POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

INTRODUZIONE

La diffusione delle tecnologie ICT a tutti i livelli della società comporta un aumento dei rischi per la sicurezza in termini di perdita di dati, intrusioni, perdita della riservatezza e violazioni della privacy, e ciò vale in particolare per i sistemi informatici, richiedendo pertanto una accurata analisi delle loro debolezze e delle possibilità di un loro utilizzo non sicuro. L'implementazione di un adeguato sistema di protezione delle informazioni si basa su una sistematica analisi delle possibili minacce, e sulla determinazione delle precauzioni da adottare. Nel seguito del documento con la sigla ACCA ci si riferisce a tale Business Unit.

RIFERIMENTI NORMATIVI

ISO/IEC 27000	Information Technology – Security Techniques – Information Security Management Systems – Overview and vocabulary
ISO/IEC 27001	Information Technology – Security Techniques – Information Security Management Systems – Requirements
ISO/IEC 27002	Information Technology – Security Techniques – Code of practice for Information Security Management
ISO/IEC 27017	Information Technology – Security Techniques – Code of practice for Information Security Controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	Information Technology – Security Techniques – Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

POLITICA

GENERALITA'

La ACCA software S.p.a. ha in carico la seguente missione:

Progettazione, sviluppo, distribuzione ed assistenza di pacchetti applicativi software. Organizzazione e realizzazione di corsi di formazione, supporti formativi multimediali ed e-learning, nel settore dell'edilizia. Progettazione, sviluppo e fornitura di programmi e servizi on-line e on-web. Realizzazione e gestione di banche dati tecniche e normative.

ACCA tratta quindi dati pubblici e riservati, dati anonimi, personali comuni o sensibili, anche ad alta criticità. Essi includono anche quelli relativi al personale e alla tutela della privacy.

Data la potenziale criticità dei dati trattati, in qualunque formato essi siano (informatico e non), è fondamentale che sia loro garantita la massima riservatezza, integrità e disponibilità.

I livelli di sicurezza da garantire devono essere tali da rispettare le clausole contrattuali e la normativa vigente, nonché la coerenza ed il bilanciamento tra:

- Rischio di impresa
- Sostenibilità economica
- Risultati delle analisi e delle valutazioni del rischio
- Politiche, codici di condotta e strategie aziendali nei confronti di dipendenti, clienti e fornitori

Le politiche ACCA, già definite nell'ambito dei Sistemi di Gestione per la Qualità, l'Ambiente e la Sicurezza e Salute dei Lavoratori, sono improntate al costante adeguamento del contesto in cui si opera ed al miglioramento dell'efficacia ed efficienza dei processi, delle prestazioni e dei controlli di sicurezza.

Di seguito sono elencati i diversi principi cardine sui quali è improntata la presente politica:

- Rispetto dei requisiti legali, delle norme tecniche e delle prescrizioni contrattuali riguardanti la sicurezza delle informazioni.
- Le informazioni devono essere accessibili solo a coloro che ne hanno necessità (principio *"need to know"*) e nei tempi stabiliti.
- Il personale deve essere opportunamente coinvolto e formato in materia di sicurezza delle informazioni, e deve seguire i princìpi etici e comportamentali prescritti e condivisi.
- I Fornitori devono essere opportunamente tenuti sotto controllo; i rapporti tra ACCA e le aziende fornitrici di prodotti e servizi devono essere basati su una contrattualistica che tenga conto delle aspettative di entrambe le parti e della chiara definizione degli accordi commerciali, delle tempistiche e dei requisiti e responsabilità tecniche ed organizzative, includenti quelli relativi alla protezione delle informazioni.
- La natura dei servizi erogati richiede già di per sé di tenere in considerazione i requisiti di sicurezza sin dalla contrattazione con i Clienti.

La responsabilità finale della sicurezza delle informazioni è in carico alla Direzione, che delega i Responsabili ad attuare quanto necessario, e secondo specifici Organigrammi, in accordo con il Responsabile dei Sistemi IT ed il Responsabile delle Risorse Umane.

Pur essendo la *governance* delegata a diverse funzioni, la Direzione mantiene la responsabilità per fornire gli indirizzi strategici e fornire le risorse necessarie.

COMUNICAZIONE E REVISIONE DELLA POLITICA

La Direzione di ACCA Software definisce, divulga e si impegna a far comprendere e mantenere attiva la presente Politica per la Gestione della Sicurezza delle Informazioni. La divulgazione può avvenire tramite affissione in bacheca o tramite pubblicazione sulla intranet aziendale.

Essa è volta a garantire la tutela e la protezione da minacce, di origine interna o esterna, di natura accidentale o intenzionale, alle quali sono soggette le informazioni nell'ambito delle attività che rientrano nel Campo di Applicazione del Sistema di Gestione, in accordo con lo standard ISO/IEC 27001 e con le linee guida dello standard ISO/IEC 27002.

La Politica deve essere applicata a tutti i livelli in azienda, e deve essere parte degli accordi che l'azienda stipula con qualsiasi soggetto interno o esterno che risulti coinvolto nel trattamento delle informazioni che rientrano nel Campo di Applicazione del Sistema di Gestione. A tal fine, la presente Politica deve essere trasmessa, quando necessario, anche alle parti esterne (Clienti, Fornitori, Organi di vigilanza e controllo), interessate alla gestione in sicurezza delle informazioni.

