Pubblico

Revisione	1
Autore	Erica Spina
Approvata da	Andrea Ferlin
Data	04/01/2021

Indice delle Revisioni

Motivo della revisione	Data	Revisore
Aggiunta dell'ambito di certificazione	03.09.2021	ES

Sommario

1. Scopo

Il documento ha lo scopo di informare il personale in merito ai contenuti delle politiche di sicurezza delle informazioni di Professional Link S.r.l. (di seguito "PLINK" o "Organizzazione"), corredate da cenni su processi e particolari misure di sicurezza adottate.

PLINK è operatore di telecomunicazioni titolare di licenza nazionale per fornitura del servizio telefonico al pubblico e dei servizi di comunicazione dati e cloud attraverso una propria infrastruttura distribuita su alcuni nodi principali del territorio nazionale.

Grazie all'infrastruttura telematica proprietaria, PLINK è in grado di fornire numerazioni geografiche in tutti i distretti italiani e di eseguire portabilità da tutti gli operatori interconnessi.
Per PLINK la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, logica e organizzativa.

Il Sistema di Gestione per la Sicurezza delle Informazioni è fondato sul rispetto di:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti debitamente autorizzati nell'ambito dei processi gestiti;
2. **Integrità**: salvaguardare contenuti e consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. **Controllo**: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Privacy**: garantire la protezione e il controllo dei dati personali e del loro trattamento.

2. Destinatari

La presente procedura si rivolge a tutti i dipendenti di PLINK (destinatari INTERNI), oltre ai soggetti esterni che a qualunque titolo collaborano ed esercitano attività in favore di PLINK, tra cui, a titolo esemplificativo e non esaustivo, consulenti, partner, RSPP (destinatari ESTERNI).

3. Contesto dell'organizzazione

PLINK ha determinato i fattori esterni e interni pertinenti agli obiettivi che si è prefissata e che possono influenzare la sua capacità di conseguire gli esiti previsti per il proprio sistema di gestione per la sicurezza delle informazioni.

3.1 Scopo del Sistema di Gestione della Sicurezza delle Informazioni

L'oggetto di certificazione è il seguente: "*progettazione, gestione e manutenzione di servizi di telecomunicazione e di information technology*".
Il campo di applicazione della presente Politica si applica a tutti i requisiti richiesti della norma e Professional Link S.r.l. assicura la capacità per garantire la sicurezza delle informazioni.

3.2 Interdipendenze nell'organizzazione

La seguente tabella riporta lo schema dei processi e la loro interazione:

Processo	Primario o di Supporto	Interno o Esterno	Interagisce con
Commerciale	P	I/E	Provisioning / Tecnico / Assurance/ Cliente
Delivery - Provisioning	P	I/E	Commerciale / Tecnico / Cliente
Tecnico	P	I	Commerciale / Provisioning / Assurance
Assurance	P	I/E	Tecnico / Provisioning /Cliente
Acquisto	S	E	Amministrazione
Human Resources	S	I	Tutti/ Consulenti esterni
Amministrazione	S	I/E	Tutti/ Commercialista
Gestione Sistema Qualità	S	I	Tutti/ Ente di certificazione
Gestione Sistema Sicurezza delle Informazioni	S	I	Tutti/Ente di certificazione

3.3 Comprensione del contesto

PLINK definisce, e periodicamente rivaluta, il contesto in cui opera, i soggetti coinvolti, le opportunità e i possibili rischi impattanti sul proprio Sistema di Gestione per la Sicurezza delle Informazioni.
PLINK ha monitorato le parti interessate rilevanti per il Sistema di Gestione per la Sicurezza delle Informazioni e dei requisiti ad esse applicabili. In particolare:

- Contesto Interno: riguarda le persone che sono direttamente coinvolte nella gestione dei processi aziendali. Sono valutate sia le competenze sia le performance che devono essere elevate (garantite dai controlli previsti e monitorate nella valutazione degli indicatori). Altresì, vengono valutati il know how aziendale frutto di un'esperienza pluriennale e consolidata nel settore delle telecomunicazioni e la comunicazione interna e con tutte le parti interessate, che deve essere efficace e continua.
    - Le Persone: estrema attenzione è dedicata alle persone che operano all'interno dell'azienda, in un ambiente accogliente, mettendo a disposizione attrezzature adeguate e moderne. Il tutto perfettamente in linea con la legislazione riguardante la sicurezza sul lavoro che prevede anche, corsi specifici di aggiornamento e visite mediche periodiche.
    - La conoscenza: conoscenza e competenza nelle attività sono costantemente mantenute attive dalla programmazione di formazione e addestramento durante l'anno. Costanti e sistematici training on the job sono eseguiti direttamente per tutte le attività svolte. Considerata la varietà di tipologie di clienti su cui si opera, l'operatore viene sistematicamente istruito in base alle modalità operative richieste dal Committente, compresi gli aspetti cogenti.
    - La tecnologia e le prestazioni: il sistema gestionale è in grado di rispondere a tutte le esigenze sia gestionali che a quelle relative alle specifiche tecniche richieste dai Clienti.
    - Gli aspetti legali: La necessità di adeguarsi alle norme cogenti è considerato un elemento qualificante nei confronti del Cliente e di distinzione nei confronti del mercato.

Altri fattori interni sono da prendere in considerazione per una efficace gestione dei processi, poiché possono comunque andare ad influenzare la gestione della Sicurezza delle informazioni, tra cui per esempio, le

eventuali rimostranze dei Clienti per il mancato rispetto delle specifiche tecniche richieste per un certo servizio o eventuali errori non intenzionali degli operatori, per i quali PLINK si è dotata di una procedura per una gestione puntuale ed accurata.

- Contesto Esterno: riguarda le persone coinvolte nella gestione dei processi aziendali indirettamente, quali clienti, fornitori, operatori.

    - I Clienti principali sono aziende operative nei settori più svariati e vanno dalle piccole strutture alle grandi aziende le cui aspettative sono andate in crescendo nel tempo. Le aspettative degli stessi sono sempre tendenti al miglior risultato possibile. Per quanto riguarda il servizio deve essere necessariamente coerente con le aspettative contrattualizzate ed anche con i livelli target definiti dal mercato. Vista l'attenzione mostrata nei confronti del Cliente, la Società pone risalto alla scarsità dei reclami ricevuti. Nuove potenziali esigenze del cliente sono oggetto di esplorazione, rappresentano la possibilità di dare continuità, sviluppo e innovazione all'attività. Si stanno sviluppando altri settori in campi affini o contigui che rappresentano opportunità positive di diversificazione e di ampliamento della gamma dei servizi offerti.

    - I collaboratori, inteso come tutte le risorse umane che concorrono alla erogazione del servizio offerto e che devono rispettare le prescrizioni previste dalla normativa vigente in tutti gli ambiti. Sono tenuti molto in considerazione.

    - I fornitori garantiscono all'azienda il rispetto dei requisiti contrattualmente previsti in termini di conformità dei prodotti e dei servizi offerti. L'impostazione aziendale è comunque improntata ad un loro pagamento puntuale e molti degli stessi sono diventati storici nel tempo.

    - Aspetto tecnologico: stante la tipologia dei servizi gestiti vi è un continuo aggiornamento normativo in materia. Sono effettuati, inoltre, controlli dell'operatività dei servizi e del corretto utilizzo dei prodotti definiti e l'eventuale e opportuno aggiornamento.

4. Leadership e ruoli e responsabilità

La Direzione, periodicamente, definisce e rivalida gli obiettivi del Sistema di Gestione della Sicurezza delle Informazioni con le strategie operative di PLINK.
Inoltre, comunica a tutte le risorse necessarie, per la corretta applicazione del Sistema di Gestione di Sicurezza delle Informazioni, l'importanza del miglioramento continuo, fornendo guida e sostegno a tutto il personale.
Sarà compito della Direzione:

1. attuare, sostenere e verificare periodicamente la presente Politica, a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa e sempre a tutte le parti interessate;
2. garantire le risorse necessarie per l'efficace protezione delle informazioni;
3. definire gli obiettivi in materia di sicurezza delle informazioni;
4. riesaminare periodicamente gli obiettivi e la Politica per la sicurezza delle informazioni per accertarne la continua idoneità, soprattutto con riferimento alle evoluzioni significative del business,

alle eventuali nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio e al verificarsi di significativi incidenti di sicurezza, oltre che all'evoluzione del contesto normativo o legislativo.

