GRUPPO MASTROTTO

POLITICA
GRUPPO MASTROTTO S.p.A.

P7013G

SICUREZZA DELLE INFORMAZIONI

Natura della revisione: Prima emissione

- ☐ politica controllata n°.....
- ☐ politica non controllata

	Redatta: Ufficio ICT	Verificata da: GCFO	Approvata da: CdA	
Firma				
Date	**22/12/2022**	**19/06/2023**	inizio applicabilità	**24/07/2023**

Indice

Premessa

Le *Informazioni*, in ogni loro forma (stampata, scritta, memorizzata, scambiata e trasmessa con differenti strumenti, etc.), sono elementi di valore strategico, fondamentali per l'efficacia, la continuità ed il successo del business aziendale. Ogni *informazione* è pertanto un bene da proteggere, a partire dalla sua creazione e durante tutto il suo ciclo di vita, mediante politiche ed azioni di gestione mirate, nel rispetto dei requisiti normativi applicabili e della tutela dei valori e dell'immagine aziendale.

In particolare, tutte le tipologie di informazioni finanziarie, commerciali, tecniche o contrattuali relative a clienti, partner e dipendenti sono riconosciute dalla società Gruppo Mastrotto S.p.A. (in seguito anche "Gruppo Mastrotto") come risorse strategiche.

I sistemi tecnologici che processano, archiviano e trasmettono tali informazioni sono elementi chiave in ogni processo di business: dall'affidabilità di tali sistemi dipendono la qualità del servizio fornito ai Clienti, le prestazioni, l'innovazione, la capacità di crescita e, in ultima analisi, la sostenibilità del Gruppo Mastrotto.

La salvaguardia di tale complesso patrimonio di risorse informative richiede l'individuazione e l'adozione di misure adeguate di sicurezza - di natura organizzativa, tecnologica ed operativa - in grado di minimizzare i rischi di accessi non autorizzati, di alterazione, di indisponibilità, di divulgazione, di perdita o di distruzione, sia accidentali che dolosi.

Per raggiungere l'obiettivo, il Gruppo Mastrotto deve adottare un approccio strutturato, consistente in un insieme organico di norme per la sicurezza delle informazioni ed in un processo stabile e ripetibile di gestione, misura e controllo del relativo livello di attuazione.

Il risultato è un sistema di gestione della sicurezza delle informazioni in grado di guidare, a tutti i livelli, i comportamenti e le scelte tecnologiche per garantire nel tempo la costante tutela delle informazioni aziendali e dei sistemi informativi funzionali ai processi di business.

1. Scopo

Il presente documento ha l'obiettivo di definire le linee di indirizzo per la gestione della Sicurezza delle Informazioni del Gruppo Mastrotto, fornendo un'adeguata protezione del patrimonio informativo aziendale e garantendo la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informativi del Gruppo Mastrotto, al fine di proteggerli da minacce interne o esterne, intenzionali od accidentali.

All'interno della presente Politica, in linea con i requisiti di business del Gruppo Mastrotto ed in conformità con la normativa cogente, gli standard internazionali e le best practice applicabili, vengono stabiliti:

- i Principi generali di Sicurezza delle Informazioni;
- i Ruoli e Responsabilità per il governo della Sicurezza delle Informazioni;
- gli obiettivi, in funzione della tutela e della continuità del business del Gruppo Mastrotto.

1.1. Principi generali

Il personale del Gruppo Mastrotto è tenuto ad osservare le modalità e i principi esposti nel presente documento, le pertinenti norme di legge e regolamentari vigenti e applicabili e la pertinente documentazione organizzativa e normativa vigente e applicabile. Il non rispetto di quanto sopra comporta la sanzione da parte di Gruppo Mastrotto tramite l'applicazione del sistema disciplinare aziendale.

In particolare, devono essere osservati i seguenti principi generali:

- le informazioni sono una componente strategica del patrimonio aziendale in quanto costituiscono elemento fondamentale su cui si basano tutti i processi aziendali. A tal fine il patrimonio informativo deve essere tutelato e gestito in termini di disponibilità, integrità e riservatezza al fine di:
  - garantire che i processi aziendali possano operare in maniera efficace ed efficiente;
  - evitare eventi a impatto negativo sul business (perdita di reputazione, perdita di fiducia dei clienti, perdita di *know how*, danni economici, problematiche legali, etc.);
  - assicurare la continuità del business;
- il Gruppo Mastrotto e la Dirigenza rispettano, promuovono e sostengono concretamente, i principi contenuti in questo documento e si fanno parte attiva nella diffusione e nell'attuazione di quanto stabilito;
- la definizione e realizzazione degli obiettivi di sicurezza delle informazioni deve:
  - essere allineata con la strategia di business e dei sistemi informativi,
  - supportare gli obiettivi di business evidenziando i rischi correnti ai responsabili del business,
  - essere integrata con il ciclo di vita dei sistemi e dei servizi di gestione delle informazioni,
  - supportare il ciclo di vita dei dati;
  - essere proporzionale ai rischi stimati ed alle perdite operative contabilizzate;
- il personale, interno ed esterno, che necessita di accedere ai sistemi informativi per attività di progettazione, sviluppo, esercizio e manutenzione deve essere opportunamente selezionato, formato e responsabilizzato;
- gli investimenti ed i costi operativi per garantire la protezione del patrimonio informativo aziendale sono allocati sulla base dei rischi stimati e al "valore" dei dati da proteggere;
- i servizi, gli strumenti ed i comportamenti che realizzano la sicurezza dei dati devono seguire l'evoluzione delle tecnologie impiegate, nonché considerare l'evoluzione delle minacce potenziali ed il rinnovo del contesto normativo;
- il patrimonio informativo aziendale deve essere protetto da tutte le minacce, interne ed esterne, intenzionali o accidentali. Il personale deve averne cura in quanto bene intangibile, sotto il profilo della riservatezza, dell'integrità e della disponibilità;
- tutto il personale deve ricevere adeguata formazione in merito a ruoli e responsabilità per la protezione dei dati per acquisire consapevolezza relativamente all'uso delle informazioni

