetica ed etica delle tecnologie. In particolare i suoi studi si focalizzano sulla gestione dell'innovazione: internet e l'impatto del *Digital Age*, le biotecnologie per il miglioramento umano e la biosicurezza, le neuroscienze e le neurotecnologie.

Tale collaborazione ha posto le basi per la definizione del progetto *Ethical Experience* nel digitale, avviato a fine 2020, con l'obiettivo di accrescere la consapevolezza etica nella cultura organizzativa e nell'*execution* quotidiana di Sogei.

Primo passo di questo percorso è stato prendere coscienza della prassi etica ed esplicitarla attraverso la Tavola dell'Etica Digitale di #NoidiSogei, ovvero l'insieme di valori e principi etici che orientano il nostro agire.

Il secondo passo ha previsto la costruzione, attraverso un approccio *bottom-up*, di un modello operativo applicato al processo produttivo. A tal fine, sono stati organizzati 4 *Ethical Lab*, momenti di co-progettazione aventi l'obiettivo di individuare requisiti, *best practice* e azioni da

seguire durante lo sviluppo delle soluzioni digitali per i nostri Clienti, che hanno coinvolto circa 40 persone appartenenti alle diverse strutture organizzative interessate.

Il percorso proseguirà dal 2022 con la sperimentazione del nuovo approccio su un prodotto/servizio pilota, fino ad una adozione a regime del modello. La valutazione in base a criteri di *Ethical Quality* dei prodotti sviluppati consentirà infatti di attribuire ai nostri servizi gli *Ethical badge*, un riconoscimento che renderà immediatamente visibile ai nostri Clienti l'impegno assunto e le *skill* consolidate da #NoidiSogei.

L'etica nel digitale rappresenterà una competenza propria del curriculum Sogei e apporterà un ulteriore valore aggiunto per i nostri Clienti garantendo un importante vantaggio competitivo.

### **Tavola dell'etica digitale**

L'*Ethical eXperience* si fonda sulla Tavola dell'Etica digitale, che accompagna la realizzazione dei prodotti/servizi affinché questi sappiano "prendersi cura" delle persone che li utilizzano.

La Tavola, riportata anche nel codice etico, è composta da:

- *Ethical drivers*, principi che danno una direzione all'agire e regolano la scelta del proprio comportamento cercando di tutelare, attuare e migliorare il valore;
- *Ethical Values*, valori che contribuiscono positivamente alla vita della persona (es. onestà, libertà, dignità, etc.).

La definizione della Tavola dell'Etica digitale è partita da una *survey* indirizzata al *top management* e finalizzata ad ascoltare i principi e i valori etici da loro vissuti in azienda. Per analizzare e sintetizzare i risultati ottenuti sono stati attuati dei passi metodologici che tenessero conto non solo del contesto di #NoidiSogei, ma anche del dibattito internazionale sull'etica digitale.

### **Modello dell'etica digitale**

Il modello, disegnato sulla base delle risultanze del dibattito internazionale in corso, mira a guidare la riflessione sulle implicazioni etiche dei servizi e dei prodotti sviluppati da Sogei e a individuare requisiti, *best practice* e azioni da seguire durante le diverse fasi del processo di produzione delle soluzioni digitali per i nostri Clienti, ma è scalabile ad ulteriori processi.

In particolare, il modello prevede l'utilizzo di *checklist* che rappresentano uno stimolo alla riflessione sui temi etici:

- *Checklist* di Triage, al fine di valutare la rilevanza dei temi etici per uno specifico prodotto/servizio da sviluppare, in considerazione delle scelte tecnologiche (AI, *big data*, social media, *blockchain*, *cloud*, etc.), dei dati utilizzati e delle tipologie di utenti, evidenziando quando è necessario un approfondimento analitico successivo;

- *Checklist* operative da compilare nel corso dello sviluppo del prodotto/servizio, al fine di individuare le *best practice* da mettere in atto nelle diverse fasi di processo a fronte dei soli temi etici risultati rilevanti nei momenti precedenti.

I temi etici considerati, in linea con quanto definito nello studio di Harvard, sono protezione dei dati personali, *accountability*, sicurezza e *safety*, trasparenza e possibilità di spiegare il funzionamento, correttezza e non discriminazione, perdita del controllo umano, responsabilità professionale e promozione dei valori umani.

### **6.1.7.3 Etica del lavoro e conflitti di interessi**

Nell'ultimo triennio, Sogei ha rivolto la sua attenzione allo studio, alla diffusione e all'applicazione dell'etica del lavoro. Un tema complesso con cui ci si confronta giornalmente nell'esercizio delle proprie attività professionali. Il percorso iniziato, nel 2018, con la nomina del *Chief Ethics Officer* e continuato nel 2019 con la revisione e diffusione del Codice Etico e l'implementazione di un processo per la gestione dei conflitti di interessi, nel 2020, si è posto come obiettivo principale di promuovere la disseminazione della cultura dell'etica in azienda, attraverso seminari, forum, *survey*, etc.

Nel 2021, Sogei ha realizzato e reso fruibile a tutti i dipendenti, una soluzione informatica del processo di Gestione dei Conflitti di Interessi. La messa in linea sulla intranet della nuova applicazione, ha lo scopo di ottimizzarne il flusso operativo, garantendo la gestione, consultazione, conservazione e tutela digitale dei dati, conformemente a quanto normato in materia di sicurezza e privacy.

Il progetto di ingegnerizzazione, avviato nel corso del 2020, rappresenta per Sogei una opportunità per applicare e sperimentare le conoscenze e le nuove metodologie ispirate alla *Ethical eXperience*, intesa come capacità di realizzare servizi e prodotti con un impatto reale e positivo sulla azienda e sulla società civile. Il piano, inoltre, comprende una fase di revisione e aggiornamento della procedura che sarà conclusa nei primi mesi del 2022 e che ritrae la volontà di Sogei sia di applicare nuovi modelli di comunicazione volti a valorizzare la chiarezza e immediatezza delle informazioni, sia la determinazione a perfezionare e snellire quei processi che sono impattati dalle misure di prevenzione alla trasparenza e corruzione previste nella procedura di Gestione dei conflitti di interesse. Successivamente alla fase di approvazione si procederà, nel corso del 2022, con l'elaborazione e avvio della relativa formazione.

L'attività di valutazione del Comitato *Ethics & Compliance*, relazionata periodicamente al Consiglio di Amministrazione e agli altri Organi di controllo, non ha portato, nel corso del 2021, alla classificazione di alcun caso di conflitti di interesse.

## 6.2 IL MODELLO DI CONTROLLO E GESTIONE DEI RISCHI

Il ruolo istituzionale e strategico ricoperto, la natura e la molteplicità dei dati e delle architetture gestite, la rilevanza e dimensione delle infrastrutture a supporto, comportano necessariamente una particolare attenzione alla individuazione e gestione dei rischi da parte di Sogei.

