CLASSIFICAZIONE DOCUMENTO: USO INTERNO

MERIDIAN GROUP

Politica SGI

Sicurezza delle Informazioni, Cloud, Privacy nei servizi cloud e Intelligenza Artificiale

Redatto da	Flavia Testa, Giulia Moretti	
Approvato da	Alessandro Moretti	
Emesso da	HR & Legal Division	
Versione	v. 2	04/06/2026

Sommario

© 2024 – All Rights Reserved.

© 2024 – All Rights Reserved.

1 Gestione del documento

1.1 Scopo del documento

La presente Politica SGI definisce gli indirizzi, i principi, gli obiettivi e gli impegni della Direzione Meridian per la protezione delle informazioni, la sicurezza dei servizi cloud, la protezione delle informazioni personali identificabili trattate in ambienti cloud e la governance dei sistemi di intelligenza artificiale.

La Politica costituisce documento di indirizzo del Sistema di Gestione Integrato e supporta la conformità agli standard ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 42001, oltre che ai requisiti normativi, regolamentari, contrattuali e organizzativi applicabili.

La Politica stabilisce criteri comuni per assicurare riservatezza, integrità, disponibilità, autenticità, responsabilità, trasparenza, supervisione, tracciabilità, controllo e miglioramento continuo nella gestione delle informazioni, dei servizi, degli asset tecnologici e dei sistemi AI.

1.2 Campo di applicazione

La Politica si applica all'intero perimetro del Sistema di Gestione Integrato Meridian, come di seguito indicato:

per la ISO/IEC 42001: Progettazione, sviluppo di una piattaforma di cyber security che utilizza modelli di intelligenza artificiale.

per la ISO/IEC 27001: Progettazione, sviluppo, erogazione e integrazione di una piattaforma di cyber security, distribuita anche in modalità Saas, ed erogazione dei relativi servizi di cyber intelligence secondo lo Statement of Applicability rev.01 del 14/04/2026. Le attività di erogazione di una piattaforma di cyber security, distribuita in modalità SaaS, sono state verificate per quanto riguarda l'applicazione dei controlli delle linee guida ISO/IEC 27017:2015, ISO/IEC 27018:2019.

La Politica si applica a personale interno, collaboratori, consulenti, fornitori, partner e altre parti interessate che accedono a informazioni, sistemi, servizi cloud, dati personali, asset tecnologici o sistemi di intelligenza artificiale riconducibili a Meridian.

Il perimetro include informazioni e dati trattati su infrastrutture interne, servizi cloud, ambienti SaaS, ambienti di sviluppo, test e produzione, sistemi di logging e monitoraggio, piattaforme di cyber intelligence, componenti AI, basi informative, prompt, output, dataset, modelli e documentazione tecnica o organizzativa.

© 2024 – All Rights Reserved.

1.3 Riferimenti normativi e documentali

Riferimento	Applicazione nella Politica
ISO/IEC 27001	Sistema di Gestione per la Sicurezza delle Informazioni e requisiti di governance, risk management, controllo, misurazione e miglioramento.
ISO/IEC 27017	Linee guida e controlli per la sicurezza delle informazioni nei servizi cloud, incluse responsabilità condivise, protezione degli ambienti cloud e gestione del rapporto tra cloud service provider e cloud service customer.
ISO/IEC 27018	Protezione delle PII nei servizi cloud pubblici, con particolare attenzione al trattamento in qualità di processor/responsabile del trattamento, ove applicabile.
ISO/IEC 42001	Sistema di gestione per l'intelligenza artificiale, governance, valutazione di impatti e rischi, responsabilità, trasparenza, supervisione e uso responsabile dei sistemi AI.
GDPR e normativa privacy applicabile	Principi di liceità, correttezza, trasparenza, minimizzazione, limitazione della finalità, sicurezza, accountability e tutela dei diritti degli interessati.

1.4 Definizioni e acronimi

Termine	Definizione
SGI	Sistema di Gestione Integrato Meridian.
ISMS / SGSI	Sistema di Gestione per la Sicurezza delle Informazioni.
AIMS	Sistema di Gestione per l'Intelligenza Artificiale.
PII	Informazione personale identificabile, riferibile direttamente o indirettamente a una persona fisica.

© 2024 – All Rights Reserved.