- ogni utente è tenuto ad accedere ai soli dati e sistemi necessari allo svolgimento della propria mansione lavorativa (con riferimento alla *Politica di Gestione degli accessi e delle identità* e al *Regolamento interno per l'utilizzo del sistema informatico);*
- le terze parti cui è concesso l'accesso ai dati ed ai sistemi operativi del Gruppo Mastrotto devono impegnarsi a rispettare gli obiettivi di sicurezza del Gruppo stesso;
- l'assicurazione della continuità del business è un obiettivo fondamentale per il Gruppo Mastrotto e a tutti i dipendenti è richiesto di contribuire secondo ruolo e mansione;
- qualsiasi violazione rilevata o probabile deve immediatamente essere comunicata e gestita seguendo le prescritte procedure (con riferimento a *Procedura di Gestione incidenti di Sicurezza delle Informazioni*);
- la sicurezza è un processo aziendale e, come tale, è sottoposto a costante azione di miglioramento.

La presente Politica è ispirata ai principi degli standard internazionali *ISO/IEC 27001* e *ISO/IEC 27002,* nonché alla norma specifica del settore industriale automotive *Trusted Information Security Assessment Exchange (TISAX).*

2. Applicabilità

La Politica di Sicurezza delle Informazioni si applica indistintamente a tutte le Funzioni e Direzioni di Gruppo Mastrotto, in riferimento a tutti i processi aziendali.

L'attuazione della presente politica è obbligatoria per tutti coloro (i.e. dipendenti, collaboratori esterni e fornitori) che, nello svolgimento della propria attività lavorativa, utilizzano i sistemi informativi aziendali e concorrono al trattamento delle informazioni, dei processi e delle risorse di proprietà del Gruppo, nonché al trattamento di dati personali e a tutti i processi e alle risorse coinvolte nelle operazioni di raccolta, elaborazione, conservazione, trasferimento ed utilizzo di dati personali concernenti persone fisiche.

A tal fine, tutto il personale deve avere accesso al contenuto del presente documento e la conoscenza è ritenuta fondamentale per il corretto svolgimento dell'attività di business e delle relative attività di supporto.

2.1. Eccezioni

In linea di principio, la Politica deve essere applicata senza eccezioni. Tuttavia, in caso di problematiche rilevanti è possibile richiedere una deroga alle funzioni preposte al governo della Sicurezza delle Informazioni documentando i motivi della richiesta. Tali funzioni, valutati i rischi derivanti dalla richiesta, provvederanno ad approvare o rifiutare la deroga. In ogni caso tutte le eccezioni saranno sottoposte a verifica e riconferma periodica da parte del Responsabile del governo degli aspetti di Sicurezza delle Informazioni.

3. Riferimenti e modulistica utilizzata

3.1. Riferimenti interni

Politiche	Gestione degli accessi e delle identità	P7016G
Procedure e istruzioni operative collegate	Provisioning e De-provisioning utenze	P7004G
	Revisione periodica utenze	P7006G
	Regolamento interno per l'utilizzo del sistema informatico	P7015G
	Gestione incidenti di Sicurezza delle Informazioni	P7014G

3.2. Riferimenti a leggi, norme e regolamenti

- D. Lgs. n. 231/2001 – Disciplina della responsabilità amministrativa delle persone giuridiche;
- Provvedimento del Garante per la privacy 27 novembre 2008, pubblicato sulla G.U. n. 300 del 24 dicembre 2008 – "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", fatti salvi altri
- Regolamento Europeo n.679/2016 General Data Protection Regulation (GDPR);
- D. Lgs. 10 agosto 2018, n. 101, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679;
- Standard/Best practice nazionali e internazionali:
    - UNI CEI EN ISO/IEC 27000:2020 - Tecnologie informatiche — Tecniche di sicurezza — Sistemi di gestione per la sicurezza delle informazioni — Panoramica e vocabolario
    - UNI CEI ISO/IEC 27001:2017 – Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni – Requisiti;
    - UNI CEI ISO/IEC 27002:2022 – Tecnologie informatiche - Tecniche per la sicurezza - Raccolta di prassi sui controlli per la sicurezza delle informazioni;
    - ISO/IEC 27005 - Information technology — Security techniques — Information security risk management
    - ISO/IEC 27701:2019 - Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines
    - UNI EN ISO 22301:2019 Sicurezza e resilienza - Sistemi di gestione per la continuità operativa (SGCO) – Requisiti;
    - UNI ISO 31000:2018 – Gestione del rischio - Principi e linee guida;
    - NIST Special Publication 800-53 (Rev. 4) "Recommended Security Controls for Federal Information Systems";
    - NIST Special 800-30 "Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology".
    - Trusted Information Security Assessment Exchange (TISAX) - Standard di riferimento per la sicurezza delle informazioni del settore automobilistico europeo

3.3. Definizioni ed acronimi

Termine	Descrizione
Amministratore di Sistema	Figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.
Backup	Copia di Sicurezza dei Dati su supporto esterno/centralizzato al fine di prevenire la perdita definitiva di dati a seguito di eventi malevoli, accidentali o intenzionali
Disponibilità	Proprietà delle informazioni di essere accessibili e utilizzabili su richiesta di un'entità autorizzata (ISO/IEC 27000). Una compromissione della disponibilità, ad esempio, potrebbe comportare l'impossibilità di accedere a informazioni e/o documenti necessari per lo svolgimento dei compiti istituzionali e/o per l'erogazione dei servizi
GDPR	General Data Protection Regulation (Reg. UE 679/2016)
Integrità	Proprietà di accuratezza e completezza delle informazioni trattate (ISO/IEC 27000). Una compromissione dell'integrità, ad esempio, potrebbe comportare che le informazioni vengano alterate, volontariamente o involontariamente
Misure di Sicurezza	Iniziative di natura tecnica, tecnologica o organizzativa volta a modificare la probabilità o gli effetti derivanti dall'avverarsi di una situazione di rischio
Miglioramento continuo	Attività ricorrente mirata ad accrescere la capacità di soddisfare i requisiti
Responsabile del Governo degli Aspetti di Sicurezza delle Informazioni	Figura di supporto all'Ufficio ICT con competenze relative alla definizione della strategia di sicurezza informatica, dell'implementazione dei programmi di protezione degli asset aziendali e dello sviluppo di processi volti a mitigare i rischi in ambito sicurezza delle informazioni.
Riservatezza	Proprietà che le informazioni non siano rese disponibili o divulgate a persone, entità o processi non autorizzati (ISO/IEC 27000). Una compromissione di riservatezza, ad esempio, potrebbe comportare la divulgazione di informazioni e/o documenti sensibili a soggetti non autorizzati o malintenzionati
Rischio	Probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione
Ruolo	Figura rilevante per le attività aziendali e alla quale sono associati determinati privilegi.
Utente	Dipendente, collaboratore esterno o, in generale, chiunque utilizzi le dotazioni o gli strumenti informatici assegnategli dal Gruppo Mastrotto in virtù del proprio rapporto con il Gruppo Mastrotto stesso.
Utenza	Entità digitale associata a un utente necessaria per operare sul sistema informativo aziendale. A un'utenza sono associate delle abilitazioni e dei privilegi che esprimono cosa l'utenza può fare e dove può farlo.