Il processo di gestione dei rischi vede coinvolti molteplici attori che, ciascuno per l'area di propria competenza, provvedono a un continuo monitoraggio dei rischi potenziali, sia sulla base di metodologie strutturate di *risk assessment* e strumenti applicativi a supporto, che secondo un approccio di continuo presidio operativo.

E' stato quindi adottato un modello di gestione integrata (*Enterprise Risk Management, ERM*) ispirato alle *best practice* internazionali che coinvolge, ciascuno per le proprie competenze, gli organi di *governance*, l'organizzazione aziendale, ed i c.d. *risk specialist*, ossia quelle figure deputate a presidiare specifici perimetri di rischio (ad esempio il dirigente Preposto alla redazione dei documenti contabili societari, che monitora i rischi amministrativo-contabili, e il Responsabile Prevenzione della Corruzione e Trasparenza, responsabile del presidio dei rischi corruttivi).

La valutazione dei principali profili di rischio, effettuata nell'ambito del progetto di realizzazione del sistema ERM, ha portato ad evidenziare le seguenti aree principali di rischio e gli eventi rischiosi sottostanti.

Aree di rischio	Eventi rischiosi
<b>Strategici</b>	<p>Scelte del <i>top management</i> con impatto sugli obiettivi strategici</p> <p>Percezione dell'immagine della Società da parte di clienti, fornitori, opinione pubblica e autorità</p> <p>Evoluzione/innovazione imprevedibile della tecnologia e dei costi/investimenti ad essa connessi</p> <p>Eventuale irrigidimento delle condizioni sociopolitiche o economiche</p>
<b>Operativi</b>	<p>Rapporto con i clienti</p> <p>Atti dolosi/accidentali o eventi di forza maggiore</p> <p>Guasti o malfunzionamenti</p> <p>Sviluppo dei servizi applicativi</p> <p>Gestione delle attività operative</p> <p>Relazioni con i fornitori</p>
<b>Financial Reporting</b>	<p>Svolgimento delle attività e degli adempimenti necessari per la corretta rilevazione dei fatti di gestione aziendale</p>
<b>Compliance</b>	<p>Responsabilità contrattuale o extra-contrattuale</p> <p>Violazione di leggi, regolamenti o autoregolazioni</p>

Aree di rischio	Eventi rischiosi
	Evento di infortunio o lesione a danno del personale della Società, nonché potenziali eventi di inquinamento o impatto ambientale ascrivibili alla Società

Per i rischi il cui valore residuo è prossimo o supera la soglia di *appetite*, è prevista la definizione di una strategia di trattamento del rischio stesso, che può portare alla mitigazione attraverso attività e/o progetti che possano incidere sull'efficacia dei controlli interni, al trasferimento o all'accettazione del rischio.

### **6.2.1 IL PROGETTO ERM – ENTERPRISE RISK MANAGEMENT**

Nel corso del 2021 è stato completato il *deployment* del cruscotto dei macro-rischi aziendali (rischi ERM). Ciascun rischio di livello ERM è stato costruito attraverso il consolidamento di rischi elementari, è stato collegato ad un processo aziendale ed assegnato ad un *risk owner* responsabile di monitorarlo e di aggiornarne la valutazione.

Nel mese di novembre 2021 è stata avviata la prima campagna di *assessment* dei rischi ERM, completamente dematerializzata e condotta sulla nuova piattaforma tecnologica adottata (RSA Archer), attraverso la profilazione di specifici ruoli, ed è stato possibile per i vari attori, ciascuno per le relative competenze, valutare i rischi, monitorarli e definire piani di trattamento.

I risultati delle campagne di valutazione dei rischi ERM sono disponibili al Vertice attraverso delle *dashboard* complessive e sintetiche; tutte le *dashboard* sono navigabili in modo dinamico e consentono di "sprofondare" le diverse sezioni dei grafici accedendo a viste sempre più analitiche.

Parallelamente al completamento del cruscotto ERM, nel corso del 2021, si è proceduto ad una profonda revisione del modello complessivo evolvendo dall'idea iniziale di un cruscotto *stand-alone* di macro-rischi aziendali, privo di un collegamento dinamico con l'attività di presidio di tutti gli attori del sistema di controllo, ad un sistema dalla connotazione molto più ampia che rende l'ERM un vero e proprio *funnel* di integrazione dei *risk specialist*.

In particolare, nel corso del 2021, sono stati digitalizzati, nella medesima piattaforma tecnologica che ospita l'ERM, i *workflow* di attività dei *risk specialist* che presidiano i rischi relativi agli ambiti 262/05, 231/01, 190/12, ISO-9001.

La digitalizzazione dei *workflow* di attività si è spinta ben oltre una dematerializzazione *tout court*, ed ha condotto ad una revisione complessiva dei rispettivi modelli di gestione in ottica di integrazione con l'ERM.



Nello specifico tutto il patrimonio informativo raccolto dai vari attori e le evidenze delle campagne di *assessment*, condotte da ciascuno per le rispettive competenze, confluiscono all'interno dei macro-rischi di livello ERM.

Successivamente anche le funzionalità per la realizzazione dell'intero ciclo dei piani e degli interventi di Internal Audit sono state digitalizzate in uno specifico *workspace* all'interno della piattaforma ERM.

In questo modo è stata realizzata una federazione – informativa, funzionale e di processo - tra Internal Audit ed ERM con l'obiettivo di massimizzare l'efficacia e la sostenibilità della *governance*.

In particolare, tutto il patrimonio informativo raccolto dai *risk specialist* e sintetizzato nell'ERM è reso disponibile all'Internal Auditing che, in tale modo, potrà esercitare il suo ruolo di "orchestratore" e "coordinatore" del sistema di controllo interno e gestione dei rischi con una maggiore efficacia e, d'altro canto, potrà inserire i propri rilievi nell'ERM incidendo sulla valutazione dei macro-rischi.

#### **6.2.2** **GESTIONE DEI RISCHI FINANZIARI**

Per quanto si riferisce in particolare ai rischi di carattere finanziario si forniscono di seguito alcune informazioni relative all'esposizione e gestione dei rischi di natura finanziaria connessi allo svolgimento dell'attività aziendale.

**Rischio di cambio** - L'attività svolta dalla Società non la espone a rischi di cambio.

**Rischio di liquidità** - Il rischio di liquidità è gestito tramite la disponibilità di linee di credito presso istituti bancari, grazie alle quali la Società è in grado di rispettare sempre i tempi di pagamento previsti nei contratti passivi con i fornitori, indipendentemente dalla dinamica degli incassi.

**Rischio di tasso di interesse** - I ricavi delle vendite e delle prestazioni e i flussi di cassa operativi sono sostanzialmente indipendenti dalle variazioni dei tassi di interesse di mercato.

**Rischio di credito** - Per le attività svolte, Sogei non presenta situazioni creditizie a rischio di solvibilità, in quanto riferite a committenti della PA.

**Rischio di prezzo** - I corrispettivi dei servizi erogati da Sogei sono fissati contrattualmente e soggetti a revisioni periodiche tramite benchmark. Non sono pertanto soggetti a fluttuazioni di mercato di breve periodo.

