MAPS GROUP
SHARING KNOWLEDGE

Politica integrata qualità e sicurezza delle informazioni

Maps SpA, Artexe SpA, SCS Computers Srl e Iasi Srl (l'Organizzazione) sono Software Solutions Providers che sostengono e supportano la Digital Transformation di enti e aziende attraverso la produzione e distribuzione di soluzioni che consentono ai clienti di prendere decisioni migliori e di rivedere i propri modelli di business.

In campo sanitario si ispirano ad un nuovo modello di approccio che pone il cittadino al centro dell'intero processo di erogazione dei servizi, al fine di guidare le Aziende clienti verso un miglioramento continuo dei~~l~~ propri servizi.

L'Organizzazione fonda la sua politica sui valori esplicitamente espressi nel codice etico:

- Integrità di comportamento e rispetto di Leggi e Regolamenti;
- Ripudio di ogni discriminazione e tutela delle diversità;
- Centralità, sviluppo e valorizzazione delle risorse umane;
- Trasparenza ed etica degli affari;
- Innovazione;
- Qualità, sicurezza e riservatezza dei dati;
- Legalità e contrasto al terrorismo e alla criminalità;
- Approccio al *business* e crescita sostenibile;

Inoltre, rappresenta un elemento fondamentale della politica della qualità l'affermazione di una cultura costruttiva dell'errore poiché anche l'errore, se correttamente gestito, è funzionale ad un'ottica di miglioramento.

L'Organizzazione intende proseguire nel processo di integrazione dei propri sistemi ISO 9001 e ISO IEC 27001. Gli obiettivi che si prefigge con un Sistema Integrato ISO 9001 e ISO IEC 27001 sono:

- La soddisfazione dei clienti attraverso:
  - il miglioramento continuo dei prodotti, dei sistemi SW e HW e dei servizi ad essi connessi
  - soluzioni sempre adeguate alle loro aspettative ed esigenze attraverso elevati livelli di personalizzazione ed innovazione
  - rapporto qualità prezzo
  - affidabilità del servizio
- Ritagliarsi un ruolo primario in alcuni spazi di mercato che si stanno aprendo con la Digital Transformation, configurandosi come "pionieri";
- Consolidare il proprio posizionamento nell'ambito dello sviluppo dei progetti software;
- Un approccio alle attività sistematicamente orientato alla qualità da parte di tutti i dipendenti e collaboratori;
- La definizione di modalità operative trasparenti, perché documentate e descritte e quindi condivise nei contenuti da tutti i collaboratori;
- L'agevolazione del trasferimento del know-how, grazie alla descrizione e documentazione dei processi lavorativi.
- Favorire il mutuo beneficio dei vari stakeholder.

L'Organizzazione considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo e un fattore di valenza strategica trasformabile in vantaggio competitivo. Siamo consapevoli del fatto che le nostre attività di progettazione e sviluppo per soggetti esterni e l'utilizzo di nostre soluzioni possono comportare l'affidamento di dati e informazioni critiche e per questo motivo intendiamo adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza e la disponibilità sia del patrimonio informativo interno che di quello affidato dai nostri Clienti.

Su tale linea l'Organizzazione ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento in conformità anche alle indicazioni della norma internazionale ISO IEC 27001, nell'ottica di promuovere attraverso il SGSI il miglioramento continuo delle prestazioni del sistema.

L'obiettivo generale del Sistema di Gestione per la Sicurezza delle Informazioni dell'Organizzazione è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione e sviluppo di progetti, nella realizzazione e fruizione di soluzioni proprietarie e nella erogazione dei rispettivi servizi attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali le attività stesse sono soggette, privilegiando i seguenti requisiti di sicurezza:

- Riservatezza, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi
- Integrità, ovvero la proprietà dell'informazione di rimanere "integra", tramite la riduzione a livelli accettabili del rischio che possano avvenire cancellazioni o modifiche di informazioni a seguito di interventi di entità non autorizzate o del verificarsi di fenomeni non controllabili
- Disponibilità, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi

Inoltre, con la presente politica l'Organizzazione intende formalizzare i seguenti obiettivi specifici nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine dell'Organizzazione quale fornitore affidabile e competente
- Proteggere il proprio patrimonio informativo
- Evitare al meglio ritardi nella delivery
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalizzazione
- Rispondere pienamente alle indicazioni della normativa vigente e cogente
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza su temi di sicurezza informatica

Per conseguire tali obiettivi abbiamo stabilito procedure, strumenti e responsabilità per le attività cruciali del sistema, quali:

- protezione e classificazione di tutte le informazioni
- disponibilità pronta delle informazioni alle persone effettivamente coinvolte
- sistematica analisi del rischio connesso alla gestione delle informazioni, ad ogni variazione dell'Organizzazione e per ogni commessa
- definizione delle responsabilità di gestione sicura dei dati e delle informazioni, ad ogni livello gestionale

Maps Group, inoltre al fine di garantire la sicurezza del cloud computing e proteggere le informazioni dei Clienti archiviate e gestite in Cloud, in conformità dello standard ISO/IEC 27017:2015, identifica:

