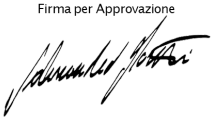
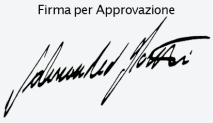
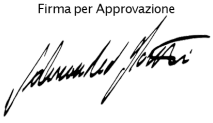
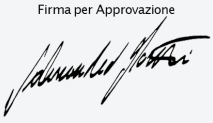
CLASSIFICAZIONE DOCUMENTO: USO INTERNO

MERIDIAN GROUP

Manuale del sistema di gestione integrato

UNI EN ISO 9001 :2015 - UNI/PdR 125 :2022 - ISO/IEC 27001 :2022 - ISO/IEC 27017 :2015 - ISO/IEC 27018 :2019 - ISO/IEC 42001:2023, UNI EN ISO 45001:2023, UNI EN ISO 14001:2015 e PAS 24000 :2022

Versione	Data	Redatto da	Approvato da	Descrizione
1.0	1/04/2026	Flavia Testa, Giulia Moretti	Alessandro Moretti Firma per Approvazione 	Prima emissione
2.0	4/06/2026	Flavia Testa, Giulia Moretti	Alessandro Moretti Firma per Approvazione 	Aggiornamento campo di applicazione ISO 27001
3.0	1/09/2026	Flavia Testa, Giulia Moretti	Alessandro Moretti Firma per Approvazione 	Aggiornamento ISO 45001
4.0	10/11/2026	Flavia Testa, Giulia Moretti	Alessandro Moretti Firma per Approvazione 	Integrazione ISO 14001 e PAS 24000

Sommario

1 L'azienda e il contesto di riferimento 3
2 L'organizzazione e la struttura operativa 3
2.1 Mansionario del sistema di Gestione Sociale 4
3 Principali servizi 6
4 Modello Commerciale su canale 7
5 Il Sistema di Gestione 7
6 Perimetro del Sistema integrato e standard applicabili 8
7 La Politica per la qualità, la SSL, l'ambiente e la Responsabilità Sociale 11
8 La Politica di Parità di Genere 13
9 La Politica per la sicurezza delle informazioni 14
9.1 La sicurezza dei servizi cloud e la protezione delle pii 14
9.2 La politica ai e il sistema di gestione per l'intelligenza artificiale 14
10 Le parti interessate 15
11 Fattori interni ed esterni 18
12 Il risk based approach 19
13 Il miglioramento continuo 21
13.1 Leadership e partecipazione 21
13.2 Misurazione delle prestazioni e miglioramento 21
13.3 Riesame della Direzione 22
14 La mappa dei processi 23
15 La gestione del cambiamento 25
16 La Comunicazione 27
17 Le Misurazioni 27
18 Documentazione di riferimento del SGI e del perimetro del sistema di gestione 28
19 Matrice sintetica standard - processi – evidenze 31

© 2024 – All Rights Reserved.

1 L'azienda e il contesto di riferimento

Meridian Group è una realtà italiana d'eccellenza nel settore della Cyber Intelligence e della Cyber Security, che offre servizi e consulenza aziendale in ambito IT ad alto valore tecnologico. La società si distingue per la capacità di fornire soluzioni avanzate e personalizzate per la prevenzione delle minacce informatiche, la protezione delle identità digitali, la formazione sulla sicurezza informatica e l'analisi del rischio cibernetico, anche attraverso modelli supportati da intelligenza artificiale.

Opera in un contesto altamente dinamico e regolamentato, influenzato da:

- un'evoluzione continua e sofisticata delle minacce cyber;
- requisiti stringenti di conformità normativa e volontaria (come ISO 9001, GDPR, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 42001, ISO 45001, ISO 14001, UNI/PdR 125 e PAS 24000);
- crescenti esigenze da parte dei clienti e delle autorità di vigilanza;
- collaborazioni strategiche con partner e fornitori ICT di rilievo.

In uno scenario globale in cui la domanda di soluzioni di Cyber Security è in costante crescita, Meridian Group si propone come un punto di riferimento per aziende e organizzazioni che cercano protezione, affidabilità e innovazione. Il settore, in rapida espansione, offre numerose opportunità per le imprese capaci di affrontare sfide complesse e mutevoli con competenza e visione strategica.

L'approccio di Meridian Group è guidato da una filosofia fondata su innovazione continua, responsabilità etica e sostenibilità delle soluzioni. Ogni progetto è concepito per trasformare le sfide digitali in opportunità concrete, attraverso strategie efficaci che garantiscano ai clienti risultati tangibili e duraturi.

2 L'organizzazione e la struttura operativa

Il Sistema di Gestione Integrato (SGI) di Meridian adotta un approccio per processi, basato sulla gestione dei rischi e sul miglioramento continuo, integrando i requisiti delle norme ISO 9001, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 42001, ISO 45001, ISO 14001, UNI/PdR 125:2022, PAS 24000 e del GDPR. Il modello operativo comprende le fasi di pianificazione, progettazione, attuazione, verifica, monitoraggio e miglioramento, secondo il ciclo Plan-Do-Check- Act (PDCA), assicurando l'integrazione dei requisiti di qualità, sicurezza delle informazioni, protezione dei dati personali, governance dell'intelligenza artificiale, salute e sicurezza sul lavoro, ambiente e parità di genere.

L'approccio è iterativo e orientato al miglioramento continuo, con attività, responsabilità e controlli definiti nelle procedure aziendali e applicati in modo proporzionato ai rischi e alle specificità dei processi. Nell'ambito dei processi tecnologici, di sviluppo software e di gestione dei sistemi di intelligenza artificiale, il modello si integra con le metodologie Agile, DevOps e Secure Software Development Life Cycle (SSDLC), assicurando che i requisiti di qualità, sicurezza, protezione dei dati, affidabilità, tracciabilità e governance dell'AI siano considerati durante l'intero ciclo di vita dei prodotti e dei servizi.

L'approccio adottato è di natura iterativa e incrementale e favorisce il coordinamento tra le diverse funzioni aziendali, evitando duplicazioni documentali e operative e garantendo una gestione unitaria dei requisiti del Sistema di Gestione Integrato.

© 2024 – All Rights Reserved.

Le attività e i controlli previsti nelle diverse fasi sono disciplinati dalle politiche, dalle procedure e dagli strumenti operativi del SGI, in funzione delle specificità dei processi e dei requisiti applicabili.

Meridian Group adotta una struttura gerarchica snella, orientata alla comunicazione aperta, alla collaborazione interfunzionale e alla rapida condivisione delle informazioni tra i team.

L'organizzazione è guidata dal Presidente e CEO che, di concerto con il Deputy CEO, definisce la visione strategica e coordina le principali linee decisionali dell'azienda. A supporto operano, tra le altre, le seguenti figure chiave come:

- il/la Chief Business & Strategy Officer, responsabile del Business e della strategia aziendale,
- il/la Chief Technology Officer (CTO), che supervisiona le attività tecnologiche, incluse la Cyber Intelligence, la Cyber Security e lo sviluppo di soluzioni basate su Intelligenza Artificiale;
- il/la Chief Intelligence Officer (CIO) per le funzioni tecniche, investigative, amministrative e di sviluppo;
- Il/la CISO, responsabile della strategia e dell'implementazione della Cybersicurezza per garantire che i sistemi, i servizi e le risorse digitali siano adeguatamente sicuri e protetti. A tal fine, definisce, mantiene e comunica la "vision", la strategia, le politiche e le procedure di Cybersicurezza e ne assicura l'attuazione in tutta l'organizzazione;
- il/la General Affairs Manager (GAM), responsabile del coordinamento delle funzioni di affari generali, risorse umane e compliance, garantendo la corretta applicazione dei processi aziendali e il supporto alla governance;
- Il/la Administration & Purchasing Manager, responsabile della gestione amministrativa e del ciclo di approvvigionamento di beni e servizi aziendali.

Il processo decisionale in Meridian è fortemente collaborativo. Le decisioni strategiche vengono condivise tra i membri del management team, valorizzando il confronto e il coinvolgimento dei responsabili di funzione attraverso brainstorming e analisi congiunte.

Per la rappresentazione grafica dell'organigramma aziendale si rimanda al documento Organigramma aziendale.

2.1 Mansionario del sistema di Gestione Sociale

Ruolo	Responsabilità nel SGS	Autorità operativa
Alta Direzione	Approva politica, perimetro e obiettivi sociali. Assegna ruoli e risorse. Conduce il riesame, valuta le prestazioni e decide sulle criticità rilevanti.	Approva il mansionario e le risorse. Decide sulle azioni di rimedio e sui casi che superano le deleghe operative
Responsabile SGS	Coordina l'attuazione della politica e verifica la conformità del SGS alla PAS 24000 e all'Allegato A. Controlla che i processi producano i risultati attesi. Coordina due diligence, consultazione dei lavoratori e formazione sui diritti umani. Verifica la disponibilità delle risorse e riferisce alla Direzione su risultati e criticità.	Richiede dati, evidenze e azioni alle funzioni. Convoca i referenti, propone risorse e porta tempestivamente alla Direzione le criticità rilevanti.
RSG – Responsabile del	Integra il SGS nei processi documentali esistenti. Coordina programma di audit, raccolta degli indicatori, registro delle	Richiede e verifica le evidenze di sistema. Coordina gli audit

© 2024 – All Rights Reserved.

Sistema di Gestione	non conformità e verifica dell'efficacia delle azioni correttive. Predispone gli elementi per il riesame.	assicurando obiettività e imparzialità.

Ruolo	Responsabilità nel SGS	Autorità operative
HR / Amministrazione del personale	Presidia selezione, verifica dell'età, contratti, orari, straordinari, riposi, retribuzioni, pari trattamento e formazione. Gestisce i rischi di lavoro minorile e forzato nelle attività di reclutamento e impiego, anche tramite eventuali agenzie. Verifica le anomalie con il consulente del lavoro e attiva le misure di competenza.	Accede alle registrazioni del personale secondo le autorizzazioni. Richiede correzioni ed effettua le segnalazioni al GAM.
Funzione acquisti / Gestione fornitori	Applica i criteri sociali nella qualifica e nel monitoraggio di fornitori e appaltatori. Valuta, con il RGS, i rischi di lavoro minorile e forzato nella filiera e segue le azioni concordate con i fornitori.	Richiede evidenze e piani correttivi. Propone la sospensione della qualifica o altre misure secondo le deleghe vigenti.
Responsabili di funzione e di servizio	Applicano i controlli sociali nelle attività di competenza. Monitorano carichi di lavoro, orari e reperibilità, ove prevista. Agevolano la partecipazione dei lavoratori e attuano le azioni assegnate.	Organizzano turni e carichi entro le deleghe. Segnalano anomalie a HR e al GAM e attivano le misure di competenza.
Datore di lavoro, RSPP e altre figure SSL	Integrano nel SGS le evidenze su rischi per la salute e sicurezza, emergenze, formazione, infortuni e quasi infortuni, secondo i rispettivi ruoli.	Esercitano le responsabilità e le autorità previste dalle rispettive attribuzioni e nomine SSL.
Gestore dei reclami sociali	Riceve e istruisce i reclami dei lavoratori e delle parti esterne. Tutela riservatezza e assenza di ritorsioni. Registra esiti e azioni di rimedio e verifica il riscontro al segnalante, ove possibile.	Accede alle informazioni strettamente necessarie. In caso di conflitto di interessi, trasmette il caso al sostituto individuato nella procedura.
Lavoratori e loro rappresentanti, ove presenti	I lavoratori applicano le misure di propria competenza, segnalano criticità e partecipano alla valutazione dei rischi e delle misure sociali. I rappresentanti raccolgono e portano proposte. L'RLS contribuisce per gli aspetti di salute e sicurezza.	Possono accedere alle informazioni pertinenti, formulare proposte e utilizzare i canali di consultazione e reclamo senza ritorsioni.

© 2024 – All Rights Reserved.