4. Governo della Sicurezza delle Informazioni

Ai fini di un efficace governo della sicurezza delle informazioni del Gruppo Mastrotto sono attuati i seguenti presidi.

4.1. Ruoli e responsabilità per la Sicurezza delle Informazioni

Di seguito sono descritti i ruoli e le responsabilità componenti il modello organizzativo interno del Gruppo Mastrotto in ambito Sicurezza delle Informazioni.

4.1.1. Responsabile del governo degli aspetti di Sicurezza delle Informazioni

Il ruolo del Responsabile del governo degli aspetti di Sicurezza delle Informazioni è di garantire che le attività attinenti alla sicurezza di informazioni e sistemi siano svolte in modo professionale, nel rispetto dei tempi concordati ed in accordo con leggi e regolamenti applicabili.

In particolare, ha i seguenti compiti e responsabilità:

- definire, in linea con gli indirizzi aziendali in ambito gestione dei rischi, ed applicare la metodologia di gestione del rischio informatico, integrando i risultati con la valutazione dei rischi operativi;
- definire, verificare e mantenere la Politica di Sicurezza delle Informazioni;
- fornire, in collaborazione con l'area legale, supporto nella definizione di clausole contrattuali (nei confronti dei fornitori) che proteggano il livello di sicurezza aziendale e garantiscano la conformità con le normative applicabili;
- supportare l'Ufficio ICT e/o le altre funzioni aziendali nell'elaborazione dei documenti necessari per la definizione, l'implementazione ed il miglioramento del sistema di gestione della sicurezza delle informazioni, quali criteri, regole, politiche, procedure e linee guida;
- effettuare comunicazioni specifiche agli utenti qualora si verificassero o possano verificare eventi critici che aumentano l'esposizione ai rischi;
- supervisionare la corretta gestione degli strumenti di protezione aziendale e più in generale della gestione del ciclo di vita degli asset informatici;
- proporre nuovi progetti e azioni migliorative in funzione dei cambiamenti tecnologici, dei risultati dell'analisi dei rischi e delle eventuali modifiche organizzative, in accordo con il piano strategico IT;
- pianificare e realizzare le opportune verifiche ispettive (audit) sulle aree di interesse, in supporto all'area organizzativa responsabile;
- definire, implementare e manutenere un processo di rilevazione, segnalazione e risoluzione degli incidenti;
- effettuare controlli sui sistemi IT sugli aspetti di gestione della sicurezza delle informazioni.

4.1.2. Area Legale/Privacy

Le aree deputate al governo degli aspetti legali e privacy, per quanto riguarda la sicurezza delle informazioni, hanno il compito di:

- collaborare alla redazione delle istanze di Privacy by Design e DPIA, all'interno delle quali sono decritti i presidi di sicurezza delle informazioni applicati o da applicare;
- prendere parte alla valutazione dell'adeguatezza delle misure di sicurezza applicate ai trattamenti di dati personali per meglio definire il livello di rischiosità dei trattamenti;
- supportare l'analisi e la gestione degli violazioni dei dati personali in relazione alla valutazione di impatto e comunicazioni verso il Garante per la Protezione dei Dati Personali;
- supportare il Responsabile del governo degli aspetti di Sicurezza delle Informazioni nel monitorare la conformità alle leggi, ai regolamenti di settore, ai regolamenti applicabili e alle obbligazioni assunte dal Gruppo Mastrotto in materia di sicurezza delle informazioni e protezione dei dati.

4.1.3. DPO

In accordo con quanto disciplinato dal GDPR, il DPO è inserito nel quadro delle funzioni di Sicurezza delle Informazioni, per quanto riguarda le attività di trattamento dei dati personali, con la cura di salvaguardarne la posizione da eventuali conflitti di interessi come richiesto dalla stessa normativa.

In particolare, il DPO ha i compiti di:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Gruppo Mastrotto in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'Autorità Garante per la Protezione dei Dati Personali;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

4.1.4. Dipendenti e collaboratori esterni del Gruppo Mastrotto

Questa Politica si applica a tutti i dipendenti, così come agli esterni e alle terze parti che lavorano per conto del Gruppo Mastrotto. Ai fini di questa politica le persone appartenenti a queste categorie sono identificate come Utenti, ed in quanto tali essi devono:

- svolgere le proprie mansioni che prevedono l'accesso alle risorse informative conformemente alle istruzioni ricevute sulle regole di comportamento applicabili;
- essere consapevoli dei rischi relativi ai propri comportamenti ed alle proprie responsabilità;
- riportare qualsiasi incidente di sicurezza o comportamento anomalo di cui vengono a conoscenza.

Tutti gli utenti sono responsabili dell'utilizzo delle risorse e degli asset assegnati – o utilizzati – e delle informazioni prodotte, gestite e distribuite mediante i sistemi aziendali secondo quanto definito nel *Regolamento interno per l'utilizzo del sistema informatico* adottato dal Gruppo Mastrotto, che gli utenti devono visionare ed accettare formalmente.