La politica della sicurezza delle informazioni viene riesaminata almeno annualmente per verificare l'adeguatezza, ed aggiornata se necessario.

In particolare, l'aggiornamento della Politica e delle prassi operative è indispensabile laddove in fase di Riesame della Direzione si identifichino:

- Evoluzioni significative del business
- Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio
- Significativi incidenti di sicurezza
- Nuovi requisiti e pressioni da parte dei mercati di riferimento
- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni

In particolare, le attività dell'azienda poggiano sul presupposto di un Sistema ICT sicuro e correttamente funzionante. Quasi tutte le informazioni presenti sono salvate e processate in formato elettronico. Le risorse ICT non sono immuni da vulnerabilità, pertanto è necessario effettuare una dettagliata catalogazione degli asset informatici, nonché una pianificazione e controllo della loro sicurezza.

La Strategia di Sicurezza ICT è divisa nei seguenti ambiti:

- Aspetti organizzativi di Sicurezza ICT (organizzazione, personale)
- Sicurezza delle infrastrutture (per esempio: data center, IDF rooms)
- Sicurezza dei supporti fisici ICT (per esempio: server, clients, componenti di rete)
- Sicurezza della rete (network and system management)
- Account Management, ovvero corretta gestione degli Accessi
- Sicurezza nelle applicazioni (per esempio: E-Mail, etc.)

SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Il punto di partenza per definire i requisiti di un Sistema di Gestione per la Sicurezza delle Informazioni consiste nell'identificare le possibili minacce presenti. Le minacce sono da un lato dipendenti dall'ambiente operativo, dall'altro dalla sensibilità delle informazioni che vengono gestite.

Esse possono essere suddivise in diverse tipologie di eventi:

1) Modifiche non autorizzate delle informazioni (perdita di Integrità)
2) Accessi non autorizzati alle informazioni (perdita di Riservatezza)
3) Impatti non previsti o non autorizzati sulla funzionalità del Sistema (perdita di Disponibilità)
4) Informazioni provenienti da fonti non affidabili (perdita di Autenticità)
5) Perdita del controllo sui dati personali (perdita di Privacy)

Una corretta gestione delle informazioni, in particolare quelle presenti su supporto informatico, è una condizione basilare per garantire e mantenere gli obiettivi fissati di Integrità, Riservatezza, Disponibilità, Autenticità e Privacy delle Informazioni.

Il mancato soddisfacimento di adeguati livelli di sicurezza porta a conseguenze molto negative:

- Danneggiamento dell'immagine aziendale
- Mancata soddisfazione del Cliente
- Sanzioni dovute al mancato rispetto della normativa vigente
- Fuga di informazioni sensibili e di know-how dall'azienda
- Danni economici e finanziari

Le regole, le procedure, le disposizioni organizzative e le responsabilità definite per conseguire gli obiettivi di Integrità, Riservatezza, Disponibilità, Autenticità e Privacy delle Informazioni, costituiscono la base del Sistema di Gestione implementato dall'azienda.

Per identificare le esigenze per la sicurezza, l'Azienda valuta periodicamente i rischi, allo scopo di determinare il livello di esposizione delle informazioni alle varie minacce presenti. I risultati di tale valutazione determinano le azioni da intraprendere, i controlli e le misure di sicurezza da adottare.

OBIETTIVI DELLA POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

1) Acquisire piena conoscenza e consapevolezza delle informazioni gestite e valutazione della loro criticità, al fine di determinare ed implementare gli adeguati livelli di protezione.
2) Realizzare una catalogazione degli asset aziendali rilevanti ai fini della gestione delle informazioni, individuando, per ciascuno di essi, un Responsabile.
3) Classificare le informazioni sulla base di determinati livelli di criticità.
4) Garantire l'accesso sicuro alle informazioni, in funzione di determinate matrici di autorizzazione, in modo da prevenirne l'accesso a chi non dispone dei diritti necessari.
5) Garantire l'accesso alle sedi ed ai singoli locali aziendali esclusivamente al Personale Autorizzato, a protezione della sicurezza degli ambienti e degli asset aziendali ivi presenti.
6) Definire procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni, includendo gli aspetti di sicurezza anche in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
7) Implementare un sistema di collaborazione e di consapevolezza tra l'organizzazione e le terze parti interessate, in modo da trattare le informazioni ad adeguati livelli di sicurezza.
8) Riconoscere con tempestività Incidenti e Anomalie, inclusi quelli riguardanti i Sistemi Informativi, gestendoli secondo procedura ed implementando adeguati sistemi di prevenzione.
9) Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con terze parti.
10) Garantire la Business Continuity aziendale ed il Disaster Recovery, attraverso l'adozione e l'applicazione di adeguate procedure di sicurezza.
11) Garantire la riservatezza, l'integrità e la disponibilità dei dati archiviati, accessibili e manipolati utilizzando i servizi di cloud computing.
12) Stabilire un quadro di responsabilità e azioni necessarie per soddisfare i requisiti normativi e le linee guida di sicurezza per il cloud computing.