3 Principali servizi

Attività chiave

Nel nostro impegno a favorire servizi di sicurezza cibernetica e Intelligenza Artificiale di alta qualità, svolgiamo una serie di attività chiave:

- Monitoraggio e Analisi delle Minacce Cibernetiche: Utilizziamo strumenti avanzati per monitorare e analizzare le minacce cibernetiche in tempo reale, permettendo una risposta rapida ed efficace;
- Formazione sulla Sicurezza Cibernetica: Offriamo programmi di formazione completi per aiutare le aziende a comprendere e combattere efficacemente la cybercriminalità;
- Rilevazione delle minacce alimentata da intelligenza artificiale: Utilizziamo l'Intelligenza Artificiale per migliorare la rilevazione delle minacce, aumentando la velocità e l'efficacia della nostra risposta;
- Valutazione del rischio cibernetico: Identifichiamo e valutiamo le potenziali vulnerabilità di sicurezza nelle infrastrutture dei nostri clienti, sviluppando strategie di mitigazione personalizzate;
- Analisi completa delle minacce cibernetiche: Identifichiamo e priorizziamo i rischi, fornendo informazioni operative per prevenire e mitigare gli attacchi.

© 2024 – All Rights Reserved.

4 Modello Commerciale su canale



5 Il Sistema di Gestione

Per poter essere riconosciuta tra i migliori player del settore, Meridian Group non si limita a soddisfare solo i requisiti previsti dalle normative cogenti di riferimento, ma ha scelto di dotarsi di un Sistema di Gestione Integrato coerente, per il perimetro oggetto di audit, con ISO 9001:2015, ISO 45001:2023, ISO 14001:2015, UNI/PdR 125:2022, PAS 24000, ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 42001:2023, come scelta strategica per:

- migliorare costantemente le proprie prestazioni nell'erogazione dei servizi in modo controllato, efficiente e misurabile;
- aumentare la soddisfazione dei propri Clienti, attraverso un approccio orientato alla qualità, alla trasparenza e alla capacità di risposta ai requisiti espressi ed impliciti;
- affrontare in modo sistematico rischi e opportunità, derivanti dal contesto in cui opera l'organizzazione, incluse le minacce emergenti e le esigenze delle parti interessate;
- garantire la sicurezza delle informazioni, tutelando la riservatezza, l'integrità e la disponibilità dei dati trattati in tutte le attività aziendali, in particolare nei servizi ad alta intensità digitale come la Cyber Intelligence, la Cyber Security e l'analisi del rischio cibernetico;
- garantire condizioni di lavoro sicure e salubri, prevenendo lesioni e malattie correlate al lavoro, eliminando i pericoli e riducendo i rischi per la salute e sicurezza dei lavoratori, anche attraverso la loro consultazione e partecipazione;

© 2024 – All Rights Reserved.

- promuovere la cultura della sicurezza e della qualità, coinvolgendo tutto il personale in un sistema strutturato di responsabilità, monitoraggio, miglioramento continuo e gestione della conoscenza;
- dimostrare il proprio impegno verso l'innovazione, la compliance normativa e la fiducia del mercato, consolidando il proprio posizionamento competitivo nel settore ad alta criticità in cui opera;
- integrare i principi di parità di genere nei processi decisionali e nelle politiche aziendali, come fattore determinante per la sostenibilità e la competitività dell'organizzazione;
- prevenire ogni forma di discriminazione diretta e indiretta legata al genere, promuovendo un ambiente di lavoro equo, rispettoso e inclusivo;
- garantire pari opportunità di accesso, sviluppo professionale, formazione e retribuzione, attraverso strumenti e criteri oggettivi e trasparenti;
- ridurre gli impatti ambientali delle proprie attività, prevenire l'inquinamento e rispettare gli obblighi di conformità ambientali;
- migliorare le prestazioni sociali rispettando i diritti umani, promuovendo condizioni di lavoro eque e operando con etica e integrità, anche attraverso la due diligence volta a individuare, prevenire e mitigare gli impatti negativi connessi alle attività aziendali e ai rapporti con fornitori e partner, nonché a porre rimedio agli impatti che l'organizzazione causa o a cui contribuisce.

L'integrazione dei requisiti ISO 9001:2015, ISO 45001:2023, ISO 14001:2015, UNI/PdR 125:2022, PAS 24000, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 42001 consente a Meridian Group di operare in modo coerente, responsabile e resiliente, allineando gli obiettivi aziendali alla gestione efficace dei processi, alla salvaguardia di un ambiente di lavoro inclusivo e rispettoso delle diversità, alla protezione delle informazioni, alla sicurezza dei servizi cloud e al governo responsabile dei sistemi di intelligenza artificiale inclusi nel perimetro del Sistema di Gestione.

6 Perimetro del Sistema integrato e standard applicabili

Il Sistema di Gestione Integrato è interpretato come sistema documentato unico, nel quale il SGI costituisce il nucleo di governo della qualità, della parità di genere e della sicurezza delle informazioni, venendo poi esteso ai requisiti specifici dei servizi cloud, della protezione delle informazioni personali identificabili trattate in ambienti cloud e del governo responsabile dei sistemi AI.

- ISO 9001:2015: definisce i requisiti per la gestione della qualità, dei processi, dei rischi e delle opportunità, finalizzati al miglioramento continuo e alla soddisfazione del cliente;
- ISO 45001:2023: definisce i requisiti per la gestione della salute e sicurezza dei lavoratori. Nel SGI Meridian la norma è attuata attraverso la Politica per la Qualità e SSL, l'identificazione dei pericoli e la valutazione dei rischi (DVR), la consultazione e partecipazione dei lavoratori, i controlli operativi, la preparazione e risposta alle emergenze e la gestione di infortuni, incidenti e near miss.
- ISO 14001:2015 (con Amd 1:2024): definisce i requisiti del sistema di gestione ambientale. Nel SGI Meridian la norma è attuata attraverso la Politica per la Qualità, la SSL e l'Ambiente, il contesto e le parti interessate, l'identificazione degli aspetti e impatti ambientali, il registro degli obblighi di conformità, gli obiettivi ambientali, i controlli operativi, la preparazione alle emergenze, il monitoraggio, gli audit interni e il riesame.
- UNI/PdR 125:2022: definisce le linee guida per la gestione della parità di genere, attraverso politiche, obiettivi e indicatori volti a ridurre le disparità e promuovere l'inclusione.

© 2024 – All Rights Reserved.

- PAS 24000:2022: definisce i requisiti per un Sistema di Gestione Sociale. Riguarda il rispetto dei diritti umani, le condizioni di lavoro, la salute e sicurezza, la consultazione dei lavoratori e l'etica aziendale. Richiede di individuare, prevenire e mitigare gli impatti negativi delle attività aziendali e della filiera, gestire i reclami e monitorare le prestazioni sociali per migliorarle nel tempo.
- ISO/IEC 27001:2022: definisce il sistema di gestione della sicurezza delle informazioni, la valutazione e il trattamento dei rischi, la Statement of Applicability, i controlli organizzativi, tecnici, fisici e di relazione con le terze parti.
- ISO/IEC 27017:2015: integra il SGSI con linee guida e controlli specifici per i servizi cloud, con particolare attenzione alla ripartizione delle responsabilità tra Meridian, clienti, provider infrastrutturali e fornitori terzi, alla segregazione degli ambienti, al logging, alla gestione delle configurazioni, al supporto tecnico e alla continuità dei servizi SaaS.
- ISO/IEC 27018:2019: integra il SGSI per la protezione delle PII trattate in ambienti public cloud, quando Meridian agisce come cloud service provider/processor o gestisce dati personali nell'erogazione dei servizi, includendo minimizzazione, segregazione, subfornitura, cancellazione/restituzione, gestione richieste e trasparenza verso i clienti.
- ISO/IEC 42001:2023: definisce l'AI Management System applicabile ai sistemi AI sviluppati, configurati o utilizzati da Meridian nel perimetro approvato, con presidi su finalità, ruoli, rischi e impatti, verifiche e validazioni, supervisione umana, segnalazioni, monitoraggio e miglioramento continuo.

L'Azienda applica il Sistema alla seguente sede:



Viale Erminio Spalla

n.9 00142 Roma (RM)

con i presenti campi di applicazione:

UNI EN ISO 9001 :2015, UNI EN ISO 45001 :2023, UNI EN ISO 14001 :2015 e PAS 24000 :2022

PROGETTAZIONE, SVILUPPO E SUPPORTO DI UNA PIATTAFORMA DI CYBER SECURITY IMPLEMENTATA IN MODALITÀ SAAS E/O ON-PREMISE ED EROGAZIONE DEI RELATIVI SERVIZI DI CYBER INTELLIGENCE. EROGAZIONE SERVIZI DI CONSULENZA E ASSISTENZA IN AMBITO IT.

Il sistema di gestione per la salute e sicurezza sul lavoro si applica a tutte le persone che operano sotto il controllo dell'organizzazione e alle attività svolte presso la sede di Roma, in smart working.

Il sistema di gestione ambientale si applica alle attività svolte nella sede di Roma, Viale Erminio Spalla 9.

© 2024 – All Rights Reserved.

UNI/PdR 125:2022

MISURE PER GARANTIRE LA PARITÀ DI GENERE NEL SEGUENTE CONTESTO LAVORATIVO: PROGETTAZIONE ED EROGAZIONE DI SERVIZI IN AMBITO IT, CYBERSECURITY E CYBERINTELLIGENCE.

ISO/IEC 42001

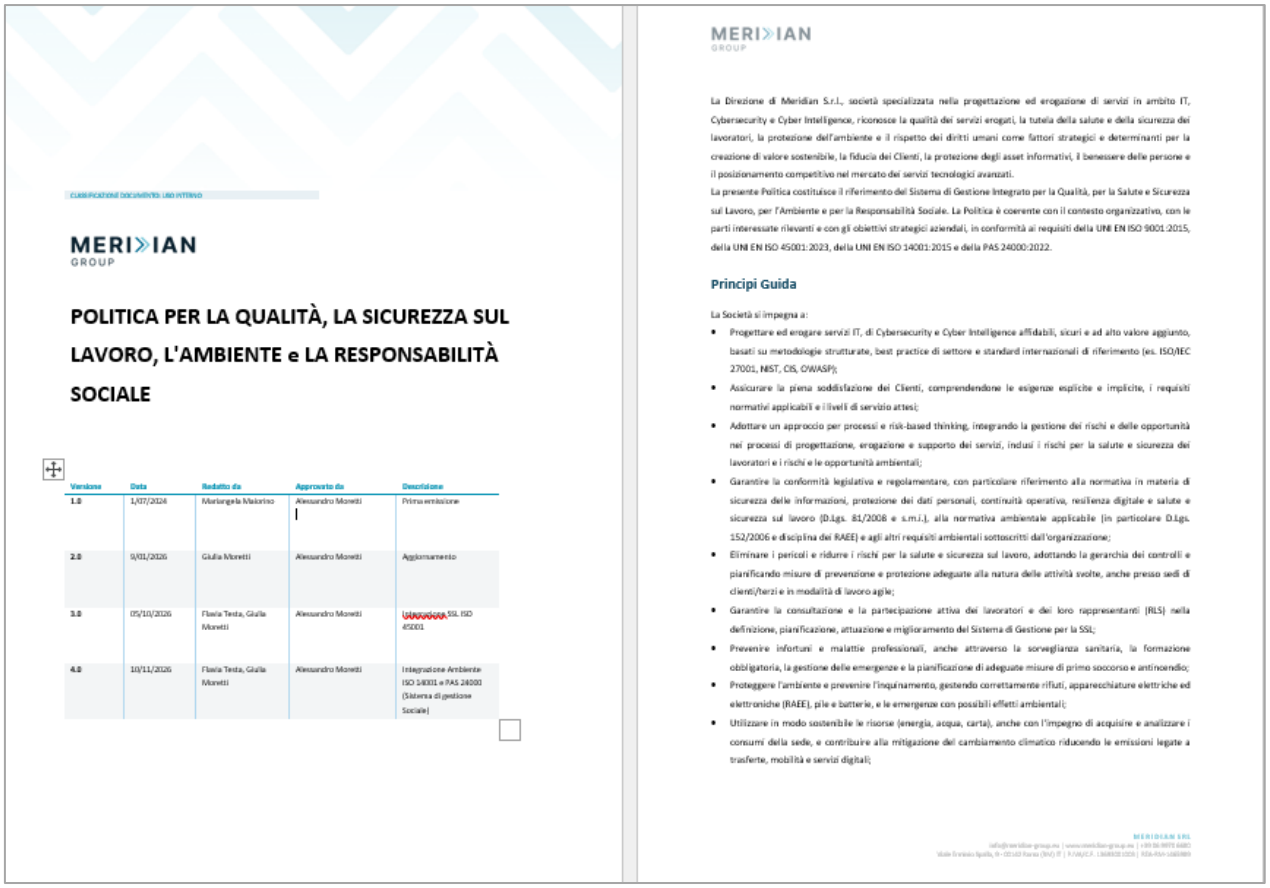
PROGETTAZIONE, SVILUPPO E USO DI UNA PIATTAFORMA DI CYBER SECURITY CHE UTILIZZA MODELLI DI INTELLIGENZA ARTIFICIALE.