Termine	Definizione
Servizio cloud	Servizio digitale erogato o utilizzato tramite risorse cloud, incluso SaaS, PaaS, IaaS o componenti analoghe.
Sistema AI / use case AI	Sistema, componente, workflow o utilizzo che impiega tecniche di intelligenza artificiale per supportare attività operative, analitiche, decisionali o di generazione di contenuti.
Risk Appetite	Livello di rischio residuo che Meridian è disposta ad accettare in condizioni ordinarie, secondo soglie definite nei documenti di risk management.
Indicatore di monitoraggio	Misura quantitativa o qualitativa utilizzata per valutare l'andamento degli obiettivi del Sistema di Gestione Integrato.

1.5 Documenti operativi e registrazioni associate

La presente Politica ha natura di documento di indirizzo. Le modalità operative, le responsabilità di dettaglio, i modelli di registrazione, le schede di governo, i registri di verifica, i moduli di segnalazione, le istruzioni d'uso e le matrici di raccordo sono disciplinati, mantenuti e riesaminati all'interno delle procedure operative specifiche del SGI e dell'AIMS.

Le evidenze prodotte in applicazione della presente Politica devono essere mantenute come informazioni documentate controllate, secondo le regole aziendali di gestione documentale, conservazione, riservatezza e disponibilità.

2 Impegno della Direzione

La Direzione riconosce la sicurezza delle informazioni, la sicurezza dei servizi cloud, la protezione dei dati personali e la governance dell'intelligenza artificiale come elementi essenziali per la fiducia dei clienti, la continuità operativa, la qualità dei servizi erogati, la tutela del know-how aziendale e la conformità ai requisiti applicabili.

La Direzione si impegna a fornire risorse, ruoli, responsabilità, indirizzi, obiettivi e supporto organizzativo adeguati per mantenere e migliorare il Sistema di Gestione Integrato e per assicurare che la presente Politica sia compresa, applicata, comunicata, riesaminata e aggiornata.

- definire obiettivi integrati per sicurezza delle informazioni, cloud, privacy e AI, assicurando coerenza con il sistema di monitoraggio, responsabilità e riesame periodico;
- applicare un approccio risk-based e proporzionato nella gestione dei rischi di sicurezza, privacy, cloud e AI;

© 2024 – All Rights Reserved.

• promuovere consapevolezza, formazione, responsabilizzazione e comportamento sicuro da parte di personale, collaboratori e terze parti pertinenti;

• assicurare il miglioramento continuo mediante monitoraggio, audit, riesame della Direzione e gestione delle azioni correttive.

3 Obiettivi integrati della Politica

3.1 Finalità degli obiettivi

Gli obiettivi della presente Politica sono definiti in modo coerente con il perimetro del Sistema di Gestione Integrato e con le esigenze di monitoraggio, rendicontazione e riesame della Direzione. La loro declinazione operativa, compresa la misurazione tramite indicatori, è gestita nelle sedi organizzative e documentali previste dal SGI, evitando duplicazioni all'interno della presente Politica.

Gli obiettivi costituiscono il raccordo tra indirizzi di Direzione, valutazione dei rischi, requisiti applicabili, aspettative delle parti interessate, efficacia dei controlli e miglioramento continuo.

3.2 Obiettivi per sicurezza delle informazioni, cloud e privacy nei servizi cloud

Meridian orienta il Sistema di Gestione Integrato al perseguimento dei seguenti obiettivi di indirizzo:

• proteggere riservatezza, integrità, disponibilità, autenticità e tracciabilità delle informazioni trattate nei processi, nei servizi e negli asset tecnologici aziendali;

• assicurare che identità, autenticazioni, privilegi, accessi remoti e account amministrativi siano gestiti secondo criteri autorizzativi, tracciabili, riesaminabili e coerenti con il principio del minimo privilegio;

• mantenere configurazioni sicure, hardening, protezione da vulnerabilità e malware, logging, monitoraggio, backup, continuità e capacità di ripristino coerenti con il rischio e con gli impegni contrattuali;

• garantire gestione tempestiva di incidenti, anomalie, non conformità e azioni correttive, assicurando escalation, contenimento, comunicazione, lesson learned e verifica di efficacia;

• governare i servizi cloud e le responsabilità condivise tra Meridian, clienti, fornitori, partner e subfornitori, assicurando protezione degli ambienti, segregazione logica, portabilità, reversibilità e cancellazione sicura;

• proteggere le PII trattate in ambienti cloud secondo i principi di liceità, correttezza, trasparenza, minimizzazione, limitazione della finalità e conservazione, sicurezza, riservatezza e accountability;

• integrare sicurezza, privacy, continuità, supply chain, auditabilità e gestione documentale nei processi di progettazione, erogazione, monitoraggio, modifica e dismissione dei servizi.