Le responsabilità relative alla sicurezza delle informazioni vengono completamente definite e assegnate, al fine di:

- migliorare la conoscenza aziendale sulle "best-practices" e mantenere l'aggiornamento in tema di sicurezza delle informazioni;
- assicurarsi che la comprensione delle tematiche di sicurezza delle informazioni in azienda sia aggiornata e completa;
- ricevere tempestivamente informazioni (alert, avvisi, patch da applicare) in merito a vulnerabilità, possibili attacchi e contromisure da applicare;
- I nuovi servizi informatici vengono valutati dal punto di vista della sicurezza delle informazioni dalle funzioni di sicurezza sin dalle prime fasi di sviluppo (Privacy by Design);
- Il rispetto dei requisiti di sicurezza nel software viene periodicamente verificato.

Ruoli e responsabilità vengono indicati e definiti con organigramma e mansionario. Al fine di impedire o quanto meno ridurre le possibilità di uso improprio, distruzione e/o modifica accidentale o non autorizzata delle informazioni, vengono correttamente tenute separate le aree di responsabilità, che possono trovarsi in conflitto tra loro.

Il solo Legale Rappresentante, in via diretta o per il tramite di collaboratori esterni o interni, a seconda della comunicazione da effettuare, è tenuto a mantenere rapporti appropriati con le Autorità preposte, tra cui AGCOM, mise, Autorità Garante per la Protezione dei Dati Personali, Ispettorato del Lavoro.

5. Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli

PLINK riconosce che tutte le informazioni e tutti i sistemi attraverso cui le stesse transitano o sono elaborate, conservate o trasmesse, devono essere soggette ad un'attenta e controllata gestione, finalizzata ad innalzarne e mantenerne i livelli di sicurezza allineati agli standard internazionali, oltre che alla normativa europea e nazionale.
Gli obiettivi che giustificano l'adozione di un Sistema di Gestione della Sicurezza delle Informazioni sono molteplici e sono:

- **Diffusione della cultura per la Sicurezza delle informazioni**; la principale linea di difesa, per assicurare il conseguimento di tale obiettivo, è rappresentata dal fattore umano, e quindi dal personale di PLINK. La difesa in questione si fonda sulla sensibilità e sulla formazione in tal senso dei singoli.
- **Prevenzione degli incidenti**; obiettivo strettamente connesso al precedente, la prevenzione permette di scongiurare il verificarsi di eventi indesiderati che potrebbero causare danni economici, di immagine e legali. Vengono, a tal proposito previste misure adeguate e preventive al fine di scongiurare il verificarsi di detti eventi, o quanto meno di mitigare il rischio del loro verificarsi.

- **Contenimento delle conseguenze degli incidenti e garanzia della continuità operativa**; in aggiunta alla prevenzione, la strategia per poter minimizzare i rischi del verificarsi di eventi dannosi o potenzialmente dannosi, è la risposta immediata ad un incidente. Per questo è stata predisposta una procedura di gestione degli incidenti della sicurezza delle informazioni, così da rendere edotti tutto il personale di PLINK sulle modalità da seguire in caso di incidente.
- **Soddisfazione dei requisiti di business e contrattuali**; tutte le informazioni di origine contrattuale hanno un'importanza strategica per il business, conseguentemente, particolare attenzione deve essere prestata a quegli aspetti di sicurezza delle informazioni che possano influenzare l'immagine aziendale. L'accesso di terze parte ai sistemi informativi aziendali deve essere controllato e stabilito da un apposito regolamento, allo scopo di mantenere un adeguato livello di sicurezza delle informazioni.
- **Soddisfazione dei requisiti cogenti e regolatori**; tutti i requisiti di sicurezza delle informazioni che hanno origine dall'ambito regolatorio cogente o che ne derivano, ricoprono particolare importanza.