ISO/IEC 27001

PROGETTAZIONE, SVILUPPO, EROGAZIONE E INTEGRAZIONE DI UNA PIATTAFORMA DI CYBER SECURITY, DISTRIBUITA ANCHE IN MODALITA' SAAS, ED EROGAZIONE DEI RELATIVI SERVIZI DI CYBER INTELLIGENCE SECONDO LO STATEMENT OF APPLICABILITY REV.01 DEL 14/04/2026. LE ATTIVITA' DI EROGAZIONE DI UNA PIATTAFORMA DI CYBER SECURITY, DISTRIBUITA IN MODALITA' SAAS, SONO STATE VERIFICATE PER QUANTO RIGUARDA L'APPLICAZIONE DEI CONTROLLI DELLE LINEE GUIDA ISO/IEC 27017:2015, ISO/IEC 27018:2019

© 2024 – All Rights Reserved.

7 La Politica per la qualità, la SSL, l'ambiente e la Responsabilità Sociale



CLASSIFICAZIONE DOCUMENTO: USO INTERNO

MERIDIAN GROUP

POLITICA PER LA QUALITÀ, LA SICUREZZA SUL LAVORO, L'AMBIENTE e LA RESPONSABILITÀ SOCIALE

Versione	Data	Redatto da	Approvato da	Descrizione
1.0	1/07/2024	Mariangela Maiorino	Alessandro Moretti	Prima emissione
2.0	9/01/2026	Giulia Moretti	Alessandro Moretti	Aggiornamento
3.0	05/10/2026	Flavia Testa, Giulia Moretti	Alessandro Moretti	Upgrade ISO 45001
4.0	10/11/2026	Flavia Testa, Giulia Moretti	Alessandro Moretti	Integrazione Ambiente ISO 14001 e PAS 24000 (Sistema di gestione Sociale)

MERIDIAN GROUP

La Direzione di Meridian S.r.l., società specializzata nella progettazione ed erogazione di servizi in ambito IT, Cybersecurity e Cyber Intelligence, riconosce la qualità dei servizi erogati, la tutela della salute e della sicurezza dei lavoratori, la protezione dell'ambiente e il rispetto dei diritti umani come fattori strategici e determinanti per la creazione di valore sostenibile, la fiducia dei Clienti, la protezione degli asset informativi, il benessere delle persone e il posizionamento competitivo nel mercato dei servizi tecnologici avanzati.
La presente Politica costituisce il riferimento del Sistema di Gestione Integrato per la Qualità, per la Salute e Sicurezza sul Lavoro, per l'Ambiente e per la Responsabilità Sociale. La Politica è coerente con il contesto organizzativo, con le parti interessate rilevanti e con gli obiettivi strategici aziendali, in conformità ai requisiti della UNI EN ISO 9001:2015, della UNI EN ISO 45001:2023, della UNI EN ISO 14001:2015 e della PAS 24000:2022.

Principi Guida

La Società si impegna a:

- Progettare ed erogare servizi IT, di Cybersecurity e Cyber Intelligence affidabili, sicuri e ad alto valore aggiunto, basati su metodologie strutturate, best practice di settore e standard internazionali di riferimento (es. ISO/IEC 27001, NIST, CIS, OWASP);
- Assicurare la piena soddisfazione dei Clienti, comprendendone le esigenze esplicite e implicite, i requisiti normativi applicabili e i livelli di servizio attesi;
- Adottare un approccio per processi e risk-based thinking, integrando la gestione dei rischi e delle opportunità nei processi di progettazione, erogazione e supporto dei servizi, indusi i rischi per la salute e sicurezza dei lavoratori e i rischi e le opportunità ambientali;
- Garantire la conformità legislativa e regolamentare, con particolare riferimento alla normativa in materia di sicurezza delle informazioni, protezione dei dati personali, continuità operativa, resilienza digitale e salute e sicurezza sul lavoro (D.Lgs. 81/2008 e s.m.i.), alla normativa ambientale applicabile (in particolare D.Lgs. 152/2006 e disciplina dei RAEE) e agli altri requisiti ambientali sottoscritti dall'organizzazione;
- Eliminare i pericoli e ridurre i rischi per la salute e sicurezza sul lavoro, adottando la gerarchia dei controlli e pianificando misure di prevenzione e protezione adeguate alla natura delle attività svolte, anche presso sedi di clienti/terzi e in modalità di lavoro agile;
- Garantire la consultazione e la partecipazione attiva dei lavoratori e dei loro rappresentanti (RLS) nella definizione, pianificazione, attuazione e miglioramento del Sistema di Gestione per la SSL;
- Prevenire infortuni e malattie professionali, anche attraverso la sorveglianza sanitaria, la formazione obbligatoria, la gestione delle emergenze e la pianificazione di adeguate misure di primo soccorso e antincendio;
- Proteggere l'ambiente e prevenire l'inquinamento, gestendo correttamente rifiuti, apparecchiature elettriche ed elettroniche (RAEE), pile e batterie, e le emergenze con possibili effetti ambientali;
- Utilizzare in modo sostenibile le risorse (energia, acqua, carta), anche con l'impegno di acquisire e analizzare i consumi della sede, e contribuire alla mitigazione del cambiamento climatico riducendo le emissioni legate a trasferte, mobilità e servizi digitali;

MERIDIAN SRL

© 2024 – All Rights Reserved.

- Considerare la prospettiva del ciclo di vita dei servizi e delle apparecchiature, privilegiando acquisti a minore impatto, la durata utile delle apparecchiature e fornitori con requisiti e certificazioni ambientali, inclusi i fornitori cloud e di data center;
- Promuovere il miglioramento continuo del Sistema di Gestione Integrato, dei processi aziendali e delle performance operative e ambientali, attraverso l'analisi dei dati, il monitoraggio degli indicatori e la gestione sistematica delle non conformità, degli infortuni e dei quasi-infortuni (near miss) e degli eventi ambientali;
- Valorizzare le competenze del personale, assicurando formazione continua, aggiornamento tecnico-specialistico, formazione obbligatoria in materia di sicurezza, formazione e sensibilizzazione sui temi ambientali e consapevolezza del proprio ruolo nel raggiungimento degli obiettivi di qualità e di SSL e ambientali;
- Favorire una cultura della sicurezza, dell'innovazione e dell'affidabilità, quale elemento distintivo nei servizi di Cybersecurity e Cyber Intelligence e nella tutela quotidiana della salute e sicurezza dei lavoratori e dell'ambiente;
- Collaborare con fornitori e partner qualificati, selezionati e monitorati in base a criteri di competenza, affidabilità, coerenza con i valori aziendali, rispetto dei requisiti di salute e sicurezza sul lavoro e dei requisiti ambientali, incluso il rapporto con la proprietà dell'immobile per gli impianti e le utenze della sede.

Principi di responsabilità sociale

In coerenza con il Codice etico e disciplinare di Meridian, la Società si impegna a rispettare i diritti umani, la dignità delle persone e i requisiti sociali applicabili, compresi quelli di legge, della contrattazione collettiva, degli accordi con le parti interessate e della PAS 24000:2022.

- Valutare con un processo di due diligence gli impatti effettivi e potenziali sui diritti umani nelle attività aziendali e nei rapporti di fornitura. Prevenire o mitigare gli impatti negativi, porre rimedio a quelli causati o a cui la Società ha contribuito e verificare l'efficacia delle misure adottate.
- Vietare il lavoro minorile, il lavoro forzato o obbligatorio e la tratta di persone. Prevenire pratiche abusive di reclutamento e garantire rapporti di lavoro regolari e verificabili, con condizioni comunicate per iscritto in modo comprensibile prima dell'inizio del rapporto. Rispettare i requisiti applicabili in materia di orario, straordinari, pause, riposi, congedi e retribuzione, assicurando pagamenti puntuali e integrali.
- Rispettare la libertà di associazione e il diritto alla contrattazione collettiva. Garantire pari opportunità e parità di trattamento, prevenire discriminazioni, molestie, violenze e abusi e tutelare la dignità e la salute fisica e psicologica delle persone sul lavoro.
- Assicurare la consultazione e la partecipazione dei lavoratori e dei loro rappresentanti, ove presenti, con particolare attenzione al personale senza ruoli direttivi. Mettere a disposizione tempo, informazioni e risorse, rimuovere o ridurre gli ostacoli alla partecipazione e dare riscontro alle proposte.
- Mettere a disposizione dei lavoratori e delle parti esterne canali accessibili per presentare reclami o segnalazioni in materia sociale. Gestire le segnalazioni con riservatezza, tutelare chi le presenta in buona fede da qualsiasi ritorsione e adottare, ove necessario, misure correttive o di rimedio.

- Condurre le attività con correttezza, trasparenza e integrità, prevenendo corruzione, estorsione e appropriazione indebita. Assicurare la veridicità delle informazioni sulle attività e sulle prestazioni aziendali e prevenire dichiarazioni ingannevoli lungo la catena di fornitura.
- Integrare criteri sociali nella qualifica e nel monitoraggio di fornitori, appaltatori e partner rilevanti, in funzione dei rischi. Comunicare gli impegni della Politica e i requisiti sociali applicabili, verificandone il rispetto e richiedendo, ove necessario, azioni correttive.

Obiettivi per la Qualità, per la Salute e Sicurezza sul Lavoro, per l'Ambiente e per la Responsabilità Sociale

La Direzione definisce e riesamina periodicamente obiettivi misurabili per la qualità, per la salute e sicurezza sul lavoro, per l'ambiente e per la responsabilità sociale, coerenti con la presente Politica, finalizzati a:

- migliorare la qualità tecnica e l'efficacia dei servizi erogati;
- ridurre il numero e l'impatto di non conformità e reclami;
- aumentare il livello di soddisfazione e fidelizzazione dei Clienti;
- rafforzare la sicurezza, la continuità e l'affidabilità dei servizi IT;
- migliorare l'efficienza dei processi interni e la capacità di risposta al cambiamento tecnologico e normativo;
- ridurre il numero e la gravità degli infortuni sul lavoro e prevenire l'insorgenza di malattie professionali;
- garantire il pieno rispetto delle scadenze di formazione obbligatoria e di sorveglianza sanitaria previste dalla normativa vigente;
- aumentare il livello di consapevolezza, formazione e partecipazione attiva dei lavoratori in materia di salute e sicurezza sul lavoro;
- assicurare l'efficacia dei piani di gestione delle emergenze e la prontezza di risposta ad eventuali incidenti.
- garantire la gestione corretta dei rifiuti e dei RAEE e il rispetto degli obblighi di conformità ambientali;
- monitorare e ridurre i consumi di carta ed energia e le emissioni connesse alle attività;
- integrare i criteri ambientali nella selezione dei fornitori critici;
- includere gli scenari ambientali nella preparazione e risposta alle emergenze e nella formazione del personale.
- verificare il rispetto delle condizioni di impiego, dei requisiti su orari, riposi e retribuzioni e degli altri requisiti sociali applicabili.
- rafforzare la consultazione, la partecipazione e la formazione dei lavoratori e verificare l'accessibilità dei canali di reclamo e l'efficacia delle risposte.
- monitorare i rischi e gli impatti sui diritti umani, anche presso i fornitori rilevanti, e verificare l'efficacia delle misure di prevenzione, mitigazione e rimedio.

