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

GRI 103-1
GRI 103-2
GRI 103-3

I 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 **Gestori PEC** (V 1.0 del 18 novembre 2009)	Vigilanza sui Gestori PEC	Si verifica esterna – AgID a richiesta sorveglianza semestrale - audit interni

Norma di riferimento	Ambito	Certificazione
Lista di riscontro per le attività di vigilanza e certificazione di conformità (Vers.1 del 14 aprile 2017) per **Conservazione digitale**	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

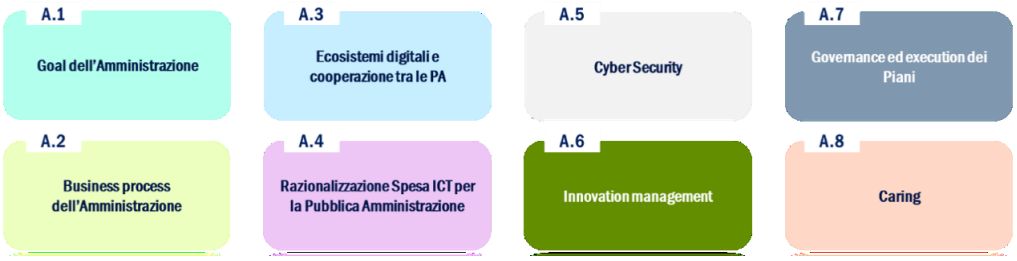
L'ascolto della voce del cliente-utente è di fondamentale importanza per l'individuazione degli interventi necessari non solo per l'evoluzione dei servizi offerti, ma anche per perseguire il miglioramento organizzativo e gestionale.

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

GRI 103-1
GRI 103-2
GRI 103-3
SDP-5

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.E' 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)

GRI 418-1
SDP-2
SDP-3
SDP-6
SDP-9

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)[1], 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

[1] *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*

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

SDP-1
SDP-4
SDP-10

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 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 coso 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 confermato 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 sevizi 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

SDP-7

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

SDP-8

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;
- *assessement* 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

GRI 102-2
GRI 103-1
GRI 103-2
GRI 103-3

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

GRI 102-13

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 RTCM UNINFO XBRL ITALIA
Corporate e *Governance*	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
Personale	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
Sicurezza	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

GRI 103-1
GRI 103-2
GRI 103-3

7. CAPITALE FINANZIARIO

Le risorse economico-finanziarie connesse all'attività di Sogei vengono utilizzate a supporto del business dei clienti garantendo annualmente un bilancio solido con posizioni robuste di capitale e liquidità in crescita che assicura, da un lato, stabilità economica e finanziaria nel medio-lungo termine e, dall'altro, la remunerazione dell'azionista, dei dipendenti e della collettività.

GRI 102-7
GRI 201-1

7.1 ANALISI DEI RISULTATI REDDITUALI

L'analisi dei risultati reddituali è di seguito commentata con il supporto del prospetto di Conto economico e delle relative tavole di sintesi, riclassificati in ottica gestionale.

valori espressi in migliaia di euro

	Bilancio 2021	Bilancio 2020	Variazione	Percentuale variazione
Ricavi delle vendite e delle prestazioni	720.999	625.665	95.334	15,2%
Variazione dei lavori in corso su ordinazione	1.473	2.530	(1.057)	-41,8%
Valore della produzione	**722.472**	**628.195**	**94.277**	**15,0%**
Consumi di materie e servizi	(416.527)	(379.148)	(37.379)	9,8%
Valore aggiunto	**305.945**	**249.047**	**56.898**	**22,8%**
Costo del lavoro	(170.993)	(161.512)	(9.421)	5,8%
Margine operativo lordo normalizzato (*)	**134.952**	**87.535**	**47.556**	**54,2%**
Ammortamenti e svalutazioni delle immobilizzazioni	(49.299)	(42.628)	(6.666)	15,6%
Accantonamenti per rischi ed oneri	(1.973)	(7.341)	5.371	-73.,1%
Proventi ed oneri diversi	(496)	(146)	(400)	139,7%
Risultato operativo	**83.183**	**37.419**	**45.764**	**122,3%**
Proventi netti da partecipazioni	400	185	215	116,2%
Saldo proventi ed oneri finanziari	(255)	(259)	4	1,5%
Risultato prima delle imposte	**83.328**	**37.345**	**45.983**	**123,1%**
Imposte	(24.021)	(10.387)	(13.634)	131,3%
Utile del periodo	**59.307**	**26.959**	**32.348**	**120,0%**

(*) *Per effetto della riclassificazione effettuata nel Bilancio 2020, della componente relativa all'attuazione del progetto "Valore Generazionale", dal costo del lavoro agli accantonamenti per rischi e oneri*

L'esercizio 2021 mostra un andamento particolarmente positivo che vede fortemente incrementati oltre che il volume dei ricavi, tutti gli indicatori gestionali e l'utile netto; tali risultati attestano l'incisiva politica di ottimizzazione ed efficientamento posta in essere dalla Società in