4.2. Pianificazione in ambito Sicurezza delle Informazioni

Nel definire e nell'adottare l'insieme delle misure per la Sicurezza delle Informazioni, il Gruppo Mastrotto deve considerare i fattori che possono determinarsi come fonti di rischio e che possono minare la sicurezza delle informazioni o, più in generale, il conseguimento degli obiettivi perseguiti. Le misure per la Sicurezza delle Informazioni sono volte a:

- assicurare che il Gruppo Mastrotto possa conseguire gli obiettivi previsti;
- prevenire, o ridurre, gli effetti indesiderati;
- realizzare il miglioramento continuo.

4.2.1. Valutazione del rischio relativo alla sicurezza delle informazioni

Il Gruppo Mastrotto deve definire e applicare un processo di valutazione del rischio relativo alla sicurezza delle informazioni secondo criteri coerenti, ripetibili ed in linea con le indicazioni dei principali standard internazionali di riferimento.

4.2.2. Trattamento del rischio relativo alla sicurezza delle informazioni

Il Gruppo Mastrotto deve definire i criteri e le modalità di trattamento del rischio relativo alla sicurezza delle informazioni. Le opzioni di trattamento del rischio sono indirizzate in relazione ai criteri di accettabilità del rischio individuati sulla base degli obiettivi stabiliti.

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

Il gruppo Mastrotto deve stabilire l'insieme delle misure per la sicurezza delle informazioni tenendo conto dei seguenti criteri:

- coerenza con le politiche dell'organizzazione;
- misurabilità;
- efficacia nel conseguire una riduzione del rischio secondo i criteri di accettabilità stabiliti in sede di trattamento del rischio.

Gli obiettivi devono essere comunicati e aggiornati per quanto appropriato.

4.3. Valutazione delle prestazioni

Ai fini di valutare le prestazioni e l'efficacia delle misure di sicurezza, il Gruppo Mastrotto determina un piano di valutazione delle misure stesse. A tal fine adotta delle procedure volte a determinare criteri coerenti e ripetibili di valutazione che includono:

- gli oggetti delle valutazioni;
- i metodi di monitoraggio, misurazione e analisi delle prestazioni;
- la periodicità delle valutazioni;
- i responsabili delle attività di valutazione;
- criteri per determinare l'adeguatezza delle misure intraprese.

4.4. Miglioramento continuo

All'esito di una valutazione di non adeguatezza delle misure di sicurezza, al fallimento delle stesse (ad esempio a seguito di un incidente di sicurezza), o in ogni caso all'emergere di una situazione di incapacità dell'organizzazione di perseguire i propri obiettivi, essa deve reagire alla situazione intraprendendo le azioni correttive applicabili ed aggiornando allo stesso tempo i criteri di valutazione ed accettazione del rischio e di valutazione delle prestazioni.

5. Principi di Sicurezza delle Informazioni

Per perseguire gli obiettivi di sicurezza definiti in precedenza, Gruppo Mastrotto adotta uno schema omogeneo ed organico di Principi di Sicurezza delle Informazioni, ispirato agli standard e alle best practices internazionali, in particolare agli ambiti che caratterizzano lo standard ISO/IEC 27001/2 e tengono conto delle indicazioni della norma TISAX.

Gli indirizzi da rispettare sono descritti di seguito.

5.1. Indicazione della Direzione in merito alla sicurezza delle informazioni

La Direzione aziendale fornisce le indicazioni ed il supporto per garantire che la sicurezza delle informazioni sia in accordo con i requisiti di business, con le leggi, con i regolamenti pertinenti, con gli impegni di natura contrattuale assunti verso i clienti e, più in generale, con gli obiettivi perseguiti a livello strategico.

Le regole per la implementazione dei Principi di Sicurezza delle informazioni devono essere definite, pubblicate e comunicate al personale ed alle terze parti interessate.

5.2. Organizzazione della sicurezza delle informazioni

Si elencano di seguito i principi di base a garanzia del fatto che l'organizzazione interna persegue adeguatamente i principi di sicurezza.

5.2.1. Organizzazione interna

Deve essere stabilito un quadro di riferimento gestionale per intraprendere e controllare l'attuazione e l'esercizio della sicurezza delle informazioni in azienda.

Affinché venga raggiunto tale obiettivo è necessario che siano definite ed assegnate tutte le responsabilità relative alla sicurezza delle informazioni; tale processo deve garantire la separazione dei compiti (intendendo con questo termine che i compiti e le aree di responsabilità in conflitto tra loro devono essere separati per ridurre le possibilità di uso improprio) e la modifica non autorizzata o non intenzionale degli asset dell'organizzazione.

L'organizzazione deve assicurarsi che le persone assegnatarie dei ruoli di Sicurezza delle Informazioni siano consapevoli dell'impatto delle loro attività.

È inoltre importante che vengano tenuti appropriati contatti con le Autorità competenti in materia di sicurezza delle informazioni, così come contatti con gruppi specialistici e/o associazioni professionali frequentate da specialisti della sicurezza delle informazioni. Infine, la sicurezza delle informazioni deve essere gestita in tutti i progetti, a prescindere dalla tipologia degli stessi.

Il Gruppo Mastrotto deve prevedere la capacità di riformare la propria organizzazione interna qualora venga valutata come non adeguata al raggiungimento degli obiettivi previsti.

5.2.2. Dispositivi portatili

Deve essere garantita la sicurezza delle informazioni nell'utilizzo degli asset portatili.
A tal scopo devono essere implementati alcuni controlli che riguardano la politica o linee guida per i dispositivi portatili e le misure di sicurezza a suo supporto al fine di gestire nel modo migliore i rischi introdotti dall'uso dei dispositivi in oggetto.

5.3. Formazione in ambito sicurezza delle informazioni e privacy

La sicurezza delle informazioni si realizza anche attraverso la sensibilizzazione e la formazione del personale per gli aspetti comportamentali comuni da mantenere in relazione alla protezione dei dati e dei sistemi (es. riconoscere un tentativo di phishing o un sito non sicuro).