La politica è comunicata e diffusa a tutto il personale e alle parti interessate mediante la comunicazione interna e la pubblicazione sul sito istituzionale.

MERIDIAN SRL
info@meridian-group.eu | www.meridian-group.eu | +39 06 9970 6680
Viale Erminio Spalla, 9 - 00142 Roma (RM) IT | P.IVA/C.F. 13693001003 | REA-RM-1480989

Impegno della Direzione

La Direzione si impegna a garantire la disponibilità delle risorse umane, economiche e strumentali necessarie per l'attuazione e il mantenimento del Sistema di Gestione Integrato per la Qualità, per la Salute e Sicurezza sul Lavoro e per l'Ambiente, ad assicurare che la presente Politica sia compresa, attuata e mantenuta a tutti i livelli dell'organizzazione, a garantire la consultazione e la partecipazione dei lavoratori e dei loro rappresentanti sui temi di SSL, e a riesaminare periodicamente la Politica per verificarne la continua adeguatezza, in relazione all'evoluzione del contesto, del mercato, della normativa e delle esigenze delle parti interessate.
La Direzione si impegna inoltre a soddisfare gli obblighi di conformità ambientali, a proteggere l'ambiente e a migliorare in modo continuo il Sistema di Gestione Ambientale per accrescere le prestazioni ambientali.
Per il Sistema di Gestione Sociale, l'Alta Direzione approva la Politica, assegna e comunica responsabilità e autorità secondo criteri non discriminatori, mette a disposizione le risorse necessarie e ne assicura la comprensione e l'applicazione. Definisce e riesamina gli obiettivi di prestazione sociale, valuta almeno annualmente l'efficacia del Sistema e ne promuove il miglioramento continuo.

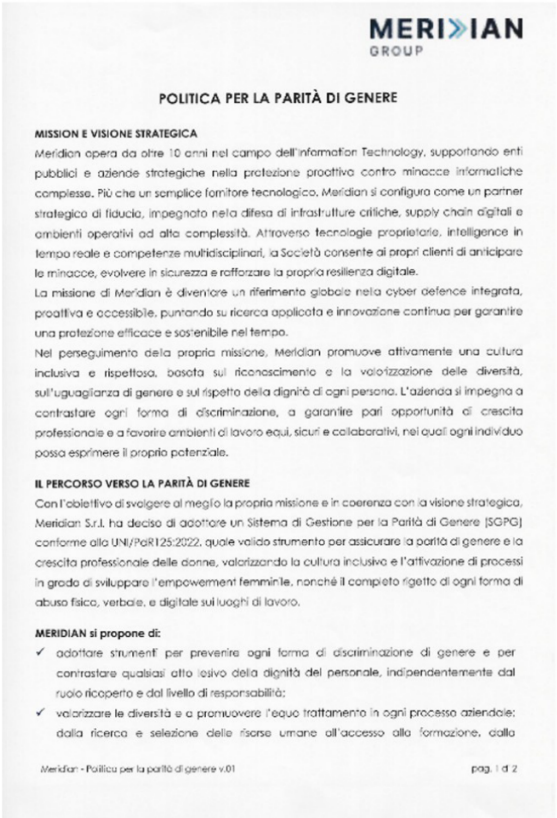
La presente Politica è diffusa internamente, resa disponibile alle parti interessate e costituisce parte integrante della strategia aziendale.

MERIDIAN SRL
info@meridian-group.eu | www.meridian-group.eu | +39 06 9970 6680
Viale Erminio Spalla, 9 - 00142 Roma (RM) IT | P.IVA/C.F. 13693001003 | REA-RM-1480989

© 2024 – All Rights Reserved.

La Politica per la Qualità, la Salute e Sicurezza sul Lavoro (SSL), del Sistema di Gestione Sociale e l'Ambiente (v. 4.0) è approvata dall'Alta Direzione ed è resa disponibile a tutto il personale tramite SharePoint/intranet e alle parti interessate secondo le modalità descritte al capitolo La Comunicazione. Con la sottoscrizione l'Alta Direzione si impegna a: fornire condizioni di lavoro sicure e salubri per la prevenzione di lesioni e malattie correlate al lavoro; eliminare i pericoli e ridurre i rischi per la SSL; soddisfare i requisiti legali e gli altri requisiti sottoscritti; consultare e far partecipare i lavoratori e i loro rappresentanti (RLS); proteggere l'ambiente e prevenire l'inquinamento; soddisfare gli obblighi di conformità ambientali; migliorare in modo continuo il sistema di gestione.

8 La Politica di Parità di Genere



MERIDIAN GROUP

POLITICA PER LA PARITÀ DI GENERE

MISSION E VISIONE STRATEGICA

Meridian opera da oltre 10 anni nel campo dell'Information Technology, supportando enti pubblici e aziende strategiche nella protezione proattiva contro minacce informatiche complesse. Più che un semplice fornitore tecnologico, Meridian si configura come un partner strategico di fiducia, impegnato nella difesa di infrastrutture critiche, supply chain digitali e ambienti operativi ad alta complessità. Attraverso tecnologie proprietarie, intelligence in tempo reale e competenze multidisciplinari, la Società consente ai propri clienti di anticipare le minacce, evolvere in sicurezza e rafforzare la propria resilienza digitale.

La missione di Meridian è diventare un riferimento globale nella cyber defence integrata, proattiva e accessibile, puntando su ricerca applicata e innovazione continua per garantire una protezione efficace e sostenibile nel tempo.

Nel perseguimento della propria missione, Meridian promuove attivamente una cultura inclusiva e rispettosa, basata sul riconoscimento e la valorizzazione delle diversità, sull'uguaglianza di genere e sul rispetto della dignità di ogni persona. L'azienda si impegna a contrastare ogni forma di discriminazione, a garantire pari opportunità di crescita professionale e a favorire ambienti di lavoro equi, sicuri e collaborativi, nei quali ogni individuo possa esprimere il proprio potenziale.

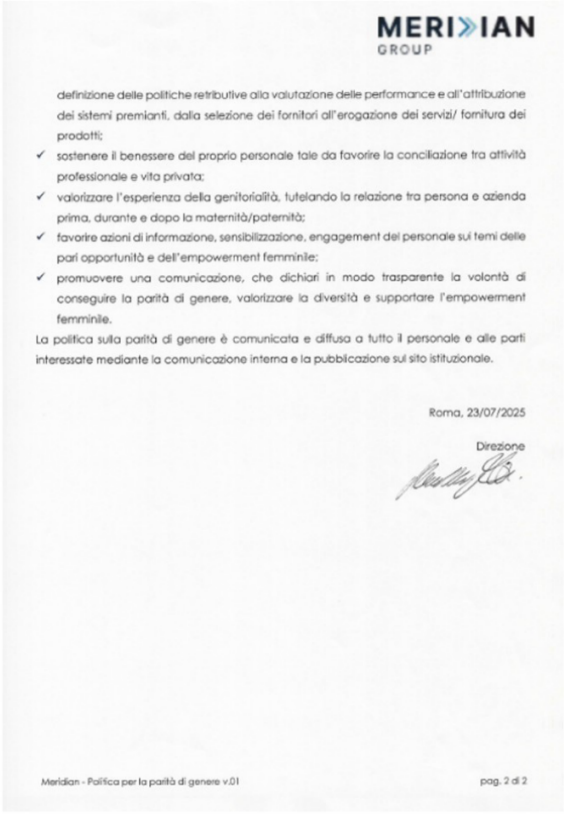
IL PERCORSO VERSO LA PARITÀ DI GENERE

Con l'obiettivo di svolgere al meglio la propria missione e in coerenza con la visione strategica, Meridian S.r.l. ha deciso di adottare un Sistema di Gestione per la Parità di Genere (SGPG) conforme alla UNI/PdR125:2022, quale valido strumento per assicurare la parità di genere e la crescita professionale delle donne, valorizzando la cultura inclusiva e l'attivazione di processi in grado di sviluppare l'empowerment femminile, nonché il completo rigetto di ogni forma di abuso fisico, verbale, e digitale sui luoghi di lavoro.

MERIDIAN si propone di:

- ✓ adottare strumenti per prevenire ogni forma di discriminazione di genere e per contrastare qualsiasi atto lesivo della dignità del personale, indipendentemente dal ruolo ricoperto e dal livello di responsabilità;
- ✓ valorizzare le diversità e a promuovere l'equo trattamento in ogni processo aziendale: dalla ricerca e selezione delle risorse umane all'accesso alla formazione, dalla

Meridian - Politica per la parità di genere v.01 pag. 1 di 2



MERIDIAN GROUP

definizione delle politiche retributive alla valutazione delle performance e all'attribuzione dei sistemi premianti, dalla selezione dei fornitori all'erogazione dei servizi/ fornitura dei prodotti;

- ✓ sostenere il benessere del proprio personale tale da favorire la conciliazione tra attività professionale e vita privata;
- ✓ valorizzare l'esperienza della genitorialità, tutelando la relazione tra persona e azienda prima, durante e dopo la maternità/paternità;
- ✓ favorire azioni di informazione, sensibilizzazione, engagement del personale sui temi delle pari opportunità e dell'empowerment femminile;
- ✓ promuovere una comunicazione, che dichiari in modo trasparente la volontà di conseguire la parità di genere, valorizzare la diversità e supportare l'empowerment femminile.

La politica sulla parità di genere è comunicata e diffusa a tutto il personale e alle parti interessate mediante la comunicazione interna e la pubblicazione sul sito istituzionale.

Roma, 23/07/2025

Direzione

Meridian - Politica per la parità di genere v.01 pag. 2 di 2

© 2024 – All Rights Reserved.

9 La Politica per la sicurezza delle informazioni

Attraverso la sottoscrizione della politica, l'Alta Direzione dimostra il proprio impegno alla qualità, alla sicurezza delle informazioni e al conseguente miglioramento continuo.

9.1 La sicurezza dei servizi cloud e la protezione delle pii

Implementare controlli di sicurezza è un passo fondamentale, ma un processo di sviluppo sicuro efficace richiede anche un robusto meccanismo di monitoraggio delle prestazioni di tali controlli e un ciclo di miglioramento continuo. Questa sezione descrive come l'organizzazione misurerà e monitorerà l'efficacia del Secure SDLC e come intende evolvere progressivamente le proprie pratiche di sicurezza nel tempo.

Per i servizi erogati in modalità SaaS e per le componenti cloud utilizzate a supporto della piattaforma, Meridian applica il SGSI in coerenza con i requisiti e le linee guida ISO/IEC 27017 e ISO/IEC 27018, assicurando che i controlli di sicurezza siano declinati rispetto alla natura cloud del servizio, alle responsabilità condivise e alle aspettative contrattuali dei clienti.

I presidi cloud comprendono la definizione delle responsabilità tra le parti, la gestione delle configurazioni e delle baseline, la segregazione degli ambienti e dei dati, il controllo degli accessi privilegiati, il logging e monitoraggio degli eventi, la gestione degli incidenti, la gestione delle vulnerabilità, il backup e Disaster recovery, la continuità operativa e il controllo dei fornitori infrastrutturali o applicativi rilevanti.

Per le informazioni personali identificabili trattate nell'ambito dei servizi cloud, Meridian adotta misure proporzionate per proteggere riservatezza, integrità e disponibilità dei dati, governare le istruzioni ricevute dal cliente, limitare l'uso dei dati alle finalità autorizzate, gestire cancellazione e restituzione al termine del rapporto, valutare subfornitori e mantenere evidenze documentali idonee ai fini di audit.