**Rischio connessi all'utilizzo di strumenti finanziari** - Sogei non opera sul mercato degli strumenti finanziari derivati e non è esposta a rischi di tale tipologia.

### **6.2.3 LA COMPLIANCE E LA GESTIONE DEI RISCHI DI NON CONFORMITA' NORMATIVA**

La *Compliance* Integrata ha il principale compito di assicurare, per la prevenzione o la mitigazione dei rischi di non conformità normativa e relativi impatti reputazionali, il controllo ex ante di procedure e prassi aziendali alla normativa di riferimento di specifiche aree definite dal Vertice aziendale, fornendo anche supporto e collaborazione alle strutture aziendali interessate a ciascun *assessment*, nonché di provvedere a prestare opinioni e pareri di *compliance* in ambito *Corporate Governance*.

Nel corso del 2021 è proseguita la realizzazione del progetto di sviluppo e integrazione ERM e Modello di Compliance Integrata, che si propone di garantire la confluenza dei rischi elementari nei rischi ERM, con l'obiettivo finale di realizzare un modello di integrazione digitale che permetta di muoversi all'interno di un perimetro coerente con gli standard definiti di sostenibilità, integrando le risultanze delle valutazioni con l'ERM, al fine di permettere la condivisione delle informazioni a livello consolidato.

Il nuovo modello dovrebbe permettere una rapida interazione con l'ERM ed essere improntato al massimo dialogo tra funzioni interne (e di gruppo) per il raggiungimento di una visione integrata dei rischi, in quanto indipendente da aspetti "meramente normativi", ma con specifico focus sui rischi che impattano maggiormente sull'operatività aziendale (rischio operativo) e/o sulla flessione degli utili o del capitale derivante da una percezione negativa dell'azienda da parte degli *stakeholder* incluse le autorità di controllo e vigilanza.

È inoltre proseguita l'attività di monitoraggio e supporto normativo alle Funzioni di OIV che, anche nel corso del 2021, ha provveduto alle verifiche di competenza e alla collaborazione interna per l'aggiornamento dei dati e delle informazioni previste dalla normativa "Trasparenza" ed ha rilasciato l'attestazione di conformità richiesta dall'ANAC circa l'assolvimento degli obblighi di pubblicazione ai sensi dell'art. 1 della legge n. 190/2012.

## **6.3 I SISTEMI DI GESTIONE DEI PROCESSI**

Il Sistema di Gestione per la Qualità (SGQ), introdotto in Azienda nel 1995, rappresenta un modello di *governance* strettamente legato alla gestione globale del sistema Sogei, ispirato ai principi di efficienza, efficacia e miglioramento continuo, finalizzato alla soddisfazione delle aspettative dei Clienti.

Il SGQ, basato sulla definizione di processi interrelati e controllati, costituisce, per queste sue caratteristiche di non settorialità e monitoraggio costante, uno strumento organizzativo e gestionale particolarmente idoneo a una realtà aziendale così complessa come quella di Sogei.

Nel 2021, nell'ottica di una piena rispondenza all'approccio *Risk Based Thinking* della norma ISO 9001, sono proseguite le attività volte al governo integrato dei rischi aziendali del sistema di gestione nel modello di *Enterprise Risk Management* (ERM).

Sogei nel 2021 ha ottenuto e mantenuto le certificazioni rispetto alle seguenti norme di riferimento.

Norma di riferimento	Ambito	Certificazione
UNI EN ISO 9001:2015	Sistema di gestione per la qualità (SGQ)	Si –RINA Rinnovato il certificato novembre 2020
UNI EN ISO 27001:2013	Sistema di gestione per la sicurezza delle informazioni (SGSI)	Si - RINA Rinnovo effettuato il 3 e 4 giugno 2021
UNI EN ISO 20000-1:2018	Sistema di gestione per i Servizi (SGS)	Si - RINA Sorveglianza il 17 e 18 giugno 2021
UNI EN ISO 22301:2014	Sistema di gestione per la Continuità Operativa (SGCO)	Si - RINA Sorveglianza il 17 e 18 giugno 2021
Linee guida per la vigilanza sui <b>Gestori PEC</b>  (V 1.0 del 18 novembre 2009)	Vigilanza sui Gestori PEC	Si verifica esterna – AgID a richiesta sorveglianza semestrale - audit interni
Lista di riscontro per le attività di vigilanza e certificazione di conformità (Vers.1 del 14 aprile 2017) per <b>Conservazione digitale</b>	Vigilanza e certificazione di conformità AgID del servizio di Conservazione digitale	Si - AgID tramite RINA Mantenuta la conformità il 22 giugno 2021
UNI EN ISO 45001:2018  (ex BS OHSAS 18001)	Sistema di gestione per la salute e sicurezza sul lavoro (SGSL)	No Implementato e oggetto di audit interni
UNI EN ISO 9001:2015	Sistema di gestione per la qualità (SGQ)	Si –RINA Rinnovato il certificato novembre 2020

Come riportato nello schema, Sogei ha effettuato il primo mantenimento della certificazione del Sistema di gestione dei Servizi (SGS) ai sensi della ISO 20000-1:2018 e del Sistema di gestione per la continuità dei servizi (SGCS) ai sensi della ISO 22301:2014, definiti inizialmente per rispondere ai requisiti previsti per il Polo Strategico Nazionale.

### **6.3.1** **DIGITALIZZAZIONE PROCESSI E MAPPA PROCESSI**

In coerenza con il percorso di digitalizzazione intrapreso da Sogei, è proseguita l'attività di evoluzione della "Mappa dei processi" all'interno dell'*Enterprise Architecture* (EA) aziendale per il quale è stato avviato un progetto, volto all'integrazione dell'EA con il costituendo **Data Lake** aziendale, che consentirà, attraverso tecniche di AI (NLP - *Natural Language Processing* e *Ontology Based Knowledge Management*) la fruizione delle informazioni in modalità più intuitiva e flessibile.

Nel 2021, nell'ottica di costruire un modello di rappresentazione dei processi aziendali che consenta di avere una visione multidimensionale e sistemica del *business* anche alla luce delle evoluzioni del mercato, è stato avviato uno studio volto alla definizione del "Modello operativo" Sogei, inteso come una raffigurazione dinamica, che offra differenti punti di vista, basata su una logica di prodotto (*minimum valuable product*) e che dia visibilità delle interazioni all'interno dell'organizzazione aziendale.

Nel 2021 è proseguita inoltre l'applicazione della metodologia *Lean/Lean Six Sigma* sui processi aziendali attraverso la conduzione di progetti dedicati.