6. Pianificazione

PLINK pianifica e implementa il Sistema di Gestione della Sicurezza delle Informazioni in modo coerente con il conseguimento degli obiettivi fissati e con la possibilità di apportare e garantire il rispetto dei requisiti RID.
L'intero Sistema di Gestione della Sicurezza delle Informazioni, essendo uno strumento dinamico, capace di recepire ogni eventuale elemento di miglioramento salvaguardando la conformità alle norme di riferimento.

6.1 Gestione dei cambiamenti

Qualora emerga la necessità di effettuare modifiche al SGSI, le modifiche sono condotte in modo pianificato e sistematico. Sono presi in considerazione:

- lo scopo delle modifiche e tutti i relativi effetti potenziali;
- la necessità di conservare l'integrità del SGQ;
- la disponibilità di risorse;
- la distribuzione o ridistribuzione delle responsabilità ed autorità.

6.2 Azioni per affrontare rischi e opportunità

PLINK ha svolto un'analisi dei rischi sulle attività svolte, coinvolgenti particolari informazioni aziendali e dati personali, utilizzando una metodologia basata sulla ISO 31000.
In merito alla metodologia adottata e alla procedura applicata, si faccia riferimento alla Procedura di Risk Assessment.

7. Supporti per la gestione del SGSI

7.1 Risorse

PLINK ha determinato e introdotto le risorse necessarie per stabilire, attuare e mantenere il sistema di gestione della sicurezza delle informazioni e per migliorarne continuamente l'efficacia.
In particolare, sono state considerate:

- l'esistenza interna di opportune risorse;
- la necessità di acquisire risorse esterne.

7.1.1 Risorse Umane

Al fine di assicurare il rispetto dei requisiti del cliente e delle norme, leggi e regolamenti cogenti, PLINK si avvale di persone volte a condurre tutte le attività.
La Direzione ha l'onere di valutare la necessità e l'adeguatezza, oltre ad assicurare per tempo la disponibilità:

- di personale addestrato, di adeguata capacità e preparazione per la direzione, esecuzione e verifica delle attività lavorative;
- di personale addestrato e di adeguata capacità per l'esecuzione degli audit interni della qualità.

7.1.2 Infrastrutture

PLINK ha determinato, rese disponibili e tenute in efficienza, le infrastrutture che concorrono a determinare la conformità dei prodotti e servizi quali:

- edifici;
- attrezzature Hardware;
- sistemi Software e apparecchiature di misurazione e di controllo;
- tecnologia per l'informazione e per la comunicazione.

7.1.3 Ambienti di lavoro

PLINK dispone di un ambiente di lavoro adeguato alle esigenze del personale e delle attività che vengono svolte, mantiene inoltre una costante attenzione a tutti i fattori legati alla sicurezza, alla salute e all'igiene (compresi i fattori fisici, ambientali ed altri fattori quali rumore, temperatura, umidità, illuminazione o condizioni atmosferiche) osservando scrupolosamente le disposizioni legislative in merito.

7.1.4 Risorse per il monitoraggio e la misura

Quando il monitoraggio e la misura sono usati per dare evidenza della conformità dei prodotti e dei servizi ai relativi requisiti, sono determinate le risorse necessarie per assicurare risultati validi e affidabili. È opportuno che le risorse messe in campo:

- siano appropriate per il tipo di misura e di monitoraggio da svolgere;
- siano tenute sotto controllo al fine di assicurare la loro continua efficienza in relazione allo scopo da conseguire.

PLINK ha allestito al suo interno un sistema di monitoraggio volto a mantenere l'efficienza non solo dei propri sistemi interni, ma anche delle infrastrutture adottate per assicurare la buona erogazione del servizio ai clienti.