Il Gruppo Mastrotto deve supportare la formazione continua del personale sulla sicurezza delle informazioni e sulla protezione dei dati personali in quanto valore aziendale riconosciuto.

Per il personale che implementa i ruoli rilevanti in ambito sicurezza delle informazioni deve essere raccomandata una formazione specialistica a seconda del ruolo, la quale permetta di mantenere aggiornato il Gruppo Mastrotto riguardo le minacce di settore e tecnologiche correnti.

Il mantenimento della conoscenza riguardo le minacce informatiche (es. campagne di phishing, famiglie di malware, attacchi a sistemi con vulnerabilità note) o le principali classi agenti di minaccia (es. cyberspionaggio, cyber-criminalità) è realizzato per mezzo della partecipazione a eventi e tavoli di lavoro promossi da organismi del settore di appartenenza e del settore della sicurezza informativa (es. CLUSIT).

5.4. Gestione degli asset

Gli asset aziendali (sia fisici che informativi) sono parte integrante del patrimonio aziendale che, come tale, devono essere adeguatamene tutelati e protetti.

5.4.1. Responsabilità per gli asset

Al fine di proteggere tutti gli asset in modo adeguato, è indispensabile identificarli e definire adeguate responsabilità per la loro protezione.

Risulta quindi necessario implementare alcuni controlli che vengono di seguito esplicitati:

- tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati; deve inoltre essere compilato e costantemente aggiornato un inventario di questi asset;
- ogni asset inserito nell'inventario deve avere un responsabile che ne governi l'uso e l'accesso;
- devono essere definite, documentate ed implementate delle regole per l'utilizzo delle informazioni aziendali e degli asset associati alla loro elaborazione;
- tutto il personale e gli utenti di parti esterne devono restituire tutti gli asset aziendali a loro assegnati al termine del periodo di impiego, del contratto o dell'accordo stipulato.

5.4.2. Classificazione delle informazioni

Per assicurare che le informazioni ricevano un adeguato livello di protezione, in linea con la loro importanza aziendale, è necessario classificarle.

Le informazioni devono quindi essere classificate in relazione ai requisiti legali, al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzata.

Deve essere inoltre sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo schema di classificazione; analogamente, deve essere sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione aziendale.

5.4.3. Trattamento dei supporti

Si deve prevenire la divulgazione non autorizzata, la modifica, la rimozione o la distruzione delle informazioni archiviate sui supporti.

Affinché sia garantito il raggiungimento di questo obiettivo è necessario prevedere l'implementazione di tre controlli fondamentali:

- per la **Gestione** dei supporti rimovibili, devono essere sviluppate delle procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato aziendalmente;
- per la **Dismissione** dei supporti, la dismissione dei supporti non più necessari deve avvenire in modo sicuro, attraverso l'utilizzo di procedure formali;

- per la **Trasporto** dei supporti fisici, i supporti che contengono informazioni devono essere protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto.

5.5. Controllo degli accessi

Il controllo degli accessi consente di monitorare in quale modo utenti e sistemi accedono ai dati aziendali.

Il sistema di controllo degli accessi deve rispondere agli obiettivi e rispettare i controlli di seguito descritti.

A tal fine, all'interno del Gruppo Mastrotto è stata adottata la seguente documentazione a cui poter fare riferimento:

- P7016G – Politica di gestione degli accessi e delle identità;
- P7004G – Procedura di provisioning e de-provisioning utenze;
- P7006G – Revisione periodica delle utenze.

5.5.1. Requisiti di business per il controllo degli accessi

È indispensabile limitare l'accesso alle informazioni e ai servizi di elaborazione delle informazioni.

È quindi necessario definire, documentare e tenere costantemente aggiornata delle linee guida di controllo degli accessi, basata sui requisiti di business e di sicurezza delle informazioni.

Inoltre, agli utenti devono essere forniti solo gli accessi a reti e servizi di rete al cui uso sono stati specificamente autorizzati.

5.5.2. Gestione degli accessi degli utenti

È indispensabile prevenire accessi alle informazioni ed ai sistemi da parte di utenti non autorizzati ed al contempo assicurare la disponibilità dell'accesso agli utenti autorizzati.

Deve quindi essere implementato un processo formale di registrazione e de-registrazione degli utenti per abilitare l'assegnazione dei diritti di accesso.

Il provisioning degli accessi degli utenti (assegnazione e revoca dei diritti di accesso), per tutte le tipologie di utenze e per tutti i sistemi e servizi, deve essere attuato mediante un processo formale. Inoltre, l'assegnazione e l'uso di diritti di accesso privilegiato devono essere limitati e controllati con adeguata frequenza.

I diritti di accesso a dati e sistemi di elaborazione, di tutto il personale e degli utenti di parti esterne devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate a ogni variazione.

Le informazioni di autenticazione degli utenti (quali, ad esempio, le password) devono essere controllate attraverso un processo di gestione formale, in modo che ne sia garantita la sicurezza.

È infine importante che i responsabili delle risorse e degli asset riesaminino ad intervalli regolari i diritti di accesso degli utenti, almeno con cadenza semestrale, al fine di mantenere attivi gli accessi secondo il principio del minimo privilegio.

5.5.3. Responsabilità dell'utente

È necessario rendere gli utenti responsabili della salvaguardia delle loro informazioni di autenticazione.

Gli utenti sono tenuti a seguire le prassi aziendali nell'uso di informazioni di autenticazione, come disciplinato all'interno del *Regolamento interno per l'utilizzo del sistema informatico.*

5.6. Crittografia

Lo scopo dei controlli crittografici è di assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni. L'uso della crittografia all'interno dell'organizzazione deve seguire procedure dirette a garantirne l'efficacia ed a salvaguardare la disponibilità delle informazioni.

Devono essere sviluppate e attuate: delle linee guida sull'uso dei controlli crittografici per la protezione delle informazioni e linee guida sull'uso, sulla protezione e sulla durata delle chiavi crittografiche per tutto il loro intero ciclo di vita.

5.7. Sicurezza fisica e ambientale

Gli aspetti di sicurezza fisica e ambientale sono fondamentali per garantire la sicurezza dei dati e dei sistemi che li elaborano e gestiscono.