© 2024 – All Rights Reserved.

3.3 Obiettivi per governance, sviluppo e uso responsabile dell'AI

Meridian orienta l'AI Management System al perseguimento dei seguenti obiettivi di indirizzo:

• assicurare che i sistemi e i casi d'uso AI siano censiti, autorizzati, documentati e riconducibili a owner, finalità, perimetro, utenti autorizzati, condizioni d'uso e limiti dichiarati;

• garantire che sviluppo, configurazione, integrazione, rilascio e modifica dei sistemi AI siano governati in modo proporzionato, riesaminabile e coerente con il contesto operativo;

• svolgere valutazioni preventive di impatto e rischio, collegando requisiti applicabili, scenari di rischio, misure di trattamento, responsabilità, decisioni di accettazione e follow-up;

• mantenere supervisione umana effettiva nei casi in cui gli output AI supportino classificazioni, valutazioni, reportistica, comunicazioni, escalation o decisioni operative rilevanti;

• assicurare qualità, provenienza, adeguatezza, sicurezza e aggiornamento di dati, basi informative, prompt, dataset, log, knowledge base e output utilizzati o generati dai sistemi AI;

• prevenire usi impropri, accessi non autorizzati, data leakage, prompt injection, allucinazioni, bias, drift, degrado delle performance e altri comportamenti non coerenti con la destinazione prevista;

• garantire verifica, validazione, re-validation, monitoraggio, segnalazione delle criticità e gestione delle anomalie dei sistemi AI secondo criteri tracciabili e proporzionati;

• assicurare trasparenza e informazioni adeguate agli utenti e alle parti interessate pertinenti sul ruolo dell'AI, sui limiti degli output, sulle modalità di supervisione e sui canali di segnalazione.

3.4 Riesame degli obiettivi e miglioramento continuo

Gli obiettivi sono riesaminati almeno annualmente e comunque in occasione di modifiche significative al contesto organizzativo, tecnologico, normativo o contrattuale, di variazioni del perimetro SGI, di incidenti o criticità rilevanti, di modifiche sostanziali ai servizi cloud o ai sistemi AI, nonché degli esiti di audit, verifiche, risk assessment e riesami della Direzione.

Gli esiti del monitoraggio alimentano il miglioramento continuo del Sistema di Gestione Integrato e possono determinare aggiornamenti a obiettivi, controlli, responsabilità, procedure, istruzioni operative, azioni di trattamento e piani di formazione o awareness.

4 Principi generali di sicurezza delle informazioni

Meridian adotta principi generali applicabili a processi, servizi, asset, dati, applicazioni, infrastrutture, sistemi cloud e sistemi AI, con l'obiettivo di garantire protezione, resilienza, auditabilità e miglioramento continuo.

© 2024 – All Rights Reserved.

• classificazione e trattamento delle informazioni in funzione della criticità, della sensibilità, del valore per il business e dei requisiti applicabili;

• controllo degli accessi basato su identità individuali, principio del minimo privilegio, segregazione dei compiti e revisione periodica dei profili autorizzativi;

• protezione dei dati mediante misure tecniche e organizzative adeguate, incluse crittografia, hardening, segmentazione, logging, monitoraggio, backup, gestione delle vulnerabilità e protezione da malware;

• gestione sicura del ciclo di vita degli asset, dei sistemi, dei dati, dei supporti, degli ambienti cloud, delle integrazioni e dei componenti software;

• gestione tempestiva degli incidenti e delle anomalie, con classificazione, escalation, contenimento, investigazione, comunicazione, lesson learned e azioni correttive;

• continuità operativa, resilienza, disponibilità dei servizi e capacità di ripristino coerenti con i requisiti contrattuali, di business e di sicurezza;

• gestione dei fornitori e delle terze parti sulla base di requisiti di sicurezza, privacy, cloud, AI, continuità, auditabilità e responsabilità contrattuali;

• miglioramento continuo tramite obiettivi misurabili, audit interni, riesame della Direzione, trattamento delle non conformità e monitoraggio delle performance del Sistema di Gestione.