Per le implementazioni On-Premise, i controlli cloud e privacy sono applicati nella misura in cui Meridian progetta, sviluppa, configura, supporta o mantiene la piattaforma e i relativi servizi, ferma restando la ripartizione delle responsabilità con il cliente definita nei contratti, nelle offerte tecniche, nei piani di progetto o nella documentazione di supporto.

9.2 La politica ai e il sistema di gestione per l'intelligenza artificiale

Meridian adotta la Policy d'utilizzo degli strumenti AI quale documento di indirizzo dell'AI Management System, con l'obiettivo di assicurare che lo sviluppo, la configurazione, l'utilizzo e il riesame dei sistemi di intelligenza artificiale avvengano in modo responsabile, coerente, controllato e migliorabile.

La Policy stabilisce principi di uso responsabile, sviluppo responsabile, proporzionalità, accountability, coerenza con i requisiti applicabili, coerenza con il framework aziendale e miglioramento continuo. Tali principi sono tradotti in obiettivi, criteri minimi, ruoli, evidenze e flussi di controllo applicabili ai sistemi AI inclusi nello scopo dell'AIMS.

Per ciascun caso d'uso AI rilevante sono mantenute, in misura proporzionata, evidenze relative a finalità e destinazione prevista, owner e funzioni coinvolte, utenti autorizzati, requisiti, input e output, limiti d'uso, rischi principali, verifiche e validazioni, autorizzazione all'uso, supervisione umana, segnalazioni e trigger di riesame. Nel

© 2024 – All Rights Reserved.

perimetro iniziale rientrano i sistemi AI formalmente approvati da Meridian, inclusi i casi d'uso a supporto di traduzione e sintesi di ticket e alert, valutazione di escalation, classificazione di notizie OSINT e instradamento per cluster, chatbot per interrogazione controllata di contenuti perimetrati, classificazione di alert e generazione di report con supervisione dell'analista.

10 Le parti interessate

Meridian ha individuato le parti interessate rilevanti per il proprio Sistema di Gestione Integrato (SGI), comprendente gli aspetti di qualità, parità di genere, di sicurezza delle informazioni, sicurezza dei servizi cloud, protezione delle PII trattate in ambienti cloud e governo dei sistemi di intelligenza artificiale, oltre ai presidi organizzativi già adottati in materia di qualità, persone e inclusione. Tali parti includono:

A. Clienti, utilizzatori e persone interessate dai servizi

- Clienti, in particolare quelli con requisiti specifici in ambito Cyber Security e che condividono i principi e i valori di inclusione;
- Clienti SaaS e clienti con installazioni On-Premise, interessati alla disponibilità, sicurezza, tracciabilità e continuità dei servizi erogati e alla chiara ripartizione delle responsabilità operative;
- Utilizzatori autorizzati della piattaforma e dei servizi di Cyber Intelligence, interessati alla correttezza delle informazioni, alla protezione dei dati e alla trasparenza delle funzionalità supportate da AI;
- Interessati e soggetti cui si riferiscono eventuali dati personali trattati nei servizi cloud, rispetto ai quali Meridian presidia riservatezza, minimizzazione, limitazione d'uso, cancellazione e gestione degli obblighi privacy applicabili
- Esigenze sociali dei clienti già censiti. Considerare, ove pertinenti, i requisiti contrattuali o di qualifica relativi a diritti umani, condizioni di lavoro, etica e gestione responsabile della filiera.

B. Lavoratori, collaboratori, rappresentanze e candidati

- Dipendenti e collaboratori, direttamente coinvolti nella creazione di un ambiente di lavoro sicuro, salubre, rispettoso e che valorizzi le diversità e nell'attuazione dei processi e nell'applicazione delle misure di sicurezza;
- Lavoratori e Rappresentante dei Lavoratori per la Sicurezza (RLS), consultati e coinvolti nell'identificazione dei pericoli, nella valutazione dei rischi e nelle decisioni in materia di SSL;
- Sindacati, coinvolti attivamente nei processi di definizione e monitoraggio delle politiche di SSL, di parità di genere e non discriminazione
- Candidati, in relazione ai quali vi è l'impegno di trasparenza nei processi di selezione e pari opportunità di accesso all'organizzazione, indipendentemente da genere, età, etnia, situazione famigliare o matrimoniale, etc. e una valorizzazione nelle competenze e nell'esperienza senza pregiudizi o stereotipi di genere
- Familiari, con i quali vi è una condivisione dei valori e delle tematiche di sicurezza sul lavoro, non discriminazione e tutela della parità di genere al di fuori del contesto organizzativo e un miglioramento dello stile di vita (work-life balance) e del benessere familiare;

© 2024 – All Rights Reserved.

- Esigenze sociali dei dipendenti e collaboratori. Considerare la chiarezza delle condizioni di impiego, l'equità retributiva, il rispetto di orari e riposi, la tutela da discriminazioni e molestie e l'accesso a un meccanismo di reclamo riservato e senza ritorsioni.
- Lavoratori non dirigenti e loro rappresentanti, ove presenti. Esigenza di ricevere informazioni comprensibili e di contribuire direttamente alla definizione di obiettivi, alla valutazione dei rischi e alla scelta delle misure del SGS, anche per chi lavora da remoto o presso clienti.
- Esigenze delle rappresentanze sindacali. Assicurare la libertà di associazione, la contrattazione collettiva e l'interlocuzione sulle condizioni di lavoro, includendo le eventuali RSA o RSU.

C. Fornitori, appaltatori e partner

- Fornitori strategici e tecnologici, che operano su infrastrutture e sistemi critici;
- Fornitori cloud, infrastrutturali, software, open source e servizi di terzi, che possono incidere sulla sicurezza, sulla continuità, sulla privacy e sull'affidabilità dei sistemi e dei servizi erogati;
- Appaltatori, lavoratori autonomi e visitatori presenti in sede, con i quali si realizzano cooperazione e coordinamento per la gestione dei rischi interferenziali.
- Partner tecnologici, enti normativi e altri stakeholder che possono influenzare – o essere influenzati da – il Sistema di Gestione della Sicurezza delle Informazioni;
- Fornitori e appaltatori rilevanti per gli impatti sociali**.** Individuare le loro esigenze di chiarezza sui requisiti sociali applicabili, sui criteri di qualifica e sulle modalità di segnalazione.
- Lavoratori di fornitori, appaltatori ed eventuali subappaltatori rilevanti. Verificare le condizioni di lavoro applicate (equità e sicurezza), il rispetto dei diritti e accesso al meccanismo di reclamo, in relazione agli impatti delle attività affidate.
- Agenzie per il lavoro e intermediari di reclutamento che necessitano di indicazioni chiare sui requisiti aziendali applicabili alla selezione, al reclutamento e alle condizioni di impiego del personale.

D. Direzione, funzioni aziendali e figure del sistema integrato

- Funzione risorse umane, richiedente un allineamento tra obiettivi di SSL, Diversity & Inclusion e le politiche organizzative di gestione delle risorse umane.
- Datore di Lavoro, RSPP, preposti, addetti alle emergenze (antincendio e primo soccorso) e Medico Competente, figure della prevenzione con compiti definiti dal D.Lgs. 81/2008;
- DPO (Data Protection Officer), figura di controllo per la protezione dei dati personali;
- ISM (Information Security Manager), responsabile dell'attuazione e del monitoraggio del SGSI;
- Owner, utenti, sviluppatori e supervisori dei sistemi AI, coinvolti nel ciclo di vita, nell'uso autorizzato, nella verifica, nella validazione e nel monitoraggio dei casi d'uso AI;
- Alta Direzione e funzioni di coordinamento del SGS (GAM e RSG). Necessitano di informazioni sui rischi sociali, sull'attuazione della Politica, sul raggiungimento degli obiettivi e sull'efficacia delle azioni, per definire priorità e risorse.

© 2024 – All Rights Reserved.

E. Autorità, istituzioni e soggetti di verifica

- Autorità di vigilanza (es. Garante Privacy), che impongono obblighi normativi e regolatori;
- Istituzioni, richiedenti conformità normativa, eticità, trasparenza, onestà nella tenuta delle relazioni e una comunicazione informativa annuale alla Consigliera di Parità di Genere e della famiglia;
- Enti di controllo e istituzioni in materia di SSL (es. ASL, INAIL, Ispettorato del Lavoro, Vigili del Fuoco), che definiscono obblighi e svolgono attività di vigilanza;
- Auditor, organismi di certificazione e altri soggetti di assurance, interessati alla disponibilità di evidenze documentate, tracciabili e coerenti con il perimetro di audit.

Per ciascuna parte interessata, Meridian ha definito i requisiti, le aspettative e i canali di comunicazione, al fine di assicurare un approccio strutturato, trasparente e allineato ai principi di conformità e miglioramento continuo.

© 2024 – All Rights Reserved.

11 Fattori interni ed esterni

FATTORI INTERNI	FATTORI ESTERNI
Modello organizzativo e distribuzione di ruoli, responsabilità e risorse per il SGS, anche tra le funzioni che gestiscono personale, commesse e fornitori.	Contesto di mercato e concorrenza disponibilità di competenze specialistiche e pressione su prezzi e tempi di consegna, con possibili effetti sui carichi di lavoro.
Sistema normativo interno, inclusi i presidi sulle condizioni di lavoro, la tutela dei diritti umani, l'etica e l'integrità aziendale.	Soci in affari con particolare attenzione alla ripartizione delle responsabilità e alla capacità di influenzare le prassi sociali nelle attività condivise
Modello commerciale, criteri di acquisizione e pianificazione delle commesse, sostenibilità degli impegni di servizio rispetto alle risorse disponibili e presidi di integrità nei rapporti commerciali.	Contesto legislativo evoluzione delle norme e della contrattazione collettiva applicabili a rapporti di lavoro, retribuzioni, orari, riposi, pari trattamento e salute e sicurezza.
Contratto di rete, modalità di collaborazione tra le imprese aderenti e chiarezza delle responsabilità sociali nelle eventuali attività condivise.	Cambiamenti nelle aspettative ed esigenze dei clienti, inclusi eventuali requisiti contrattuali o di qualifica su condizioni di lavoro, diritti umani, etica e filiera.
Risk based approach management, capacità di individuare e valutare rischi e opportunità sociali e impatti sui diritti umani nelle attività aziendali e nella filiera.	Continuità dell'erogazione dei servizi dovuta al contesto legislativo in evoluzione, con possibili richieste di copertura fuori orario o interventi urgenti.
Presenza di dati particolari e informazioni critiche gestite internamente, inclusa la riservatezza delle informazioni relative a lavoratori e reclami sociali.	Minacce e vulnerabilità emergenti nel dominio digitale e cyber con possibili picchi di attività per il personale coinvolto nella risposta agli incidenti.
Livello di cultura della sicurezza all'interno dell'organizzazione, propensione a segnalare criticità e possibilità per i lavoratori di partecipare senza timore di ritorsioni.	Evoluzione tecnologica e requisiti imposti dalle normative sulla sicurezza (es. GDPR, NIS2)
Politiche interne per la parità di genere, estensione del pari trattamento alle altre forme di discriminazione e alle diverse tipologie di lavoratori	Reputazione aziendale e aspettative ESG di stakeholder, investitori, clienti, in particolare sulla trasparenza delle prestazioni sociali e sulla gestione responsabile della filiera.
Cultura aziendale e sensibilizzazione sui temi di genere, consapevolezza sui diritti umani, sulla libertà di associazione, sulle condizioni di lavoro e sulla prevenzione di molestie e abusi	Evoluzione culturale e sociale in tema di inclusività
Presenza di strumenti di segnalazione e gestione delle molestie, accessibilità ed efficacia del meccanismo di reclamo sociale per lavoratori e parti esterne, riservatezza e protezione dalle ritorsioni.	Benchmark di settore e buone pratiche DE&I della concorrenza incluse le prassi su equità retributiva, conciliazione e coinvolgimento dei lavoratori.
Pratiche di conciliazione vita-lavoro e flessibilità oraria, gestione dei carichi, degli straordinari, dei riposi, della disconnessione e dell'eventuale reperibilità.	Raccomandazioni UE e orientamenti nazionali su parità e non discriminazione
Presenza di piattaforma Cyber Security erogata in modalità SaaS e/o On-Premise, organizzazione del supporto e copertura degli interventi presso clienti o fuori orario, ove previsti.	Evoluzione dei requisiti e delle aspettative dei clienti su cloud security, data protection e continuità dei servizi
Gestione di componenti AI a supporto di classificazione, analisi e reporting, possibili effetti sulle persone interessate dagli output e, se pertinenti, sull'organizzazione del lavoro o sul trattamento dei lavoratori.	Evoluzione tecnologica, normativa e di mercato sui sistemi AI e sull'affidabilità degli output
Dipendenze da provider infrastrutturali, software, modelli, librerie e componenti di terzi, ricorso a fornitori e appaltatori e capacità di conoscere e influenzare le condizioni di lavoro nelle attività affidate.	Rischi di supply chain, vulnerabilità emergenti, indisponibilità di servizi terzi e modifiche contrattuali. Nei servizi e nei contesti di fornitura pertinenti, considerare anche subappalti, condizioni di impiego, salute e sicurezza e possibili rischi di sfruttamento, lavoro minorile o forzato.
Organizzazione del lavoro in sede, in smart working e in trasferta o presso i clienti; postazioni di lavoro a videoterminale; livello di cultura della sicurezza e di partecipazione dei lavoratori in materia di SSL, con attenzione ai rischi psicosociali,	Evoluzione del quadro normativo e delle richieste di clienti ed enti di controllo in materia di SSL (D.Lgs. 81/2008, L. 81/2017); rischi presenti presso le sedi di clienti e fornitori; eventi esterni