Di seguito gli obiettivi ed i controlli che è necessario prevedere in quest'ambito.

5.7.1. Aree sicure

La definizione di aree sicure ha come obiettivo prevenire l'accesso fisico non autorizzato, danni e disturbi alle informazioni aziendali e alle strutture di elaborazione delle informazioni.

Affinché questo obiettivo sia raggiunto, è necessario implementare alcuni controlli che vengono meglio specificati di seguito.

Deve essere definito un perimetro di sicurezza fisica; si devono cioè definire e usare dei perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni.

Le aree di sicurezza devono essere protette da appropriati controlli per l'ingresso che assicurino che solo il personale autorizzato abbia il permesso di accedervi; per quanto riguarda uffici, locali e strutture si deve progettare e implementare un adeguato livello di sicurezza fisica.

Al fine di limitare i danni in caso di calamità naturali, attacchi malevoli e incidenti si devono definire ed implementare adeguate misure di protezione fisica.

Il lavoro in aree sicure è particolarmente delicato, ragion per cui devono essere progettate e attuate procedure che ne regolino lo svolgimento.

I punti di accesso, come le aree di carico e scarico e altri punti attraverso i quali persone non autorizzate potrebbero accedere ai locali, devono essere controllati e, se possibile, isolati dalle strutture di elaborazione delle informazioni per evitare accessi non autorizzati.

5.7.2. Apparecchiature

Devono essere definiti i controlli relativi alle apparecchiature che ne devono prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l'interruzione delle attività operative dell'organizzazione.

Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari, mentre i cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi devono essere protetti da intercettazioni, interferenze o danneggiamenti.

Tutte le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità.

La sicurezza delle apparecchiature e degli asset all'esterno delle sedi è particolarmente importante; devono quindi essere previste misure di sicurezza per gli asset all'esterno delle sedi aziendali, considerando i diversi rischi derivanti dall'operare all'esterno dei locali aziendali; inoltre, il trasferimento all'esterno di una qualsiasi tipologia di asset non può avvenire senza la preventiva autorizzazione del relativo owner.

Devono anche essere implementati dei controlli che garantiscano la dismissione sicura o il riutilizzo delle apparecchiature, in modo particolare quelle che contengono supporti di memorizzazione devono essere gestite in modo tale da garantire che ogni dato critico venga adeguatamente tutelato. Allo stesso modo le apparecchiature incustodite devono ricevere una protezione adeguata alla criticità dei dati in essi contenuti.

All'interno di tutti i luoghi di lavoro ove vengono trattati dati aziendali devono essere adottate linee guida di "scrivania pulita" per i documenti e i supporti di memorizzazione rimovibili, e linee guida di "schermo pulito" per i servizi di elaborazione delle informazioni.

5.8. Sicurezza delle attività operative

5.8.1. Procedure operative e responsabilità

Le attività operative delle strutture di elaborazione delle informazioni devono essere corrette e sicure.

Per garantire il rispetto dell'obiettivo, si devono prevedere diversi controlli che riguardano sia la parte organizzativa/formale sia la parte operativa.

Per quanto riguarda la parte organizzativa/formale, si devono documentare e pubblicare le procedure operative mettendole a disposizione di tutti gli utenti che le necessitano.

Per la parte più propriamente operativa, si devono implementare i controlli di seguito descritti.

- gestione dei cambiamenti, siano essi aziendali, relativi ai processi di business, alle strutture di elaborazione e a tutti i sistemi che potrebbero influenzare la sicurezza delle informazioni: tutti i cambiamenti devono essere controllati e documentati.
- gestione della capacità: devono essere effettuate proiezioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste, inoltre l'uso delle risorse deve essere monitorato al fine di intercettare nel più breve tempo possibili problemi di disponibilità.
- separazione degli ambienti di sviluppo, test e produzione: gli ambienti di sviluppo, test e produzione devono essere separati per ridurre il rischio di accesso o cambiamenti non autorizzati all'ambiente di produzione.

5.8.2. Protezione dal malware

Le informazioni e le strutture preposte alla loro elaborazione devono essere protette contro il malware.

Per garantire il raggiungimento di questo obiettivo è necessario implementare dei controlli di individuazione, di prevenzione e di ripristino relativamente al malware.

5.8.3. Backup

Deve essere garantita la protezione rispetto alla perdita di dati e configurazione dei sistemi, in termini di disponibilità ed integrità.

Per il raggiungimento di questo obiettivo è necessario effettuare il backup delle informazioni; in particolare devono essere effettuate delle copie di backup dei dati, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo linee guida di backup definite.

Il processo di backup prevede verifiche di integrità delle istanze e test periodici di utilizzabilità dei supporti, attraverso la simulazione di ripristino.

La retention dei backup è allineata alle esigenze di compliance in termini di conservazione minima richiesta e termini massimi entro i quali non è più possibile conservare i dati, in conformità con leggi, regolamenti e impegni contrattuali. L'applicazione del principio di oblio non deve compromettere l'integrità delle immagini dati/sistemi, necessaria per garantire il ripristino.

5.8.4. Raccolta di log e monitoraggio

Deve essere garantita la registrazione di eventi e la generazione di evidenze per monitorare la sicurezza, oltre che per richieste normative.

A tal fine il sistema di log degli eventi deve aderire ai seguenti requisiti:

- deve essere effettuata, mantenuta e riesaminata periodicamente la raccolta dei log che raccoglie gli eventi di sicurezza, le eccezioni, i malfunzionamenti generati firewall, dispositivi antintrusione (IPS), dispositivi di

rilevamento delle potenziali intrusioni (IDS), dei server che si occupano di gestire accessi e flussi in ingresso e uscita dalla rete interna (es. internet proxy, VPN server)

- I log devono quindi essere protetti da manomissioni e accessi non autorizzati; gli orologi di tutti i sistemi pertinenti che elaborano informazioni a livello aziendale o di dominio di sicurezza devono essere sincronizzati rispetto a una singola sorgente temporale di riferimento, affinché i dati provenienti dai vari sistemi possano essere correttamente collegati e correlati
- I log degli amministratori di sistema rivestono un ruolo di particolare importanza per la sicurezza ed il rispetto della normativa vigente. Le modalità e la retention delle registrazioni deve essere conforme alle indicazioni di leggi e regolamenti nonché alle indicazioni dell'Autorità Garante per la Protezione dei Dati Personali.