7.1.5 Conoscenza (Know How) aziendale

Sono determinate le conoscenze necessarie per conseguire la conformità dei servizi. Le conoscenze sono conservate e rese disponibili nella misura in cui sono utili.
In previsione di miglioramenti, PLINK considera le conoscenze esistenti e determina il modo di sviluppare tali

conoscenze.
Per acquisire competenze supplementari, si agisce sulle risorse interne attraverso:

- l'analisi dei punti di debolezza e dei punti di forza;
- la ricerca di documenti, testi, evidenze relativi alle conoscenze richieste;
- la conservazione e la valorizzazione delle esperienze efficaci realizzate;

e sulle risorse esterne attraverso:

- reperimento di standard, norme, linee guida, best pratics, etc…;
- la partecipazione a conferenze, convegni, congressi, seminari;
- il reperimento e la consultazione di stampa specializzata;
- l'istituzione di una rete di condivisione di dati con clienti e fornitori;
- l'attivazione di consulenze.

7.2 Competenze

PLINK determina la competenza necessaria per il personale che svolge attività che influenzano la qualità del servizio fornito.
Assicura che tale personale sia competente sulla base di un'appropriata formazione ed esperienza.
Ove applicabile, fornisce addestramento o intraprende altre azioni per acquisire le necessarie competenze e valuta l'efficacia delle azioni realizzate. PLINK ha organizzato una tabella a matrice in cui, per ogni ruolo dell'organigramma, è possibile avere evidenza delle competenze acquisite.

7.3 Consapevolezza

Tutto il personale di PLINK deve avere adeguata formazione relativa a temi specifici del SGSI che si può riassumere in:

- formazione di base;
- formazione ed implementazione operativa (processi e procedure).

Le attività di addestramento del personale sono registrate e costituiscono il riferimento per le attività di monitoraggio del coinvolgimento e della crescita professionale del personale.

7.4 Comunicazione

L'Azienda ha determinato quali comunicazioni, interne ed esterne, siano rilevanti ai fini della gestione del SGSI. È definito:

- cosa è necessario comunicare;
- quando comunicare;
- il destinatario della comunicazione;
- come comunicare, (il mezzo di comunicazione).

Un corretto flusso di informazioni tra i dipendenti è indispensabile perché non si verifichino malintesi, intempestività ed errori.
Campo di applicazione: tutte le attività di comunicazione con le parti interessate.
Le attività seguono questi criteri:
Comunicazione interna: dal basso verso l'alto e viceversa.

La comunicazione dal basso comprende la gestione dei rilievi, osservazioni, proposte provenienti dal personale di PLINK**.** La comunicazione dal basso avviene sempre in modo verbale solo le eventuali risposte e/o provvedimenti (quando ritenuto importante e/o opportuno) sono redatti in forma scritta o via e-mail.
La comunicazione dall'alto avviene per mezzo di:

- comunicati interni diffusi agli interessati (via e-mail);
- riunioni generali;
- incontri singoli su argomenti specifici;
- avvisi nella intranet aziendale.

Comunicazione esterna: importante è la gestione della comunicazione esterna.
PLINK si avvale di molti strumenti per poter rendere edotti i soggetti terzi di attività o per dare comunicazioni varie:

- Otrs, sistema di ticketing che permette di fornire riscontro all'interessato. Il sistema è composto da diverse code dedicate a ciascuna area e distinte per competenze, il personale risponderà per la propria competenza (il sistema è meglio descritto nella procedura di gestione degli asset);
- E-mail, strumento principalmente utilizzato ai fini della comunicazione;
- Portali di operatori fornitori.

8. Contatti con le autorità

PLINK mantiene appropriati contatti con le autorità pertinenti.
La Direzione identifica le autorità con le quali essere in contatto a supporto della attività svolta.
A titolo esemplificativo, sono individuate quali Autorità pertinenti:
- Garante Privacy in caso di Data Breach in merito a incidenti che coinvolgono la protezione dei dati personali;
- Autorità Regionali;
- AGCOM;
- MISE;
- Polizia Postale;
- Agid

9. Contatti con gruppi specialistici

Per quanto riguarda i contatti con gruppi specialistici, il Legale Rappresentante e i referenti dei reparti specialistici sono iscritti a newsletter relative a temi specifici dell'erogazione del servizio e delle novità normative.
Sulla base del contenuto delle informazioni delle varie newsletter i suddetti responsabili provvedono a smistarle alle competenze interessate.