© 2024 – All Rights Reserved.

all'accessibilità e alla possibilità di consultare e coinvolgere chi opera fuori sede.	con impatto sulla sicurezza dei lavoratori (es. eventi climatici estremi)

FATTORI INTERNI	FATTORI ESTERNI
Presenza di dati personali e informazioni dei clienti in servizi cloud e ambienti di supporto	Aspettative di trasparenza, accountability e protezione delle PII da parte di clienti, interessati e autorità
Sistema di gestione ambientale e ruolo del Responsabile SGA (RSGA)	Cambiamento climatico (ondate di calore, allagamenti) e richieste dei clienti sul clima (ISO 14001, Amd 1:2024)
Sala server, apparecchiature IT, uso di carta e di energia e gas	Obblighi di conformità ambientali (D.Lgs. 152/2006, RAEE, reati ambientali del D.Lgs. 231/2001)
Sede in sublocazione: dati e documenti degli impianti disponibili tramite la proprietà	Sublocazione: utenze e impianti a carico del sublocatore. Dipendenza dai tempi di intervento del sublocatore e dalla disponibilità delle evidenze di manutenzione e sicurezza degli impianti.
Composizione dell'organico e modalità di impiego, incluse le eventuali differenze tra dipendenti, collaboratori, tirocinanti e personale somministrato. Capacità di verificare le condizioni di assunzione, inquadramento, retribuzione e orario.	Disponibilità e prassi delle eventuali agenzie per il lavoro e degli intermediari di reclutamento, incluse le condizioni applicate al personale inserito o somministrato.
Canali di consultazione e partecipazione sui temi sociali, capacità di coinvolgere direttamente i lavoratori non dirigenti, eventuale presenza di rappresentanze e accessibilità dei canali per chi opera da remoto o presso clienti.	Evoluzione delle relazioni industriali e degli accordi collettivi di settore, per quanto rilevante per le condizioni di lavoro e il dialogo con i lavoratori.

12 Il risk based approach

Meridian adotta una metodologia integrata di identificazione, valutazione e gestione dei rischi e delle opportunità, correlata alla definizione degli obiettivi aziendali e orientata al miglioramento continuo delle prestazioni del Sistema di Gestione Integrato (SGI).

Il Sistema di Gestione favorisce i flussi informativi top-down e bottom-up, assicurando il coinvolgimento delle funzioni aziendali e una visione sistemica e coordinata dei rischi e delle opportunità nei diversi ambiti normativi.

In ottica ISO 9001:2015, Meridian identifica e valuta i rischi e le opportunità connessi ai processi aziendali, con particolare riferimento alla qualità dei servizi erogati, alla soddisfazione dei clienti, alla conformità ai requisiti contrattuali, all'efficacia dei processi operativi, alle competenze del personale e all'affidabilità dei fornitori. La valutazione è aggiornata in funzione dell'evoluzione del contesto organizzativo e operativo e consente di individuare azioni finalizzate a prevenire effetti indesiderati, migliorare le prestazioni e cogliere opportunità di sviluppo. Gli esiti sono formalizzati nel Risk Assessment ISO 9001, recentemente aggiornato con l'individuazione di nuovi rischi e opportunità.

In ottica UNI/PdR 125:2022, Meridian considera i rischi e le opportunità connessi alla parità di genere, alle pari opportunità e all'inclusione, con particolare attenzione ai processi di selezione, assunzione, sviluppo professionale, crescita e remunerazione, alla conciliazione vita-lavoro, alla genitorialità e alla prevenzione di discriminazioni, molestie e disparità di trattamento. La valutazione è supportata dal monitoraggio degli indicatori previsti dalla Prassi di Riferimento, dalle attività del Comitato Guida e del Referente del Sistema di Gestione per la Parità di Genere, nonché dalle iniziative di miglioramento del clima e del benessere organizzativo.

© 2024 – All Rights Reserved.

In ottica ISO/IEC 27001:2022, l'approccio è esteso alla valutazione e gestione dei rischi per la sicurezza delle informazioni, comprendendo le minacce alla riservatezza, integrità e disponibilità dei dati e dei sistemi. Il Risk Assessment supporta l'identificazione dei controlli di sicurezza appropriati e delle misure di trattamento necessarie.

Il risk-based approach è inoltre esteso ai servizi cloud e alle implementazioni SaaS/On-Premise, in coerenza con ISO/IEC 27017 e ISO/IEC 27018, considerando i rischi relativi a disponibilità e continuità dei servizi, segregazione logica, configurazioni, protezione delle PII, responsabilità condivise, subfornitori, accessi privilegiati, vulnerabilità e incidenti.

Per i sistemi AI inclusi nel perimetro ISO/IEC 42001:2023, Meridian applica una valutazione proporzionata dei rischi e degli impatti, considerando finalità e destinazione prevista, dati e fonti informative, affidabilità degli output, supervisione umana, possibilità di errore o uso improprio, trasparenza e necessità di verifica, validazione e riesame.

Per la salute e sicurezza sul lavoro, anche nell'ambito del percorso di certificazione ISO 45001, Meridian identifica i pericoli e valuta i rischi per i lavoratori attraverso il Documento di Valutazione dei Rischi (DVR), aggiornato in occasione di cambiamenti significativi, infortuni, incidenti, near miss rilevanti e variazioni normative. I rischi sono trattati secondo la gerarchia delle misure di prevenzione e protezione, con il coinvolgimento dei lavoratori e dell'RLS. Le opportunità di miglioramento della salute e sicurezza sono considerate nell'ambito della pianificazione e del riesame della Direzione.

Per l'ambiente i rischi e le opportunità derivano dagli aspetti ambientali significativi, dagli obblighi di conformità e dal contesto (UNI EN ISO 14001:2015, 6.1). Sono valutati nel Risk Assessment (processo "Ambiente (SGA)") con probabilità, impatto, controlli e azioni, e le azioni sono tracciate nel DB Azioni di miglioramento. Gli aspetti e gli impatti sono valutati nel Registro degli aspetti e impatti ambientali con la metodologia della PR Gestione ambientale.

Per la responsabilità sociale, Meridian identifica e valuta i rischi e le opportunità del Sistema di Gestione Sociale (SGS) a partire dal contesto aziendale, dalle esigenze delle parti interessate, dai requisiti applicabili e dagli esiti della consultazione e partecipazione dei lavoratori (PAS 24000:2022, § 6.1). I rischi e le opportunità sono documentati nel Risk Assessment aziendale, con indicazione dei controlli esistenti e delle azioni da attuare. Attraverso la due diligence sui diritti umani, Meridian mantiene un inventario dei rischi, valuta gli impatti effettivi e potenziali delle proprie attività e dei rapporti di fornitura, definisce misure di prevenzione e mitigazione e prevede rimedi per gli impatti che causa o a cui contribuisce (Allegato A.1). Le azioni sono tracciate nel DB Azioni di miglioramento, con responsabili, scadenze e verifica dell'efficacia.

Gli esiti delle valutazioni confluiscono negli strumenti documentali applicabili ai diversi ambiti del SGI, tra cui Risk Assessment, piani di trattamento, Statement of Applicability, documentazione di governance AI, DVR, indicatori di monitoraggio, registri delle non conformità e azioni correttive, definizione degli obiettivi sociali, nel piano di lavoro annuale del SGS e nel riesame della Direzione.

La Direzione riesamina periodicamente i risultati delle valutazioni, l'efficacia delle misure adottate e lo stato delle azioni pianificate, assicurando la coerenza tra rischi, opportunità, obiettivi aziendali e miglioramento continuo.

© 2024 – All Rights Reserved.

13 Il miglioramento continuo

13.1 Leadership e partecipazione

- Politiche
- Contesto, parti interessate e fattori interni e esterni
- Pianificazione
- Identificazione dei rischi e delle opportunità
- Individuazione delle prescrizioni legali e di altro tipo, tenuta del registro delle prescrizioni legali e degli altri requisiti SSL e verifica periodica della conformità
- Individuazione e verifica del rispetto dei requisiti applicabili in materia sociale, inclusi quelli contrattuali concordati con le parti interessate.
- Risk Assessment del SGI
- Due diligence sui diritti umani, con inventario dei rischi, valutazione degli impatti effettivi e potenziali delle attività aziendali e dei rapporti di fornitura, misure di prevenzione e mitigazione e rimedi per gli impatti che Meridian causa o a cui contribuisce.
- Identificazione dei pericoli e valutazione dei rischi per la SSL (DVR)
- Indicatori ed obiettivi
- Documentazione del SGI incluse le evidenze delle consultazioni, delle proposte dei lavoratori, delle decisioni e dei riscontri forniti.
- Consultazione e partecipazione dei lavoratori (RLS, riunione periodica ex art. 35 D.Lgs. 81/2008, segnalazione di pericoli, near miss e infortuni)
- Consultazione e partecipazione sui temi sociali, con particolare attenzione al coinvolgimento diretto dei lavoratori non dirigenti e dei loro rappresentanti, ove presenti. Meridian raccoglie i loro contributi prima delle decisioni sulla Politica e sugli obiettivi sociali e li coinvolge nella valutazione dei rischi, nella definizione delle misure e nella verifica della loro efficacia.
- Identificazione degli aspetti e degli impatti ambientali e degli obblighi di conformità ambientali (Registro aspetti e obblighi)

La Direzione approva la Politica ambientale, assegna ruoli e responsabilità del SGA e nomina il Responsabile del SGA (RSGA), definito nel Mansionario. Promuove la partecipazione dei lavoratori alla prevenzione degli impatti ambientali e alla segnalazione di anomalie.

Per il SGS, l'Alta Direzione approva la Politica sociale, assegna e comunica i ruoli, le responsabilità e le autorità definiti nel Mansionario e assicura le risorse necessarie. Promuove la consultazione e la partecipazione dei lavoratori mettendo a disposizione tempo, informazioni comprensibili, formazione e canali accessibili. Rimuove o riduce le barriere alla partecipazione e tutela da ritorsioni chi segnala criticità in buona fede. Nel riesame della Direzione valuta le prestazioni sociali, gli esiti delle consultazioni e l'efficacia delle azioni intraprese.