5.8.5. Controllo dei software di produzione (Change and Release)

È necessario assicurare l'integrità dei sistemi di produzione affinché le elaborazioni da essi eseguite siano allineate alle specifiche necessarie all'attività di business, ed inoltre deve essere assicurata l'integrità dei sistemi dal punto di vista delle vulnerabilità.

Per garantire che l'obiettivo sia raggiunto devono essere formalizzate ed applicate delle procedure per il controllo dell'installazione dei software sui sistemi di produzione.

Il monitoraggio dei rilasci di patch di sicurezza per i prodotti software, licenziati oppure open source, è responsabilità del gestore dell'asset. Inoltre, il gestore dell'asset deve conoscere i limiti di validità della licenza d'uso e del supporto erogato dal produttore in modo da governare gli asset in esercizio e mitigare i rischi di sicurezza.

La verifica di compatibilità e l'installazione delle patch di sicurezza (risoluzione di vulnerabilità note o rilevate dal produttore) devono essere installate nel più breve tempo possibile per le componenti in utilizzo. Nei casi gravi ed urgenti si può valutare la necessità di interrompere il servizio per consentire l'aggiornamento della configurazione dell'asset; per la gestione dei casi ordinari deve essere definito un accordo preventivo con i referenti di business in merito a metodi e tempi standard per procedere agli aggiornamenti (release plan).

Il processo di cambiamento del software in produzione deve essere documentato così da descrivere le componenti o funzionalità oggetto di rilascio, i test eseguiti in ambiente non produttivo che ne hanno verificato l'adeguatezza, la decisione in merito al fatto di non eseguire i test; infine deve essere registrata l'autorizzazione da parte del referente di business per rilasci evolutivi o adeguativi a fronte delle risultanze dei test.

5.8.6. Gestione delle vulnerabilità tecniche

Si deve prevenire lo sfruttamento di vulnerabilità tecniche note e ricercare vulnerabilità specifiche attraverso l'esecuzione di *vulnerability assessment*.

Questo obiettivo viene raggiunto controllando le installazioni dei software e gestendo le vulnerabilità tecniche dei software e hardware utilizzati.

In particolare, le informazioni sulle vulnerabilità tecniche dei sistemi utilizzati devono essere ottenute in modo tempestivo; deve quindi essere valutata l'esposizione a tali vulnerabilità e devono essere intraprese appropriate contromisure per affrontare i rischi potenziali conseguenti, in considerazione al rischio informatico intrinseco dei processi supportati.

Per gli asset che erogano servizi esposti in internet e a più alto rischio operativo intrinseco, si deve prevedere la scansione delle vulnerabilità e l'esecuzione di *penetration test*.

5.8.7. Audit dei sistemi informativi

L'organizzazione deve programmare periodiche attività di audit sui sistemi informativi volti all'individuazione di stati che possono compromettere la disponibilità, la riservatezza o l'integrità dei sistemi informativi stessi.

Le attività di audit devono essere inquadrate in una programmazione pluriennale.

5.9. Sicurezza delle comunicazioni

La garanzia di avere sicurezza sulle comunicazioni elettroniche, si articola su diversi piani ed è ottenuta grazie ai controlli che di seguito vengono descritti.

5.9.1. Gestione della sicurezza della rete

È necessario assicurare la protezione delle informazioni nelle reti utilizzate per l'elaborazione delle informazioni.

Per garantire che l'obiettivo sia raggiunto si devono implementare i controlli descritti di seguito:

- le reti devono essere segregate in modo da raggruppare rispettivamente servizi, utenti e sistemi informativi;
- devono essere formalmente identificati regole di sicurezza in modo da gestire la rete attraverso meccanismi di selezione del traffico e della disponibilità;
- infine, le reti devono essere gestite e controllate per proteggere le informazioni presenti nei sistemi e nelle applicazioni.

La crittografia delle informazioni in transito, ove supportata dalle tecnologie, è da considerarsi lo standard by default da attivare per l'intera comunicazione (es. crittografia di canale), la cui applicazione può essere esclusa solo a seguito di decisione motivata del Responsabile del Governo degli Aspetti di Sicurezza delle Informazioni.

5.9.2. Trasferimento delle informazioni

Si deve mantenere la sicurezza delle informazioni trasferite all'interno dell'azienda e scambiate con qualsiasi entità esterna.

È pertanto di fondamentale importanza che siano formalizzate e pubblicate le procedure per il trasferimento delle informazioni che devono descrivere tutti i controlli formali necessari a garantire la protezione del trasferimento delle informazioni, a cura del Responsabile del Governo degli Aspetti di Sicurezza delle Informazioni e del Responsabile dell'Ufficio ICT.

In caso di trasferimento di informazioni verso parti esterne devono essere formalizzati degli accordi appositi dai responsabili delle Direzioni e/o funzioni coinvolte. In caso il trasferimento o la condivisione riguardi dati che sono ritenuti critici per il business o che debbano essere tutelati ai sensi della normativa vigente, devono essere formalmente stipulati degli accordi di riservatezza o di non divulgazione. Questi devono riflettere le necessità aziendali per la protezione delle informazioni e devono essere riesaminati periodicamente.

5.10. Acquisizione, sviluppo e manutenzione dei sistemi

5.10.1. Requisiti di sicurezza dei sistemi informativi

È necessario garantire che la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi. Questo include anche i requisiti specifici per i sistemi informativi che forniscono servizi attraverso reti pubbliche.

Affinché sia rispettato l'obiettivo si devono implementare diversi controlli, di seguito descritti:

- i requisiti relativi alla sicurezza delle informazioni devono essere parte integrante dei requisiti per i nuovi sistemi informativi o per l'aggiornamento di quelli esistenti; inoltre, le informazioni che transitano su reti pubbliche devono essere protette da potenziali attività fraudolente, da divulgazioni accidentali di dati e da modifiche non autorizzate dai dati;
- per quanto attiene l'integrità e la non ripudiabilità delle transazioni dei servizi applicativi è necessario che le informazioni elaborate non siano soggette a trasmissioni incomplete, errori di instradamento, alterazione non autorizzata di messaggi, divulgazione non autorizzata, duplicazione non autorizzata di messaggi.