5 Principi specifici per sicurezza cloud e protezione delle PII nei servizi cloud

5.1 Sicurezza dei servizi cloud

Meridian assicura che l'uso, la progettazione e l'erogazione di servizi cloud siano governati secondo responsabilità definite e tracciabili. In funzione del contesto, Meridian può operare come cloud service provider, cloud service customer o entrambe le cose; in ogni caso, le responsabilità di sicurezza devono essere chiarite, documentate e mantenute coerenti con accordi contrattuali, requisiti di servizio e controlli applicabili.

• definire e comunicare responsabilità condivise tra Meridian, clienti, fornitori cloud, partner e subfornitori, incluse responsabilità su configurazioni, identità, logging, backup, incidenti, continuità e cancellazione dei dati;

• proteggere ambienti cloud e virtualizzati tramite segregazione logica, gestione sicura delle configurazioni, hardening, controllo degli accessi privilegiati, monitoraggio e gestione delle vulnerabilità;

• assicurare che provisioning, modifica, migrazione e dismissione dei servizi cloud siano autorizzati, documentati e verificabili;

• gestire in modo controllato account amministrativi, interfacce di gestione, chiavi, segreti, API e integrazioni tra servizi;

© 2024 – All Rights Reserved.

• mantenere log e informazioni di monitoraggio adeguate per rilevare eventi, anomalie, accessi non autorizzati, degradi di servizio e incidenti;

• prevedere misure di continuità, backup, ripristino, portabilità, reversibilità e cancellazione sicura coerenti con gli impegni contrattuali e con il ciclo di vita del servizio.

5.2 Protezione delle PII nei servizi cloud

Meridian protegge le PII trattate in ambienti cloud secondo i principi privacy applicabili e secondo le responsabilità definite nei rapporti contrattuali con clienti, fornitori e subfornitori. Quando Meridian opera quale responsabile del trattamento/processor per conto del cliente, tratta le PII esclusivamente sulla base delle istruzioni documentate e delle finalità autorizzate.

• trattare dati personali solo per finalità determinate, esplicite e autorizzate, evitando trattamenti ulteriori incompatibili o non richiesti dal cliente/titolare;

• applicare minimizzazione, limitazione della conservazione, segregazione logica e misure di sicurezza commisurate alla natura dei dati e al contesto del trattamento;

• supportare, nei limiti del ruolo ricoperto, la gestione delle richieste degli interessati, degli obblighi di informazione, delle valutazioni privacy e delle verifiche richieste dal cliente/titolare;

• disciplinare contrattualmente il ricorso a sub-responsabili o fornitori che trattano PII, assicurando requisiti di sicurezza, riservatezza, localizzazione, trasferimento, auditabilità e notifica delle modifiche rilevanti;

• prevedere restituzione, cancellazione o anonimizzazione delle PII al termine del rapporto o quando non più necessarie, secondo istruzioni documentate e requisiti applicabili;

• notificare e gestire tempestivamente violazioni, anomalie o incidenti che interessano PII secondo ruoli, tempi, canali e responsabilità definiti nelle procedure applicabili.

6 Principi specifici per governance, sviluppo e uso responsabile dell'AI

6.1 Principi guida AI

Meridian promuove lo sviluppo, l'adozione e l'utilizzo di sistemi AI secondo principi di responsabilità, controllo umano, sicurezza, trasparenza, qualità, affidabilità, conformità, proporzionalità e tutela degli stakeholder.

• i sistemi AI devono essere utilizzati solo per finalità legittime, determinate, coerenti con il contesto di impiego e compatibili con le regole aziendali applicabili;

• i sistemi AI devono essere sviluppati o configurati in modo coerente con le finalità dichiarate, il contesto d'uso previsto e le esigenze di controllo organizzativo;

© 2024 – All Rights Reserved.

• le decisioni di governance AI devono essere proporzionate alla rilevanza del sistema AI, al suo contesto di utilizzo e ai possibili impatti sul business, sui clienti, sui processi e sulle parti interessate;

• le decisioni relative ad adozione, sviluppo, aggiornamento e uso dei sistemi AI devono essere riconducibili a responsabilità organizzative identificate e supportate da adeguata tracciabilità documentale;

• la governance AI deve essere mantenuta coerente con il framework aziendale di sicurezza, privacy, qualità, risk management e compliance.