13.2 Misurazione delle prestazioni e miglioramento

- Audit interni

© 2024 – All Rights Reserved.

- Monitoraggio processi
- Gestione non conformità e azioni correttive
- Gestione di infortuni, incidenti, near miss e non conformità SSL
- Gestione di incidenti, reclami e non conformità in materia sociale, con tutela della riservatezza e protezione da ritorsioni. Analisi delle cause con la partecipazione dei lavoratori pertinenti, definizione delle azioni correttive e verifica della loro efficacia
- Valutazione della conformità ai requisiti legali e agli altri requisiti applicabili in materia sociale, inclusi gli impegni contrattuali concordati
- Valutazione periodica della conformità ai requisiti legali e agli altri requisiti SSL
- KPI
- Monitoraggio degli indicatori di prestazione sociale pertinenti all'Allegato A, per uso interno ed esterno. Analisi e valutazione dei risultati almeno annuale, considerando anche l'efficacia delle misure adottate a seguito della due diligence sui diritti umani e le prestazioni dei fornitori rilevanti
- Monitoraggio degli indicatori ambientali e valutazione della conformità agli obblighi ambientali
- Gestione di eventi e non conformità ambientali

13.3 Riesame della Direzione

- Pianificazione e miglioramento continuo.

Il Riesame considera: modifiche del contesto, degli obblighi di conformità, rischi e opportunità; grado di raggiungimento degli obiettivi e tendenza delle prestazioni; esito della valutazione di conformità; non conformità, eventi e azioni correttive; esiti di monitoraggio, misurazione e audit; adeguatezza delle risorse; comunicazioni rilevanti delle parti interessate, comprese autorità e clienti; opportunità di miglioramento.

Gli esiti del Riesame pertinenti al Sistema di Gestione Sociale sono comunicati ai lavoratori e ai loro rappresentanti, ove presenti, così come l'aggiornamento delle azioni di miglioramento con responsabili, scadenze e modalità di verifica.

© 2024 – All Rights Reserved.

14 La mappa dei processi

La mappa dei processi di Meridian Group rappresenta in modo integrato le attività gestite secondo il ciclo Plan-Do- Check-Act e secondo i requisiti applicabili di ISO 9001:2015, ISO 45001:2023, UNI/PdR 125:2022, ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 42001:2023.

Organizzata secondo il ciclo Plan–Do–Check–Act, assicura il controllo della qualità, la sicurezza delle informazioni e il miglioramento continuo dell'organizzazione.

- Pianificazione strategica
- Analisi del contesto e delle parti interessate
- Identificazione e valutazione di rischi e opportunità
- Analisi di genere nel contesto organizzativo e nei processi
- Definizione degli obiettivi e indicatori di parità di genere
- Leadership, ruoli e responsabilità
- Gestione della documentazione e delle registrazioni
- Gestione delle risorse umane e comunicazione interna
- Processi inclusivi di recruiting, valutazione e avanzamento carriera
- Politiche per la conciliazione vita-lavoro e flessibilità
- Gestione delle infrastrutture, dei sistemi e dell'ambiente di lavoro
- Gestione Infrastruttura ICT
- Controllo accessi e identità digitali (IAM)
- Monitoraggio e raccolta log (SIEM)
- Gestione degli incidenti di sicurezza (IRP)
- Qualifica fornitori e approvvigionamento
- Monitoraggio della catena di fornitura in ottica DE&I
- Sviluppo nuovi servizi
- Sviluppo e proposizione commerciale
- Gestione ordini e attivazione commesse
- Progettazione ed erogazione di servizi di consulenza
- Cyber Threat Intelligence
- Monitoraggio delle identità digitali (Kitsune Platform)
- Gestione dei servizi cloud SaaS e dei controlli specifici ISO/IEC 27017
- Protezione delle PII trattate nei servizi cloud secondo ISO/IEC 27018
- Governo dei casi d'uso AI e dell'AI Management System
- Verifica, validazione, monitoraggio e riesame dei sistemi AI
- Gestione dei fascicoli tecnici e delle evidenze AI
- Gestione dei livelli di servizio, della continuità operativa e del disaster recovery per la piattaforma
- Amministrazione, finanza e controllo
- Rilevazione e analisi della soddisfazione del cliente
- Valutazione delle prestazioni (KPI, audit interni, riesami)

© 2024 – All Rights Reserved.

- Monitoraggio degli indicatori di parità di genere (es. gender pay gap, accesso alla formazione, rappresentanza)
- Audit interni sul sistema di gestione per la parità
- Gestione rilievi, reclami, non conformità e azioni correttive
- Aggiornamento periodico del piano strategico di parità di genere
- Gestione del cambiamento
- Identificazione dei pericoli e valutazione dei rischi per la SSL (DVR)
- Consultazione e partecipazione dei lavoratori anche in ambito sociale
- Controlli operativi SSL e gestione di appalti e fornitori (DUVRI)
- Preparazione e risposta alle emergenze
- Gestione di infortuni, incidenti e near miss
- Valutazione della conformità ai requisiti legali SSL e ai requisiti sociali
- Identificazione e valutazione degli aspetti e impatti ambientali
- Gestione degli obblighi di conformità ambientali
- Gestione di rifiuti e RAEE
- Preparazione e risposta alle emergenze ambientali
- Monitoraggio dei consumi e delle prestazioni ambientali
- Due diligence sui diritti umani
- Pianificazione delle prestazioni sociali e piano di lavoro annuale
- Sviluppo delle capacità, competenze e consapevolezza sul SGS
- Gestione dell'etica e dell'integrità aziendale

© 2024 – All Rights Reserved.

15 La gestione del cambiamento

La necessità di operare cambiamenti che impattano sul Sistema di Gestione può emergere da differenti ragioni, tra le quali:

- piani di sviluppo aziendale e strategico,
- modifiche delle politiche aziendali,
- cambiamenti legislativi, delle norme cogenti e dei regolamenti in genere, della contrattazione collettiva o degli impegni contrattuali applicabili in materia di condizioni di lavoro, diritti umani, salute e sicurezza, etica e integrità.
- segnalazioni del personale e/o altre parti interessate del contesto aziendale, esiti della consultazione e partecipazione dei lavoratori, reclami sociali, audit, riesami o verifiche di conformità che evidenziano la necessità di modificare processi, controlli o risorse del SGS
- sviluppi delle conoscenze e delle tecnologie,
- modifiche nei requisiti cogenti e/o requisiti applicabili,
- modifiche operative e/o di documenti attestanti le valutazioni dei rischi,
- cambiamenti organizzativi e variazioni delle modalità di impiego o dell'organizzazione del lavoro che incidono su mansioni, organici, carichi, orari, straordinari, riposi, reperibilità o accesso ai canali di consultazione e reclamo.
- cambiamento di fornitori, appaltatori o outsourcer, subappaltatori o servizi esternalizzati che può incidere sulle condizioni di lavoro o sui diritti umani nella filiera, anche a seguito degli esiti della due diligence.
- impatto sul cambiamento climatico;
- variazioni degli aspetti ambientali o degli obblighi di conformità
- introduzione di nuove attività, mansioni, attrezzature, postazioni di lavoro o modifiche ai locali e agli impianti della sede con impatto sui pericoli e sui rischi per la SSL;
- modifiche alle modalità di lavoro (smart working, trasferte, attività presso le sedi dei clienti) e all'organizzazione del lavoro;
- infortuni, incidenti, near miss o esiti della sorveglianza sanitaria che evidenzino la necessità di rivedere la valutazione dei rischi.
- modifiche significative a modelli AI, dataset, tassonomie, prompt, criteri di classificazione, componenti di terzi o modalità di supervisione;
- modifiche rilevanti all'architettura cloud, ai provider infrastrutturali, alle modalità di erogazione SaaS/On-Premise o ai meccanismi di segregazione e protezione dei dati;
- modifiche al campo di applicazione, ai clienti serviti, ai trattamenti di PII o alla ripartizione delle responsabilità contrattuali con clienti e fornitori.

In funzione della tipologia di cambiamento/modifica, possono emergere specifiche necessità che comportano l'apertura di iter decisionali e/o specifiche approvazioni a cura di personale qualificato e preposto. È necessario che qualsiasi azione di cambiamento che abbia impatto sul Sistema di Gestione aziendale avvenga in modo controllato, assegnando le responsabilità in materia di gestione delle modifiche e stabilendo la sequenza delle diverse fasi in funzione degli elementi tipici di sviluppo di un processo di cambiamento.

© 2024 – All Rights Reserved.

La necessità di apportare cambiamenti/modifiche comporta soprattutto una valutazione di una serie di attività, riconducibili a:

- Aggiornamento del contesto o delle politiche aziendali;
- Aggiornamento della valutazione dei rischi/opportunità aziendali e relative azioni conseguenti (incluso l'aggiornamento del DVR per gli aspetti SSL). Per i cambiamenti pianificati, temporanei o permanenti, che possono incidere sui risultati attesi del Sistema di Gestione Sociale (SGS), individuazione e valutazione dei rischi e delle opportunità prima dell'attuazione con il coinvolgimento dei lavoratori interessati, con particolare attenzione ai non dirigenti, e dei loro rappresentanti, ove presenti.
- Verifica del rispetto dei requisiti cogenti e di tutti gli altri requisiti applicabili e pertinenti;
- Attività di formazione del personale coinvolto nel cambiamento/modifica;
- Aggiornamento della documentazione tecnica e/o di Sistema (procedure, istruzioni, etc.) e relative azioni conseguenti.

In caso di cambiamento non intenzionale, il responsabile del processo ne riesamina le conseguenze sul Sistema di Gestione Sociale e adotta, ove necessario, le misure per mitigare gli effetti negativi.

© 2024 – All Rights Reserved.

16 La Comunicazione

Il processo di comunicazione interna ed esterna - con particolare riferimento alla Politica Qualità, SSL e alla Politica per la Parità di Genere, è l'insieme delle strategie e delle azioni poste in essere dall'azienda allo scopo di diffondere una corretta conoscenza dei temi in ambito, promuovere un rapporto costante di dialogo e di cooperazione tra le parti interessate e agevolare il processo di costruzione del consenso.

Le comunicazioni avvengono tramite e-mail e mediante l'intranet aziendale che consente un aggiornamento continuo sulla vita dell'azienda.

Per i servizi cloud e per la piattaforma erogata ai clienti, Meridian assicura che le comunicazioni rilevanti in materia di sicurezza, continuità operativa, incidenti, modifiche significative e responsabilità condivise siano gestite tramite canali controllati e con tracciabilità adeguata.

Per i sistemi AI inclusi nello scopo dell'AIMS, Meridian rende disponibili agli utenti autorizzati istruzioni sintetiche, limiti d'uso, criteri di supervisione umana e canali di segnalazione delle criticità. Le informazioni verso clienti o altre parti interessate sono fornite secondo criteri di appropriatezza, trasparenza e protezione delle informazioni riservate.

Per la SSL, Meridian assicura che la Politica e le informazioni rilevanti (nomine, procedure di emergenza, misure di prevenzione e protezione) siano comunicate a tutti i lavoratori, ai visitatori e agli appaltatori tramite intranet/SharePoint, e-mail, riunioni e formazione. I lavoratori possono segnalare pericoli, situazioni di rischio, near miss e infortuni al proprio responsabile, all'RSPP o all'RLS, secondo le modalità previste dalla procedura Consultazione e partecipazione dei lavoratori. Le comunicazioni con gli enti di controllo sono gestite dalla Direzione con il supporto dell'RSPP.

La comunicazione ambientale interna avviene tramite il canale aziendale e la formazione. La comunicazione esterna con autorità, clienti, proprietà e fornitori è gestita da HR & Legal e dalla Direzione; l'RSGA registra le richieste ambientali ricevute e le risposte.