### **6.3.2**    **CUSTOMER SATISFACTION**

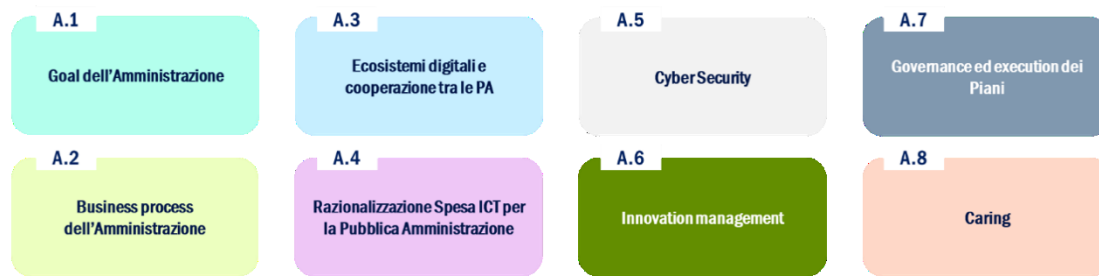
L'ascolto della voce del cliente-utente è di fondamentale importanza per l'individuazione degli interventi necessari non solo per l'evoluzione dei servizi offerti, ma anche per perseguire il miglioramento organizzativo e gestionale.

L'analisi dei risultati raccolti attraverso la misurazione oggettiva della soddisfazione del cliente consente di individuare le azioni necessarie a fornire prodotti e servizi sempre più rispondenti alle sue esigenze e aspettative. Per tale motivo Sogei ha perfezionato nel corso degli anni un sistema di ascolto del cliente/utente, mediante l'adozione di un processo strutturato che ha l'obiettivo di accrescere la qualità dei servizi offerti e consolidare il clima di fiducia e trasparenza.

A partire dalla fine del 2020, dopo tanto tempo e con il *commitment* del Vertice aziendale, è stato avviato un percorso progettuale volto alla realizzazione nell'anno 2021 di una campagna di Rilevazione della *Customer Satisfaction*, funzionale a:

- valutare la soddisfazione percepita, da parte di Clienti e Utenti, rispetto all'offerta SOGEI;
- individuare, sulla base dei feedback dichiarati dai Clienti, potenziali aree di ottimizzazione, evoluzione e ampliamento degli attuali modelli di collaborazione adottati tra Sogei e Amministrazioni;

La *survey*, rivolta a due diversi *cluster*, "Apicale" (Vertici dei clienti/Amministrazione) e "Manageriale" (Ruoli di responsabilità *Business/ICT* dei clienti/Amministrazione) ha consentito di approfondire insieme ai Clienti Istituzionali alcuni ambiti dell'offerta Sogei ritenuti di maggior valore.



L'indagine, di natura qualitativa e corredata da alcune valutazioni quantitative su temi specifici, si è svolta attraverso interviste al *cluster* "Apicale" e *focus group* con il cluster "Manageriale". Dall'analisi dei risultati è emerso che i temi relativi a *Cybersecurity* e *Goal dell'Amministrazione* rappresentano il principale punto di forza di Sogei mentre l'area percepita maggiormente da migliorare è *l'innovation management*. Inoltre, sono stati individuati alcuni temi specifici ritenuti significativi per il futuro, quali ad esempio, l'interoperabilità dei dati e la reingegnerizzazione dei processi.

Nel 2021, Sogei ha inoltre supportato il proprio cliente nello svolgimento delle rilevazioni sui propri servizi, in particolare:

- Dipartimento delle Finanze, sul servizio di gestione telematica del processo tributario (PTT) (indagine quantitativa e qualitativa);
- Ragioneria Generale dello Stato (IGIT), sul servizio RED EVO (indagine quantitativa);
- Agenzia delle Entrate, sui servizi erogati ai contribuenti diversamente abili (indagine qualitativa).

#### 6.4 GOVERNO DELLA SICUREZZA E DATA PROTECTION

Sogei ha maturato, negli anni, la consapevolezza che la sicurezza e più in generale la protezione delle informazioni debba essere ideata, progettata, implementata e gestita, non solo attraverso processi strutturati e l'implementazione di misure di sicurezza logica (*firewall*, crittografia, etc.) e fisica, ma anche attraverso l'implementazione di un sistema di governo di "*Information Security & Data Protection*", presidiato da un *Chief Information Security Officer* (CISO), che permetta di governare e monitorare tutta la "filiera della sicurezza".

In questa organizzazione si inserisce la figura del *Data Protection Officer* (DPO), che svolge un ruolo chiave nel sorvegliare e monitorare l'attuazione degli adempimenti previsti dal "*General Data Protection Regulation* (GDPR)" e nel promuovere la cultura in tali ambiti.

La formazione è un elemento fondamentale a sostegno della protezione delle informazioni e della prevenzione degli incidenti e più in particolare dei *data breach* e, per adempire a tale scopo, sono stati utilizzati vari strumenti passando dalla classica formazione con docenti specializzati fino all'utilizzo delle piattaforme *social* disponibili. In particolare nel corso del 2021 sono stati erogati 7 corsi di formazione attraverso piattaforme di collaborazione e e 48 corsi in modalità *e-learning*, di cui 1 per i neo assunti sul *General Data Protection Regulation* – GDPR. È stato, inoltre, avviato un canale sulla piattaforma *social* Yammer, a disposizione di tutti dipendenti, con l'obiettivo di fornire informazioni, aggiornamenti e approfondimenti dal canale del Garante privacy e dalla stampa accreditata sulle novità normative, italiane ed europee, che riguardano il trattamento di dati personali.

A cura del DPO è continuato il percorso di sensibilizzazione attraverso la pubblicazione di pillole tematiche relative alla *Data Protection* sulla intranet e sui canali *social* aziendali.

#### **6.4.1 COMPUTER EMERGENCY RESPONSE TEAM (CERT)**

Nel 2021 il CERT Sogei ha visto confermare un approccio sempre migliorativo nei riguardi dei flussi di condivisione da e verso gli Enti istituzionali impegnati nel campo della *cybersecurity*, consolidando sia la gestione degli eventi *cyber* e che l'implementazione della piattaforma di *Cyber Threat Intelligence*, focalizzata su strumenti *open source* personalizzati, quali MISP, TheHive e Cortex, volti a garantire pienamente la loro integrazione nei processi consolidati di questo team. L'istanza MISP pubblica ha assicurato la raccolta di circa 400K IoC provenienti dai vari enti federati e, di conseguenza, avviato i vari processi di analisi per verificare la loro applicabilità nei contesti di riferimento. Con gli strumenti TheHive e Cortex, è in via di consolidamento l'automazione di gran parte dei processi di analisi e gestione degli eventi di sicurezza e allo stato attuale si è pronti per una fase sperimentale di utilizzo in configurazione *multi-tenant*. Sono infine state completate le attività preliminari all'abilitazione automatica degli IoC con le strutture tecniche Sogei con cui il CERT collabora giornalmente.

Inoltre il CERT Sogei ha continuato la sua collaborazione con la Guardia di Finanza nell'ambito della produzione di report dettagliati di *Cyber Threat Intelligence*, grazie all'ausilio di strumenti di analisi e ricerca che giornalmente individuano eventi di sicurezza su fonti aperte e chiuse, svelano tattiche, tecniche e motivazioni degli attori (*threat actors*) coinvolti nelle campagne di attacco.