6.2 Sviluppo responsabile dei sistemi AI

Ogni iniziativa di sviluppo, addestramento, configurazione significativa o integrazione di un sistema AI deve essere riferita a una finalità organizzativa chiara, approvata e coerente con lo scopo dell'AIMS. Le principali assunzioni di sviluppo, il perimetro funzionale, le limitazioni note e il ruolo dell'intervento umano devono essere documentabili e riesaminabili.

• definizione dei requisiti del sistema AI, incluse finalità, destinazione prevista, contesto di utilizzo, utenti, fonti, input, output, limiti, requisiti di sicurezza, privacy, qualità, compliance e supervisione umana;

• progettazione, sviluppo o configurazione responsabili, con identificazione dei punti di controllo, dei ruoli decisionali, delle condizioni di verifica aggiuntiva e dei casi di sospensione o rivalutazione;

• verifica e validazione prima del rilascio o dell'uso operativo, nonché in occasione di modifiche sostanziali;

• autorizzazione all'uso solo quando finalità, requisiti, validazione, ruoli di supervisione, utilizzatori autorizzati, condizioni d'uso e limiti siano stati formalizzati e siano disponibili le evidenze minime richieste;

• riesame delle modifiche significative riguardanti modello, dati, logica di funzionamento, criteri di classificazione, fonti, componenti rilevanti, contesto di utilizzo, output, integrazioni o modalità di supervisione.

6.3 Uso responsabile e supervisione umana

I sistemi AI devono essere utilizzati in coerenza con finalità, limiti e condizioni d'uso definiti da Meridian per ciascun caso d'uso approvato. L'output AI supporta, e non sostituisce indebitamente, il giudizio professionale umano nei processi in cui siano richieste valutazioni, classificazioni, comunicazioni, reportistica o decisioni operative.

• l'uso dei sistemi AI deve avvenire da parte di soggetti autorizzati o legittimati, con adeguata consapevolezza del ruolo dello strumento AI nel processo operativo;

• deve essere mantenuto un livello di supervisione umana coerente con il contesto di utilizzo e con il rischio del sistema AI;

• non è consentito utilizzare sistemi AI per finalità diverse da quelle approvate, in contesti non valutati, come sostituto non autorizzato del giudizio professionale o in presenza di anomalie che ne rendano non appropriato l'impiego;

© 2024 – All Rights Reserved.

• le informazioni agli utenti devono includere scopo del sistema, modalità corrette di utilizzo, limiti principali, ruolo della supervisione umana, divieti di utilizzo e canali di supporto o segnalazione;

• criticità, anomalie, usi impropri, degradi di performance, reclami o carenze informative devono essere segnalati, valutati, tracciati e gestiti secondo le procedure applicabili.

7 Risk management, Risk Appetite e trattamento

Meridian adotta un approccio integrato e risk-based per identificare, analizzare, valutare, trattare, monitorare e riesaminare rischi relativi a sicurezza delle informazioni, cloud, privacy e AI. Le valutazioni devono considerare impatti su clienti, processi, servizi, continuità operativa, conformità, diritti e libertà degli interessati, affidabilità dei sistemi AI e responsabilità contrattuali.

I rischi sono trattati mediante misure tecniche, organizzative, procedurali o contrattuali proporzionate alla classe di rischio e all'appetito al rischio approvato. Il trattamento può prevedere mitigazione, monitoraggio, accettazione motivata o sospensione/evitamento, secondo le regole definite nei documenti di risk management.

Gli obiettivi del SGI e gli indicatori di monitoraggio approvati sono utilizzati per misurare l'efficacia dei controlli, verificare l'allineamento dei rischi residui al Risk Appetite, monitorare l'avanzamento delle azioni di trattamento e supportare il riesame della Direzione.

8 Ruoli e responsabilità

Ruolo / funzione	Responsabilità di indirizzo
Direzione	Approva la Politica, assicura risorse e indirizzi, riesamina le performance del SGI e assume le decisioni sui rischi non accettabili o sulle azioni prioritarie.
Responsabile del Sistema di Gestione / Chief Quality Officer	Coordina il mantenimento del SGI, il monitoraggio degli obiettivi, audit, riesami, non conformità e azioni di miglioramento.
Information Security Manager	Presidia la sicurezza delle informazioni, il controllo degli accessi, logging, incidenti, vulnerabilità, continuità e verifiche tecniche di sicurezza.
Chief Technology Officer / IT Manager	Garantisce l'attuazione tecnica dei controlli su infrastrutture, servizi cloud, backup, ripristino, hardening, patching, logging e disponibilità.
DPO / funzione privacy	Presidia gli aspetti privacy, PII, DPIA ove applicabili, accordi privacy con fornitori, richieste degli interessati

© 2024 – All Rights Reserved.