- I ruoli e responsabilità sulla gestione della sicurezza del servizio cloud: L'attribuzione delle responsabilità e dei ruoli relativi alla sicurezza del cloud computing è specificamente identificata tramite un accordo, di condivisione o suddivisione delle responsabilità, in carico al cliente e al fornitore, identificato, registrato e comunicato in modo chiaro. Il cliente del servizio cloud è responsabile per tutti gli aspetti delle soluzioni di sicurezza e gestione del servizio erogato qualora non specificamente indicata la responsabilità del fornitore di servizio. I fornitori di cloud e i clienti di servizi cloud sono ciascuno responsabili per problemi nelle funzioni sotto il loro controllo. Alcune responsabilità possono inoltre essere condivise tra cliente e fornitore;
- Le informazioni archiviate nell'ambiente del Cloud a cui il Cliente può avere accesso e che sono gestite dal Fornitore del servizio Cloud;
- gli asset mantenuti sul Cloud (applicazioni);
- i processi in multi-tenant che si possono svolgere nel Cloud virtuale (se presenti);
- gli utenti del Cloud ed il contesto in cui essi utilizzano il servizio;
- gli amministratori del servizio Cloud dei Clienti che hanno un accesso privilegiato;
- la localizzazione geografica del Provider del Cloud ed i Paesi in cui quest'ultimo può archiviare i dati relativi al Cloud (anche temporaneamente). I requisiti base di sicurezza delle informazioni applicabili alla progettazione ed alla implementazione del servizio Cloud;
- I rischi derivanti da addetti ai lavori autorizzati;
- accesso agli asset del Cliente da parte del Provider ;
- procedure per il controllo accessi;
- comunicazioni con il Cliente durante il change management;

- allineamento e sicurezza degli ambienti virtuale e cloud;
- accesso ai dati del Cliente del servizio Cloud e loro protezione;
- gestione del ciclo di vita dell'account del Cliente;
- comunicazione di Data Breach e linee guida per la condivisione delle informazioni, per aiutare le investigazioni.

Maps Group, inoltre assicura il rispetto dei principi di sicurezza dei dati e delle informazioni nella gestione del cloud computing sanciti dal Regolamento UE 679/2016, e garantisce l'implementazione dei controlli richiesti per il trattamento di dati personali implementando adeguate misure di protezione, nel rispetto dei requisiti previsti dalla ISO/IEC 27018:2019:

Scelta e Consenso: agevolazione dell'esercizio dei diritti di accesso, rettifica e/o cancellazione da parte dell'interessato, attraverso le indicazioni specificate nel contratto.
Finalità del trattamento: le finalità del trattamento sono rese note nel contratto di servizio.
Minimizzazione dei dati: file e documenti temporanei sono cancellati o distrutti entro un periodo specificato e documentato.
Limitazione all'uso, alla conservazione e alla divulgazione: Non avviene la divulgazione di dati personali a terze parti. La richiesta di divulgazione di dati personali da parte di autorità amministrative o giudiziarie è notificata al cliente in maniera tempestiva, ove consentito dalla legge.
Trasparenza: il ricorso a subappaltatori da parte del provider è reso noto al cliente del servizio Cloud prima del loro utilizzo. Le disposizioni per l'utilizzo dei subappaltatori sono riportate in chiaro nel contratto tra il provider e il cliente. Il provider informa il cliente in modo tempestivo di eventuali modifiche previste in questo senso.
Accountability: In caso di violazioni che comportano perdite, diffusione o modifica dei dati personali (data breach), effettua la notifica tempestivamente al cliente attraverso un processo interno di Incident Management.
Conformità alla privacy: il provider indica i Paesi in cui sono conservati i dati, anche derivanti dall'utilizzo di subappaltatori e indica specifici accordi contrattuali applicati in merito al trasferimento internazionale di dati. Il provider informa tempestivamente il cliente di eventuali modifiche previste a tale riguardo.

Le figure chiave che partecipano al conseguimento degli obiettivi sono le seguenti:

IL PERSONALE DIPENDENTE

Attua le procedure in osservanza di questa policy e provvede alla segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

LA DIREZIONE

Ha il compito di fissare gli obiettivi, assicurare un indirizzamento chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di sicurezza. Promuove la sicurezza garantendo la congruità dei singoli budget, coerentemente alle politiche e alle linee strategiche aziendali definite.

RESPONSABILE DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni ed in particolare di:

a) emanare tutte le norme necessarie, ivi inclusa la tipologia di classificazione dei documenti, affinché l'Organizzazione possa condurre, in modo sicuro, le proprie attività
b) adottare criteri e metodologie per l'analisi e la gestione del rischio
c) suggerire le misure di sicurezza organizzative, procedurali e tecnologiche a tutela della sicurezza e continuità delle attività
d) pianificare un percorso formativo, specifico e periodico in materia di sicurezza per il personale
e) controllare periodicamente l'esposizione dei servizi dalle principali minacce
f) verificare gli incidenti di sicurezza e adottare le opportune contromisure
g) promuovere la cultura relativa alla sicurezza delle informazioni

TUTTI I SOGGETTI ESTERNI

I fornitori (di beni e di servizi) che intrattengono rapporti con l'Organizzazione devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di idonee clausole contrattuali all'atto del conferimento dell'incarico.

La direzione verificherà periodicamente l'efficacia e l'efficienza del Sistema di Governo per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business dell'Organizzazione, al fine di garantire il suo corretto adeguamento.

Parma 31/01/2024

Indice di revisione - data	Motivazione della revisione e parti revisionate	Redatto/Verificato	Approvato
08/03/2021	Prima edizione	Sara Magri Franco Iorio	Marco Ciscato
04/01/2022	Seconda edizione	Giovanni Betuzzi Franco Iorio	Marco Ciscato
08/02/2023	Inserito nell'ambito di certificazione SCS Computers	Giovanni Betuzzi Franco Iorio	Marco Ciscato