In ambito formativo, nei primi mesi del 2021 il CERT Sogei ha erogato, su esplicita richiesta della Guardia di Finanza (GdF), un corso introduttivo alla *Cyber Threat Intelligence*; tale corso, erogato al SOC della GdF e diviso in una parte teorica ed in una pratica, ha approfondito le tematiche relative al *cyber threat hunting*, ai modelli di analisi e alle tecniche di contestualizzazione e correlazione necessarie per l'individuazione delle minacce, sfruttando strumenti di tipo OSINT e proprietari.

Sempre in ambito formativo, nel secondo semestre 2021, si è conclusa la terza sessione dell'Iniziativa di *Cybersecurity Awareness* che coinvolge i dipendenti dell'Agenzia delle Entrate. L'iniziativa ha come obiettivo l'aumento della consapevolezza riguardo le minacce *cyber*. Le prossime sessioni saranno svolte nel 2022 e mirano a coprire tutti i dipendenti dell'Agenzia delle entrate.

Nel corso del 2021 il CERT Sogei ha inoltre:

- pubblicato, sfruttando le nuove piattaforme di collaborazione messe a disposizione dall'Azienda (in particolare "Yammer") 7 avvisi riguardanti i temi di prevenzione e *awareness* in ambito *cybersecurity*; il canale dedicato "CERT Sogei" ha in tal modo costituito un veicolo importante di condivisione delle principali attività svolte quotidianamente dal CERT;
- gestito 4.046 eventi classificati per varie tipologie di evento/incidente e suddivisi per le diverse aree della *Constituency* del CERT Sogei. Nel dettaglio:
  - casi di *malware* (47%): identificati in *e-mail* e in altri vettori di codice malevolo, fronteggiati attivando le opportune strutture di sicurezza IT per l'aggiornamento dei sistemi di protezione e di rimozione;
  - possibili minacce verso le infrastrutture e i servizi gestiti da Sogei (6,4%): identificati i possibili vettori di attacco o di sfruttamento di vulnerabilità (tramite informazioni provenienti dalle fonti di *intelligence* e dalle attività di ricerca del CERT), gestiti attivando le opportune strutture aziendali per la mitigazione del rischio o la risoluzione della potenziale vulnerabilità;
  - eventi relativi a *spam* e *phishing* (42,5%): identificati, grazie anche alle segnalazioni degli utenti, in *e-mail* ingannevoli che mirano a rubare le credenziali di siti e servizi, risolti procedendo al blocco dei siti ad esse collegati;
  - eventi relativi alla divulgazione e dispersione (*leak*) di credenziali (1,2%): si tratta, nella quasi totalità dei casi, di *e-mail* istituzionali associate a *password* non riconducibili ad *account* "aziendali". Tali credenziali, esfiltrate da siti e portali terzi non sempre noti tramite attacchi riusciti (*Data Breach*), vengono raccolte dal CERT mediante canali di *intelligence* dedicati e comunicate direttamente all'utente stesso (nel caso di dipendente Sogei) o alla struttura di *cybersecurity* dell'Entità coinvolta (nel caso di ambito SIF) o al CERT-MEF (nel caso dei Dipartimenti Economia);
- per quanto riguarda Sogei Titolare, non è stata rilevata alcuna possibile violazione di dati personali, mentre in ambito Sogei Responsabile si sono verificati 11 eventi di violazione di dati personali, che sono stati gestiti, risolti e comunicati ai Titolari, clienti istituzionali di Sogei.

Nell'ambito dell'importante e consolidato ruolo di monitoraggio dell'attuazione dei Piani di Rientro (PdR)<sup>1</sup>, durante il 2021 il CERT ha monitorato 318 PdR di cui 134 nuovi, chiudendone 60.

#### **6.4.2 SICUREZZA FISICA**

La Sicurezza Fisica ed infrastrutturale rappresenta uno degli elementi centrali della gestione aziendale ed incide direttamente sui fattori di *governance* e sociali.

Le *policy* e le misure di *security*, che assicurano la tutela degli *asset* aziendali e del personale dipendente ed esterno che presidia il *campus* Sogei h24 e 365 giorni l'anno, sono infatti strettamente correlate all'impatto generato dalle varie attività e dal capitale umano.

È indispensabile quindi operare una continua revisione dei processi ed implementazione delle misure di sicurezza attraverso una costante valutazione dei rischi che, anche in considerazione del particolare periodo storico, sono sempre più eterogenei e aumentano in maniera direttamente proporzionale al consolidamento del ruolo di Sogei come partner strategico per la Nazione.

Il 2021 ha ulteriormente confermato il ruolo di primo piano di Sogei a supporto delle Istituzioni per la gestione della situazione emergenziale causata dalla pandemia Covid-19, richiedendo così l'ampliamento dei livelli di sicurezza sia per le minacce derivanti da fattori esterni, sia per garantire il rispetto delle normative e dei protocolli sanitari previsti nell'ambito delle misure di contrasto alla diffusione della pandemia, consentendo ai dipendenti e ai fornitori di operare nel pieno rispetto della tutela della salute.

In linea con gli obiettivi di sostenibilità, particolare attenzione è stata rivolta alla riconversione di alcune attività nell'ottica dell'impatto sui fattori ambientali attraverso l'avvio della digitalizzazione e ottimizzazione dei processi interni ed esterni che ha già prodotto importanti benefici, in particolare rispetto alla dematerializzazione cartacea e al traffico virtuale della posta elettronica, con una riduzione di circa 40% dei documenti cartacei e del 70% delle *e-mail*.

Esempio di questo nuovo percorso è il Progetto Macars, sviluppato nella sua fase iniziale nel corso del 2021, e che permetterà di semplificare e digitalizzare l'intero flusso gestionale degli accessi in azienda per tutto il personale esterno, consulenti e fornitori.

#### **6.4.3 SICUREZZA DELLE INFORMAZIONI**

Il principale input del sistema di Governo per la Sicurezza aziendale e quindi per la gestione integrata dei rischi di sicurezza logica, fisica e cibernetica, è rappresentato dal Sistema di

---

<sup>1</sup> Il Piano di Rientro è il documento che nel ciclo di sviluppo del software, a valle di un test di sicurezza (WAPT - Web Application Penetration Test), viene redatto e aggiornato ogni qualvolta vengano rilevate vulnerabilità su software in esercizio o destinato ad essere posto in esercizio, dettagliando gli interventi pianificati per sanare le suddette vulnerabilità



Gestione per la Sicurezza delle Informazioni (SGSI); tale sistema consente, attraverso un insieme strutturato di processi e una puntuale assegnazione di ruoli e responsabilità, la gestione dei rischi volta alla tutela delle informazioni trattate dall'Azienda. Il SGSI continua ad evolversi per far fronte alle esigenze di sicurezza aziendale e per rispondere ai requisiti di sicurezza che la normativa nazionale prescrive. In questa ottica le principali attività svolte nel 2021 hanno riguardato:

- la revisione della metodologia di *risk management* per l'integrazione con la *Business Impact Analysis* eseguita sui servizi;
- la conduzione di audit e *assessment* per la sicurezza delle informazioni trattate da servizi ICT critici. Nel corso dell'anno sono stati svolti 6 audit e 1 *assessment* nel rispetto della normativa AGID;
- l'aggiornamento delle politiche di sicurezza aziendali in conformità a nuovi requisiti di sicurezza informatica a cui è soggetta l'Azienda;
- il monitoraggio di indicatori di sicurezza informatica e il monitoraggio dei piani di trattamento del rischio definiti a seguito di audit e *assessment*. In ambito sicurezza delle informazioni, *data protection* e continuità operativa sono stati aperti 23 piani di rientro di cui 5 sono stati chiusi.