Ruolo / funzione	Responsabilità di indirizzo
	e valutazioni su incidenti con potenziale impatto privacy.
AI Risk & Compliance / CAIO / AIMS Manager	Presidia governance AIMS, censimento sistemi AI, impact assessment, risk assessment AI, allineamento ai requisiti ISO/IEC 42001, monitoraggio degli indicatori AI e riesame dei casi d'uso.
Owner del sistema AI / Risk Owner	Assicura che ciascun sistema AI sia definito, autorizzato, utilizzato, monitorato e riesaminato in coerenza con finalità, limiti, controlli, evidenze e azioni di trattamento approvate.
HR Manager	Supporta formazione, consapevolezza, presa visione delle policy e istruzioni operative, inclusa awareness su sicurezza e AI.
Fornitori, partner e subfornitori	Rispettano gli obblighi contrattuali e le regole applicabili in materia di sicurezza, privacy, cloud, AI, continuità, riservatezza e segnalazione di incidenti o anomalie.

9 Comunicazione, formazione e consapevolezza

La presente Politica è comunicata internamente e resa disponibile alle parti interessate pertinenti secondo criteri di appropriatezza, riservatezza e necessità di conoscenza. Il personale e le terze parti pertinenti devono essere informati delle regole applicabili al proprio ruolo e alle attività svolte.

Meridian promuove programmi di formazione e consapevolezza relativi a sicurezza delle informazioni, privacy, cloud e uso responsabile dell'AI. La partecipazione, la presa visione e il completamento dei percorsi formativi sono tracciati tramite registrazioni controllate e verifiche periodiche.

10 Monitoraggio, misurazione, audit e riesame

Meridian misura le performance del SGI attraverso indicatori approvati, audit interni, verifiche di conformità, riesami periodici, analisi di incidenti, gestione delle non conformità, andamento dei rischi e stato delle azioni di trattamento.

Il riesame della Direzione valuta almeno adeguatezza della Politica, raggiungimento degli obiettivi, efficacia dei controlli, risultati degli audit, stato di non conformità e azioni correttive, andamento dei rischi, cambiamenti interni ed esterni, evoluzione normativa e tecnologica e opportunità di miglioramento.

© 2024 – All Rights Reserved.

Gli obiettivi e gli indicatori di monitoraggio devono essere riesaminati almeno annualmente e in occasione di modifiche significative al perimetro SGI, al contesto organizzativo, ai sistemi cloud o AI, ai requisiti applicabili, ai rischi, agli incidenti o alle criticità rilevanti.

11 Gestione delle deroghe, delle non conformità e delle criticità

Eventuali deroghe alle regole della presente Politica devono essere motivate, valutate, approvate da ruoli competenti, limitate nel tempo, associate a rischi residui identificati e, ove necessario, compensate da misure alternative.

Non conformità, rilievi di audit, anomalie, incidenti, reclami, segnalazioni AI e criticità documentali devono essere registrati, valutati, assegnati a owner, trattati con azioni correttive o preventive e verificati in termini di efficacia.

Per i sistemi AI, le criticità possono riguardare output anomali, degrado di performance, errori sistematici, usi impropri, carenze informative, limiti non adeguatamente comunicati, problemi di supervisione, bias, allucinazioni, prompt injection, data leakage o comportamenti non coerenti con il contesto d'uso approvato.

12 Approvazione e validità

La presente Politica entra in vigore dalla data di approvazione e rimane valida fino a successiva revisione. La Politica è riesaminata almeno annualmente e comunque in occasione di modifiche significative del perimetro SGI, degli standard applicabili, dell'organizzazione, dei servizi, dei sistemi AI, dei rischi, degli incidenti o degli esiti di audit.

Con l'approvazione della presente Politica, Meridian conferma il proprio impegno al rispetto dei requisiti applicabili, alla protezione delle informazioni, alla sicurezza dei servizi cloud, alla protezione delle PII nei servizi cloud, alla governance responsabile dell'intelligenza artificiale e al miglioramento continuo del Sistema di Gestione Integrato.

© 2024 – All Rights Reserved.