Le attività di comunicazione relative al sistema di responsabilità sociale sono definite nel piano di comunicazione che definisce la tipologia di comunicazione, la periodicità, gli stakeholders interessati, il canale utilizzato e il responsabile.

La Politica è pubblicata sul sito istituzionale.

17 Le Misurazioni

Meridian pone grande attenzione alla misurazione delle performance dei propri processi.

Il Sistema di Gestione Integrato mette a disposizione strumenti per raccogliere, selezionare e riesaminare dati ed evidenze volti a:

- verificare il raggiungimento dei risultati rispetto agli obiettivi e alle linee strategiche definite dalla Direzione;

© 2024 – All Rights Reserved.

- dimostrare la compliance alle normative cogenti e agli standard volontari applicabili al perimetro di audit (ISO 9001:2015, UNI/PdR 125:2022, PAS 24000:2022, ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 42001:2023, ISO 45001:2023);
- garantire il controllo e il miglioramento continuo delle misure di sicurezza adottate.

Il monitoraggio dei processi avviene attraverso:

- indicatori di performance qualitativa e di sicurezza delle informazioni;
- indicatori secondo la UNI/PdR 125:2022;
- indicatori di prestazione sociale pertinenti all'Allegato A
- indicatori specifici per sicurezza cloud, protezione delle PII, governo dei casi d'uso AI e affidabilità dei servizi erogati;
- audit interni con estensione ai requisiti del SGSI;
- misurazione della qualità della relazione con i business partner e della fiducia dei clienti rispetto alla protezione dei dati;
- valutazione periodica del rischio informatico;
- gestione degli incidenti di sicurezza;
- indicatori SSL (es. infortuni e near miss segnalati, azioni correttive SSL chiuse nei tempi, ore di formazione SSL erogate, esiti delle prove di emergenza e della riunione periodica);
- controllo dell'efficacia delle contromisure tecniche e organizzative implementate.
- monitoraggio di disponibilità, continuità, backup, disaster recovery e livelli di servizio della piattaforma SaaS e delle componenti critiche;
- verifica periodica di accessi privilegiati, configurazioni, vulnerabilità, patching, logging, segregazione e sicurezza degli ambienti cloud;
- monitoraggio delle evidenze relative alla protezione delle PII, alla gestione delle richieste, alla cancellazione/restituzione dei dati e al controllo dei subfornitori;
- monitoraggio dei sistemi AI, inclusi esiti di verifica e validazione, accuratezza o metriche di qualità definite, segnalazioni, anomalie, interventi di supervisione, modifiche significative e riesami periodici;
- rendicontazione a Direzione e funzioni competenti degli esiti di audit, rilievi, non conformità, azioni correttive e miglioramenti relativi a SGSI, cloud security, PII e AIMS.
- indicatori ambientali: consumo di carta, fornitori critici con criteri ambientali, verifica degli obblighi di conformità, eventi e non conformità ambientali, prova di emergenza con scenari ambientali, formazione ambientale, azioni di miglioramento ambientale.

18 Documentazione di riferimento del SGI e del perimetro del sistema di gestione

Il Sistema di Gestione Integrato è supportato da informazioni documentate e registrazioni sottoposte a controllo, predisposte, aggiornate, conservate e rese disponibili secondo le regole interne di gestione documentale.

© 2024 – All Rights Reserved.

Ai fini degli audit relativi agli standard ISO 9001:2015, ISO 45001:2023, UNI/PdR 125:2022, PAS 24000:2022, ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 e ISO/IEC 42001:2023, costituiscono principali riferimenti documentali:

- Manuale SGI, politiche di sistema, campo di applicazione, analisi del contesto e delle parti interessate, obiettivi, indicatori, programmi di miglioramento e riesami della Direzione;
- mappatura dei processi, criteri di gestione e monitoraggio, analisi dei rischi e delle opportunità, KPI e obiettivi relativi al Sistema di Gestione per la Qualità;
- documentazione relativa alla UNI/PdR 125:2022, comprendente la politica per la parità di genere, il Piano Strategico, il file di monitoraggio dei KPI, le procedure HR e le ulteriori politiche e misure collegate;
- Statement of Applicability e relative motivazioni di inclusione o esclusione dei controlli previsti dalla ISO/IEC 27001 e dalla ISO/IEC 42001, nonché matrici di applicabilità dei controlli cloud e privacy previsti dalla ISO/IEC 27017 e dalla ISO/IEC 27018;
- Risk Assessment e piani di trattamento relativi alla sicurezza delle informazioni, ai servizi cloud, alla protezione delle PII e ai sistemi di intelligenza artificiale;
- procedure di sistema e procedure operative, incluse quelle relative alla gestione delle risorse umane, alla progettazione e sviluppo, alla gestione dei fornitori, delle non conformità, degli audit e delle azioni correttive;
- procedure e registri relativi alla gestione degli asset, delle identità e degli accessi, delle configurazioni sicure, delle vulnerabilità, dello sviluppo sicuro, degli incidenti, dei cambiamenti, dei backup, del disaster recovery e della continuità operativa;
- contratti, accordi, SLA, architetture, configurazioni, log e report di controllo relativi ai servizi cloud e alle responsabilità condivise tra le parti;
- Privacy Policy, informative, accordi sul trattamento dei dati, registri dei trattamenti, istruzioni del cliente ed evidenze relative alla gestione, restituzione e cancellazione delle PII;
- Clean Desk Policy, Smart Working Policy e ulteriori istruzioni operative applicabili alla protezione delle informazioni, dei dati personali e degli strumenti aziendali;
- Policy AI, schede di governo dei casi d'uso AI, registri di verifica e validazione, registro delle segnalazioni e delle criticità AI, istruzioni per l'utilizzo autorizzato e matrice di allineamento con le altre policy organizzative;
- fascicoli tecnici dei sistemi AI e delle componenti rilevanti della piattaforma Kitsune, comprensivi di architettura, dati utilizzati, metriche, attività di verifica e validazione, limiti, rischi, modalità di monitoraggio, gestione degli incidenti e condizioni che determinano il riesame;
- registrazioni relative ad audit interni, monitoraggi, reclami, segnalazioni, non conformità, azioni correttive e di miglioramento, formazione, consapevolezza e valutazione dell'efficacia delle misure adottate.
- documentazione SSL: Politica per la SSL, Documento di Valutazione dei Rischi (DVR) e DUVRI, registro delle prescrizioni legali e checklist di conformità, piano di emergenza e verbali delle prove, nomine e attestati di formazione (RSPP, RLS, addetti alle emergenze, preposti, Medico Competente), verbali della riunione periodica, registro di infortuni, incidenti, near miss e azioni correttive SSL.
- Documentazione ambientale: PR Gestione ambientale, Registro degli aspetti e impatti ambientali e degli obblighi di conformità, Politica per l'Ambiente, esiti delle verifiche di conformità ambientale.
- Documentazione del Sistema di Gestione Sociale (SGS), comprendente Politica sociale, campo di applicazione, ruoli, analisi del contesto e dei rischi, obiettivi, piano di sviluppo delle capacità e piano di lavoro annuale. Include le evidenze della due diligence sui diritti umani, della consultazione dei lavoratori, della

© 2024 – All Rights Reserved.

gestione dei reclami, delle verifiche di conformità e dei controlli sui fornitori rilevanti, nonché le registrazioni di comunicazione e formazione, gli indicatori sociali, gli audit interni e il riesame annuale della Direzione

© 2024 – All Rights Reserved.

19 Matrice sintetica standard - processi – evidenze

Standard	Ambito nel SGI	Processi/presidi principali	Evidenze documentali attese
ISO 9001:2015	Sistema di gestione per la qualità dei processi, prodotti e servizi	Analisi del contesto, gestione dei processi, requisiti del cliente, progettazione e sviluppo, controllo dei fornitori, monitoraggio delle prestazioni, gestione delle non conformità e miglioramento	Politica e obiettivi per la qualità, mappa e indicatori di processo, procedure, registri operativi, valutazioni dei fornitori, reclami, audit, riesame, non conformità e azioni correttive
ISO 45001:2023	Sistema di gestione per la salute e sicurezza sul lavoro	Politica SSL, identificazione dei pericoli e valutazione dei rischi (DVR), prescrizioni legali, consultazione e partecipazione dei lavoratori (RLS), formazione e competenze, controlli operativi e appalti (DUVRI), gestione del cambiamento, preparazione e risposta alle emergenze, gestione di infortuni, incidenti e near miss, audit interni e riesame	Politica per la Qualità e SSL, DVR e DUVRI, registro prescrizioni legali e checklist di conformità, nomine e verbali RLS/riunione periodica, piano formativo e attestati, piano di emergenza e verbali delle prove, registro infortuni/near miss, DB Azioni di Miglioramento, programma e rapporti di audit, verbale di riesame
ISO 14001:2015	Sistema di gestione ambientale	Contesto e parti interessate, aspetti e impatti ambientali, obblighi di conformità, rischi e opportunità, obiettivi ambientali, controlli operativi, emergenze, monitoraggio, audit e riesame	Politica per la Qualità, la SSL e l'Ambiente, Registro aspetti e obblighi di conformità, Risk Assessment, PR Gestione ambientale, registrazioni di conferimento, verifica di conformità, DB Azioni di miglioramento, verbale di riesame
UNI/PdR 125:2022	Sistema di gestione per la parità di genere e l'inclusione	Governance della parità di genere, selezione e assunzione, sviluppo professionale, equità retributiva, genitorialità e conciliazione vita-lavoro, prevenzione di abusi e molestie, monitoraggio dei KPI	Politica per la parità di genere, piano strategico, KPI e dati disaggregati, procedure HR, analisi retributive, evidenze formative, segnalazioni, audit, riesame e azioni di miglioramento
PAS 24000:2022	Sistema di gestione scoiale per la tutela dei diritti umani, la promozione di condizioni di lavoro eque e sicure e il miglioramento delle prestazioni sociali nelle attività aziendali e nei rapporti di fornitura.	Analisi del contesto e dei rischi sociali, due diligence sui diritti umani, consultazione e partecipazione dei lavoratori, gestione dei reclami sociali, controllo dei requisiti sociali dei fornitori, etica e integrità aziendale, monitoraggio delle prestazioni e miglioramento.	Politica sociale, campo di applicazione e mansionario, valutazione dei rischi e delle opportunità, obiettivi sociali, piano di sviluppo delle capacità e piano di lavoro annuale. Inventario dei rischi per i diritti umani ed evidenze di due diligence, consultazioni, reclami, valutazioni dei fornitori, verifiche di conformità, comunicazioni interne ed esterne, KPI, audit, riesame della Direzione e azioni correttive.
ISO/IEC 27001:2022	Sistema di gestione della sicurezza delle informazioni	Risk management, SoA, asset, IAM, Vulnerability, incident, sviluppo sicuro, logging, fornitori, continuità	Risk assessment, piano trattamento, SoA, procedure, registri, audit, riesame, KPI, evidenze operative
ISO/IEC 27017:2015	Sicurezza dei servizi cloud SaaS e componenti cloud	Responsabilità condivise, segregazione, configurazione, logging, amministrazione, supporto, SLA, continuità e DR	Contratti/accordi, architetture, configurazioni, log, report controllo, evidenze DR, registri incidenti e cambiamenti
ISO/IEC 27018:2019	Protezione delle PII trattate in public cloud	Istruzioni del cliente, limitazione d'uso, subfornitura, cancellazione/restituzione, trasparenza, richieste e data breach	Privacy policy/informative, DPA/accordi, registri trattamenti, istruzioni, evidenze cancellazione, valutazioni privacy, incident log
ISO/IEC 42001:2023	AI Management System e sistemi AI nel perimetro approvato	Policy AI, governance use case, risk/impact assessment, verifica e validazione,	Policy AI, schede use case, validation log, fascicoli tecnici, registro criticità,

© 2024 – All Rights Reserved.

		supervisione, segnalazioni, monitoraggio e riesame	istruzioni utenti, audit, riesame, azioni correttive

© 2024 – All Rights Reserved.