#### **6.4.4**     **CONTINUITÀ OPERATIVA**

Nel 2021 è stata confermata il mantenimento del certificato di conformità allo standard di riferimento ISO 22301:2014 del Sistema di Gestione per la Continuità Operativa (SGCO). È stata revisionata la metodologia per l'attività di *Business Impact Analysis*, volta all'individuazione dei parametri di continuità e delle risorse critiche ed integrata alla metodologia *Risk Analysis* sia in ambito SGSI che in ambito SGCO.

Il piano di Continuità Operativa è stato generalizzato ed esteso ai servizi ritenuti maggiormente critici, anche se ad oggi non inclusi nel campo di applicazione del certificato ISO22301 ed è stata finalizzata l'integrazione del suddetto Piano con il Piano di *Disaster Recovery*

Nel 2022 si prevede di estendere il campo di applicazione del SGCO includendo ulteriori servizi critici ed ampliando le attività di *testing* degli scenari di crisi.

#### **6.4.5**     **INFORMAZIONI CLASSIFICATE**

Sogei attua un Sistema di Gestione delle Informazioni Classificate (SGIC) che raccoglie e armonizza le varie procedure dedicate principalmente al personale in possesso di abilitazione di sicurezza. Congiuntamente al SGIC, è operativa e funzionante in Sogei un'area di sicurezza preposta a gestire le informazioni classificate nel rispetto della normativa sul Segreto di Stato.

L'area è gestita da una specifica struttura, governata dal Funzionario alla Sicurezza, con il supporto di altre figure aziendali, a seconda dei diversi ruoli operativi della Segreteria principale di Sicurezza Sogei.

Tutte le aree operative della Segreteria principale di Sicurezza, compresa l'infrastruttura CIS "Sicurezza dei *Communication and Information System*, ex Area EAD), sono riconosciute con specifico provvedimento dalla Presidenza del Consiglio dei Ministri – DIS e omologate dall'UCSe per trattare dati e documentazione con classifica di segretezza e qualifica di sicurezza fino a Segreto (S) – NATO UE/S.

Nel 2021 la documentazione classificata, trattata dalla Segreteria principale di Sicurezza su apposito registro di protocollo classificato, è stata di 100 richieste in ingresso e 104 richieste in uscita.

#### **6.4.6**    **DATI TUTELATI**

Sogei riceve dall'Autorità Giudiziaria e dai Clienti Istituzionali richieste riguardanti il reperimento delle operazioni registrate nel Sistema Informativo della Fiscalità, relative a uno o più soggetti (persone fisiche e giuridiche) e concernenti indagini in corso, investigazioni, accertamenti e verifiche.

Tali richieste, aventi quindi carattere riservato, considerate come "dati tutelati" e protocollate in un apposito registro dell'applicazione Protocollo, riguardano in particolare:

- l'estrazione puntuale o massiva di informazioni su contribuenti registrati nelle banche dati del SIF;
- il tracciamento delle operazioni di accesso e utilizzo dei servizi informatici effettuati dagli utenti del SIF e registrate negli archivi di log;
- l'estrazione di informazioni di tracciamento di posta elettronica e navigazione Internet;
- il tracciamento dei pagamenti delle fatture da parte della Pubblica Amministrazione, attraverso il monitoraggio della Piattaforma dei Crediti Commerciali;
- il tracciamento degli accessi al sistema NoiPA;
- l'estrazione puntuale o massiva di informazioni/documentazioni su uno o più cittadini registrati nelle banche dati del sistema NoiPA;
- estrazione delle informazioni sul Greenpass;
- estrazione delle informazioni sui decreti "sostegni";
- estrazione delle informazioni sui "Bonus".

Nell'anno 2021 sono state protocollate n. 1487 richieste in ingresso pervenute alla PEC dei dati tutelati e n. 2.066 risposte in uscita tramite la stessa PEC.

#### **6.4.7 DATA PROTECTION**

Nell'ambito del Regolamento Ue n. 2016/679 (GDPR) e del novellato Codice privacy (Decreto legislativo 30 giugno 2003, n. 196), Sogei opera in qualità di titolare dei trattamenti di dati personali effettuati in ambito societario e, in virtù della designazione conferita dalle Amministrazioni, in qualità di responsabile dei trattamenti di dati personali connessi ai servizi informatizzati erogati per conto delle Amministrazioni stesse.

Applicando il principio di *accountability* definito dallo stesso GDPR, l'azienda si è dotata di un Sistema di Gestione della Privacy (SGP) che si articola in un modello organizzativo con ruoli, responsabilità e ripartizione dei compiti tra le varie strutture rispetto al trattamento di dati personali e agli adempimenti imposti dalla normativa, in un'ottica di semplificazione, efficacia ed efficienza dell'organizzazione. Il SGP si applica a Sogei nel suo duplice ruolo di responsabile per le componenti informatizzate dei trattamenti delle Amministrazioni e di titolare dei trattamenti che svolge per le proprie funzioni societarie.

Le principali attività del 2021 hanno riguardato:

- l'aggiornamento, l'integrazione e la redazione documentale nell'ambito del SGP (*policy*, linee guida e procedure) per il recepimento dei nuovi dettami normativi a livello nazionale ed europeo, ai pronunciamenti del Garante italiano per la protezione dei dati personali e dell'EDPB (*European Data Protection Board*);
- l'informatizzazione della gestione degli adempimenti privacy sui trattamenti di dati personali, svolti per conto delle Amministrazioni o per fini societari, per renderne più agevole lo svolgimento e al tempo stesso conservarne lo storico;
- la revisione del processo per la designazione dei fornitori quali responsabili/sub-responsabili del trattamento in virtù delle decisioni della Commissione europea del 4 giugno 2021 su clausole contrattuali tipo tra titolari e responsabili (Decisione (UE) 2021/915) e sul trasferimento di dati personali verso paesi terzi (Decisione (UE) 2021/914);
- l'informazione/sensibilizzazione dei dipendenti sulle tematiche di *data protection*;
- la formazione dedicata alle strutture aziendali sulle metodologie adottate dall'azienda, di concerto con le Amministrazioni, per la protezione dei dati personali e valutazione di impatto;
- il supporto alle Amministrazioni titolari per lo svolgimento degli adempimenti privacy sui trattamenti di dati personali;

Sogei effettua inoltre periodicamente attività di verifica volte a migliorare la consapevolezza degli adempimenti previsti dalla normativa e a verificarne il corretto svolgimento.