10. Informazioni documentate

Nel SGSI sono incluse:

- le informazioni documentate richieste dalla Norma ISO 27001;
- le informazioni documentate che PLINK ritiene necessarie per l'efficacia del SGSI.

Le informazioni documentate sono identificate attraverso:

- il titolo;

- la data di emissione/aggiornamento;
- i riferimenti alle persone che hanno concorso all'emissione/aggiornamento.

Le informazioni documentate sono definite in termini di:

- supporto (ogni qualvolta ciò sia possibile è preferito il supporto elettronico piuttosto che cartaceo);
- lingua (è utilizzata, di regola, la lingua italiana, ad eccezione delle comunicazioni con i clienti/fornitori esteri, nel qual caso è utilizzata prevalentemente la lingua inglese);
- responsabilità di redazione, verifica e approvazione.

Le informazioni documentate sono:

- rese disponibili nella intranet aziendale per il personale di PLINK. Solo per quei documenti per i quali ne è prevista la conoscenza da parte di terzi esterni all'organizzazione è prevista la diffusione;
- protette da usi impropri, perdita di integrità e/o delle caratteristiche di riservatezza (Backup, cartelle con accessi profilati, antivirus, firewall).

Le informazioni documentate di origine esterna, emesse dai clienti, dai fornitori e dagli enti normativi nazionali ed internazionali, sono identificate e tenute sotto controllo.

Per quanto riguarda i dati e le informazioni nel sistema informativo aziendale si osservano le seguenti prescrizioni:

- back up come da relativa procedura interna.

PLINK, quando applicabile, tiene sotto controllo le informazioni documentate e le registrazioni della qualità attraverso prescrizioni per:

- la distribuzione, l'accesso, l'uso ed il ritiro;
- la conservazione, la protezione, la leggibilità;
- la gestione delle modifiche;
- l'archiviazione e/o la distruzione dei documenti.

11. Riesame

La Direzione riesamina il Sistema di Gestione della Sicurezza delle Informazioni ad intervalli pianificati, al fine di assicurarne la continua adeguatezza ed efficacia.

I Riesami sono pianificati e condotti considerando:

- lo stato delle azioni impostate nel riesame precedente;
- i cambiamenti interni ed esterni che siano rilevanti, incluse le decisioni strategiche aziendali;
- le informazioni in merito alle prestazioni del SGSI:
  - le non conformità e le azioni correttive;
  - i risultati dei monitoraggi e delle misure;
  - i risultati degli Audit;
  - l'adeguatezza delle risorse dedicate al mantenimento di un efficace SGSI;

- l'efficacia delle azioni intraprese per evidenziare e trattare i rischi e le opportunità;
- nuove opportunità di miglioramento.

Risultati dei Riesami

Gli output dei riesami includono decisioni ed azioni relative a:

- opportunità di miglioramento continuo;
- ogni necessità di modifica del SGSI.

Sono conservate informazioni documentate, a evidenza dei risultati dei Riesami.

12. Miglioramento

PLINK verifica periodicamente, una volta l'anno o in concomitanza di cambiamenti significativi, l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.

Il riesame permette di verificare lo stato delle azioni correttive e l'aderenza agli obiettivi esposti nella presente policy. Il risultato del riesame include tutte le decisioni ed azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni, dei controlli, nell'allocazione di risorse e responsabilità.

Per apportare miglioramenti, si farà riferimento a:

- Risultanze di Audit interni ed esterni;
- Modifiche che potrebbero avere effetti sul sistema di gestione della sicurezza delle informazioni;
- Attuazione delle azioni correttive e preventive, comprese le verifiche di efficacia;
- Sopraggiungere di particolari esigenze.

13 Miglioramento continuo

PLINK intende far crescere continuamente la coerenza, l'adeguatezza e l'efficacia del SGSI.
Sono considerati tutti i risultati delle analisi e delle valutazioni, nonché gli elementi di uscita del Riesame della Direzione, per identificare aree di prestazioni migliorabili e opportunità di miglioramento continuo.
Quando applicabile, si utilizzano strumenti, tecniche e metodologie, per investigare le cause delle non conformità, e sostenere il miglioramento continuo.