Nel 2021 sono state svolte le seguenti verifiche:

- *assessment* per la verifica dei termini e criteri inerenti ai tempi di conservazione dei dati per i trattamenti societari con la valutazione di eventuali gap e relativa definizione di piani di rientro;
- *assesement* su tutti i servizi informatizzati che trattano dati personali;
- audit e self *assessment* e su alcuni fornitori;
- audit sugli amministratori di sistema per alcuni ambiti specifici;
- audit verticali su alcuni servizi informatizzati erogati per conto delle Amministrazioni.

## **6.5 LA GOVERNANCE IT**

In questi mesi di pandemia Sogei ha iniziato a ripensare il proprio modo di lavorare per poter rispondere in maniera veloce ed efficiente alle esigenze dei cittadini e del Paese, considerando le esperienze vissute durante il primo periodo di emergenza e mantenendo “un occhio” a ciò che la ripresa, grazie anche all'utilizzo dei fondi messi a disposizione del PNRR, potrà comportare in termini di necessità di applicazioni digitali che favoriscano la trasformazione della PA.

Abbiamo riflettuto profondamente su quanto accaduto per trasformare la situazione di emergenza in un'utile opportunità di cambiamento, da sfruttare oggi e, soprattutto, nel futuro e plausibile scenario di crescita, lavorando sul miglioramento dei modelli di produzione, sulle metodologie, sulle metriche e sugli strumenti utilizzati nel processo di produzione.

### **6.5.1 NUOVO MODELLO PMO**

La *mission* rinnovata di Sogei di partner strategico della PA nel percorso di innovazione e digitalizzazione del Paese richiede un'evoluzione del ruolo strategico del PMO.

L'aumento del numero di Pubbliche Amministrazioni “servite” evidenzia la necessità dell'azienda di avere sempre la «visione d'insieme» del suo operato per verificare in modo continuativo la sua capacità di agire nell'ambito di un modello di coerenza complessiva che assicuri il rispetto di parametri di efficienza ed efficacia.

Nel corso dell'anno è stato progettato ed in parte attuato il modello di un “Nuovo PMO Sogei” tenendo conto delle nuove sfide da affrontare, sulla base di quanto è emerso dalle interviste con i responsabili delle strutture organizzative, senza tralasciare elementi metodologici e di mercato.

L'attesa è quindi quella di un PMO che abbia una vista integrata e centralizzata di tutti i progetti e delle relative dimensioni di tempi e costi oltre ad un ruolo centrale di abilitatore dell'integrazione aziendale e di facilitatore per il *decision making*.

### **6.5.2 MODELLO INDUSTRIALE**

Nel corso del 2021 è stato progettato il nuovo Modello di *Governance* Industriale a partire dalle esperienze di applicazione del Modello operativo svolte negli anni precedenti.

Mentre il Modello operativo sviluppato nel 2020 aveva il principale obiettivo di fornire dati e informazioni per orientare le scelte e le decisioni di Sogei in considerazione delle strategie dettate dal Vertice aziendale, il progetto "Modello *Governance* industriale" sviluppato nel 2021 ha avuto finalità più ambiziose in quanto si è posto l'obiettivo di definire un *framework* operativo di *governance* industriale per la valutazione oggettiva della sostenibilità industriale di nuovi contratti/progetti e per l'analisi del modello attuato dall'azienda rispetto al modello industriale atteso.

Gli elementi industriali considerati sono:

- modelli di servizio e delivery adottati;
- strategie e modelli di presa in carico delle attività (*onboarding*);
- valore interno ed esterno creato e *performance* industriali attese;
- *mapping* e definizione delle strategie di mitigazione e presidio dei rischi specifici;
- sostenibilità operativa del contratto/progetto dal punto di vista di competenze necessarie, tempi, beni/servizi per l'avvio ed *execution* del contratto/progetto.

Consolidato il modello si procederà alla realizzazione di strumenti informatici che possano agevolare l'applicazione del modello.

### **6.5.3 GOVERNANCE DELLA PRODUZIONE**

In ambito processo di sviluppo nel 2021 si è iniziato ad applicare l'approccio *Agile* e *DevSecOps* su progetti di una certa complessità, nell'ambito dei quali sono state attuate le pratiche di *Scaling Agile* per via della necessità di coordinare il lavoro di diversi team *Scrum*.

Sempre in questa occasione si è dato il via alla sperimentazione del paradigma di *shift-left* per gli aspetti di sicurezza, individuando un *security champion* che in ottica *DevSecOps* fosse in grado di anticipare il prima possibile eventuali analisi di potenziali vulnerabilità, ottimizzando il tempo necessario per il superamento dei *penetration test* finali. In quest'ottica sono stati forniti anche ulteriori strumenti di automazione dei test dinamici di sicurezza.

### **6.5.3.1 Metriche dello sviluppo software**

Il centro di competenza interno ha consolidato la collaborazione con il GUFPI e l'IFPUG condividendo la propria esperienza e le proprie soluzioni in diverse conferenze sia nazionali che internazionali. In particolare è proseguito il coinvolgimento di Sogei nell'IFPUG sui lavori di due gruppi che si occupano dell'evoluzione metodologica:

- Functional Sizing Standards Committe;
- Non-Functional Sizing Standards Committe.

Questo importante lavoro ha consentito, anche quest'anno, alla comunità dei certificati CFPS/CFPP Sogei di essere sempre allineata rispetto alle evoluzioni delle metodologie sul mercato e di poter fornire il proprio contributo alle dinamiche decisionali che le determinano.

In particolare nell'ultimo anno sono state definite le strategie di utilizzo degli *output* di alcune delle sperimentazioni avviate negli anni precedenti, quali quella a SNAP e ai SFP. La definizione di queste strategie ha portato in specifici contesti ad una vera e propria applicazione industriale, ed infatti grazie alla definizione di una modalità "rapida" per la misura del non funzionale basata su SNAP si potrà procedere, ad esempio, ad un *assessment* ampio e relativamente poco costoso di questa parte della misura dei prodotti *software*.

La novità degli ultimi mesi dell'anno è il ruolo di Sogei come *Chair* del "*Non-Functional Sizing Standards Committe*" e ciò garantisce un livello di presidio molto alto sulle metodologie di misure del non funzionale. La possibilità di partecipazione alla *governance* delle evoluzioni della metodologia è particolarmente importante in un momento in cui si sta introducendo una modalità di misura del non funzionale in diversi contesti contrattuali e in cui l'interesse verso la misura della qualità è, in generale, molto sentito sia per la PA che nei rapporti con i fornitori.

Il centro di competenza interna ha continuato ad erogare in maniera autonoma i corsi per la preparazione della certificazione CFPS/CFPP con l'obiettivo di mantenere alto il numero di certificazioni e di diffondere la cultura della misurazione in modo capillare in azienda, assicurando l'aumento della qualità dei conteggi e del livello di presidio delle attività esternalizzate.

La nuova versione dello strumento aziendale per la misura del *software* ha permesso l'utilizzo parallelo dei FP e dei SFP. È stato inoltre avviato il lavoro di integrazione di tutte le basi di dati contenenti dati di misurazione verso questo nuovo prodotto.

## 6.6 GOVERNO DELL'OFFERTA

### 6.6.1 CATALOGO SERVIZI

È lo strumento di supporto ai processi aziendali che censisce i Servizi erogati per la PA corredandoli di informazioni e attributi che ne caratterizzano gli aspetti tecnici, funzionali e di sicurezza.

Nell'anno, il Catalogo è stato oggetto di particolare interesse da parte di alcuni progetti strategici dell'area *Security Governace & Data Protection*. Alle normali attività di assistenza applicativa, supporto metodologico alla modellazione e formazione interna su specifici ambiti d'interesse, nonché alle tipiche iniziative di recupero e di bonifica dei dati, l'intero periodo è stato caratterizzato da sviluppi che hanno aggiunto importanti funzionalità allo strumento:

- **GDPR:** sono stati ulteriormente personalizzati i documenti di Misure di Sicurezza e Privacy del Servizio ICT in base al Cliente Titolare del Trattamento; è stato migliorato il criterio di calcolo del Rischio Residuo; è stata aggiornata la versione dell'anagrafica delle Misure di sicurezza FOURSec;
- **BIA:** nell'ambito della Business Impact Analysis (BIA) è stato migliorato il criterio di calcolo dell'indice di *Recovery Time Objective* (RTO) applicato a ciascun Servizio ICT, rendendo il suo valore automatico anziché discrezionale.

I Servizi ICT sono stati arricchiti con le informazioni sulla loro componente infrastrutturale, proveniente dal *Configuration Management Data Base* (CMDB);

È infine stata potenziata la federazione con il CMDB, riprogettando le interfacce di interscambio per migliorare la qualità e la completezza dei contenuti informativi trasmessi.

Nell'ottica di un continuo controllo e presidio dei contenuti, nel corso dell'anno è stata avviata una attività di *assessment* dei Servizi Tecnici finalizzata a razionalizzare l'intera anagrafica.

## 6.7 PARTECIPAZIONE ED ASSOCIAZIONI

L'adesione alle associazioni consente all'Azienda e ai propri dipendenti di usufruire dei servizi resi dalle stesse, in termini di pubblicazioni, aggiornamenti e approfondimenti sulla normativa, seminari formativi e informativi, collaborazioni e confronti necessari e strumentali allo svolgimento della propria attività istituzionale.

Le finalità principali di individuazione delle associazioni di interesse si possono così sintetizzare:

- promuovere lo scambio di informazioni e l'aggiornamento rispetto a nuovi trend tecnologici e gestionali;

- garantire l'aggiornamento professionale in ambito tecnologico e gestionale al fine di ottimizzare i processi di supporto al Cliente e all'Azienda;
- focalizzare l'attenzione su ambiti particolarmente sensibili (parità di genere, sostenibilità etico-sociale, sicurezza, privacy etc.).

L'adesione alle associazioni segue *“Linee guida e criteri di approvazione delle adesioni alle Associazioni, Enti, Fondazioni e Comitati”* che prevedono un processo di raccolta fabbisogni e approvazione qualora siano verificati i seguenti criteri per la valutazione dell'esigenza:

- **INERENZA** - Le finalità dell'associazione e i benefici conseguibili devono essere pertinenti rispetto alle attività e servizi erogati da Sogei verso i Clienti istituzionali e per le proprie esigenze di funzionamento aziendale.
- **INTERESSE** - L'adesione ad una associazione deve soddisfare una concreta necessità di appartenenza ad un contesto «associativo».
- **NECESSITÀ PROFESSIONALE** - Per garantire lo sviluppo e l'aggiornamento professionale del personale dipendente nonché per il mantenimento/rinnovo di eventuali certificazioni professionali acquisite.
- **SPECIFICITÀ** - Da intendere in termini di verifica e valutazione delle peculiari (o “originali”) “caratteristiche/competenze o comunque di altri elementi distintivi dell'Associazione cui si intende aderire e che motivano la “scelta” della stessa in alternativa ad altre eventualmente attive nel medesimo contesto. Nei casi eventuali in cui non vi sia stata una preliminare verifica/attestazione del requisito di «specificità», l'individuazione del soggetto beneficiario del contributo di adesione (quota associativa) può avvenire previa valutazione comparativa dei soggetti interessati che, a seguito di avviso pubblico con indicazione dei criteri di ricerca e valutazione, abbiano manifestato interesse a presentare la propria candidatura.
- **RAPPORTO COSTI/BENEFICI** - La spesa per il pagamento della quota associativa deve essere proporzionale ai benefici ottenuti anche considerando il costo da sostenere per l'acquisto dei servizi resi nel caso di mancata partecipazione all'associazione.

Nel 2021 Sogei ha aderito alle seguenti associazioni:

Ambito	Associazione
ICT	ASSOCIAZIONE ITALIANA PER L'INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) DAMA ITALY CHAPTER GALILEO SERVICES GUFPI-ISMA IFPUG ISACA INTERNATIONAL PROMETEIA S.P.A



Ambito	Associazione
	RTCM UNINFO XBRL ITALIA
<b>Corporate e Governance</b>	ASSIDIM ANDAF ANRA AODV 231 - ASSOCIAZIONE DEI COMPONENTI DEGLI ORGANISMI DI VIGILANZA ASSOCIAZIONE ITALIANA INTERNAL AUDITORS ASSONIME ASSOCIAZIONE FRA LE SOCIETA' ITALIANE PER AZIONI ASTRID SERVIZI S.R.L. CSR MANAGER NETWORK UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE DI ROMA
<b>Personale</b>	AIF ASSOCIAZIONE ITALIA FORMATORI ASSOCIAZIONE ITALIANA PER LA DIREZIONE DEL PERSONALE FERPI - FEDERAZIONE RELAZIONI PUBBLICHE ITALIANA HRC INTERNATIONAL ACADEMY ICF ITALIA INTERNATIONAL COACH FEDERATION ISTITUTO ITALIANO DI PROJECT MANAGEMENT VALORE D
<b>Sicurezza</b>	AIIC - Associazione Italiana Esperti in Infrastrutture Critiche A.I.P.S.A. - ASSOCIAZIONE ITALIANA PROFESSIONISTI SECURITY CLUSIT - ASSOCIAZIONE PER LA SICUREZZA INFORMATICA ECSO - EUROPEAN CYBER SECURITY ORGANIZATION ISFA ITALIAN CHAPTER