5.10.2. Sicurezza nei processi di sviluppo e supporto

La sicurezza delle informazioni deve essere progettata e attuata all'interno del ciclo di sviluppo dei sistemi.

I controlli che ne garantiscono il rispetto coprono sia gli aspetti formali che quelli sostanziali e tecnici e sono di seguito riassunti.

Per quanto riguarda gli aspetti formali si devono stabilire e formalizzare le regole per lo sviluppo del software e dei sistemi; queste devono essere applicate a tutti gli sviluppi (*minor* e *major changes* applicativi e nuovi sviluppi). Devono essere inoltre stabiliti, documentati, manutenuti e applicati a ogni iniziativa di implementazione di un sistema informativo i principi di "*security by design*" e "*security by default*" per la progettazione sicura e l'erogazione sicura del servizio.

Una volta definite le regole di sviluppo, devono essere formalizzate e implementate le procedure per il controllo dei cambiamenti di sistema.

Quando avvengono dei cambiamenti nelle piattaforme operative, si devono riesaminare e sottoporre a test di sicurezza le applicazioni critiche per il business per garantire che non ci siano impatti negativi sulle attività operative aziendali.

La modifica dei pacchetti software acquisiti deve essere limitata ai cambiamenti necessari affinché sia preservata la garanzia ed il supporto del produttore; inoltre, tutti i cambiamenti devono essere strettamente controllati.

Per quanto concerne gli strumenti e gli ambienti di sviluppo del software, è necessario che tali ambienti abbiano le funzionalità (es. applicazioni) per effettuare sviluppo e test sia funzionale che di sicurezza (es. code review, code quality, test dinamici). La configurazione degli ambienti di sviluppo deve prevedere una segregazione logica all'interno della rete aziendale e accesso limitato ai dati necessari per svolgere i test nell'ambiente di riferimento.

In caso di sviluppo affidato all'esterno, è necessario supervisionare e monitorare l'attività esternalizzata, oltre che effettuare i test funzionali e di sicurezza previsti anche per sviluppi effettuati su ambienti gestiti internamente. Il software fornito da Terze Parti deve essere adeguato alle regole e standard di sviluppo definite dal Gruppo Mastrotto.

Infine, devono essere stabiliti dei protocolli di validazione, test e criteri di accettazione qualora il software sviluppato preveda innovazioni funzionali e/o tecnologiche importanti per l'esercizio.

5.10.3. Dati di test

È necessario assicurare la protezione dei dati usati per i test proporzionalmente al valore aziendale dei dati impiegati e rispetto alle normative rilevanti (ex art.32 del GDPR).

Per garantire che l'obiettivo sia raggiunto i dati di test devono essere scelti con attenzione, protetti e tenuti sotto controllo.

L'accesso agli ambienti di test che gestiscono dati derivati da elaborazioni dei dati di produzione, devono essere controllati con le stesse modalità con cui sono concessi gli accessi ai dati di produzione da cui sono ricavati, salvo poter dimostrare che non sia riconducibile il legame.

5.11. Relazione con i fornitori

5.11.1. Sicurezza delle informazioni nelle relazioni con i fornitori

Gli asset aziendali accessibili da parte dei fornitori devono essere protetti durante l'esecuzione delle attività esternalizzate (es. accesso, elaborazione, archiviazione, etc.).

A tal fine è necessario implementare controlli che, in questo specifico caso, sono prevalentemente di tipo organizzativo/formale, tra cui la l'applicazione dei processi di autorizzazione (profilazione accessi) e autenticazione.

Gli accordi con i fornitori devono includere specifiche clausole per gestire i rischi relativi alla sicurezza delle informazioni associati ai servizi e ai prodotti oggetto della fornitura, sulla base delle valutazioni dei rischi operativi e dei rischi inerenti i diritti e le libertà delle persone fisiche (ex-GDPR).

In particolare, devono essere definite linee guida per la sicurezza delle informazioni nei rapporti con i fornitori che devono documentare i requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset

aziendali da parte dei fornitori. Le linee guida o i requisiti di sicurezza espressi è preferibile che siano inclusi nel contratto come allegato tecnico.

Nel caso di fornitura di componenti dell'infrastruttura IT, tali componenti devono rispettare i criteri di accettazione relativi alla sicurezza ovvero devono poter essere configurati per eseguire i processi aziendali in sicurezza, essere compatibili con l'architettura tecnica ed essere supportati dal produttore per il tempo di impiego.

5.11.2. Gestione dell'erogazione dei servizi dei fornitori

Negli accordi con i fornitori, devono essere garantiti:

- il livello concordato di sicurezza delle informazioni;
- il livello di erogazione dei servizi.

Per garantire che l'obiettivo sia raggiunto si devono monitorare, riesaminare e sottoporre a verifiche periodiche i servizi erogati dai fornitori.

Particolare attenzione deve inoltre essere posta alla gestione del cambiamento dei servizi erogati dai fornitori che deve essere gestito tenendo conto della criticità delle informazioni di business, dei sistemi e dei processi coinvolti e della rivalutazione dei rischi.

5.12. Gestione degli incidenti relativi alla sicurezza delle informazioni

Deve essere garantito un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza.

La gestione degli incidenti è una componente fondamentale per la protezione dell'azienda e dei suoi asset. Una gestione degli incidenti adeguata alla realtà aziendale passa per alcuni controlli formali, tecnici/pratici e un processo di riesame e miglioramento. Ognuno di questi viene brevemente descritto in seguito.

Il processo di gestione degli incidenti deve stabilire ruoli e responsabilità affinché le procedure assicurino una risposta rapida, efficace e ordinata agli incidenti relativi alla sicurezza delle informazioni. La classificazione dell'incidente deve essere adeguata a poter attivare fasi del processo di gestione oppure altri processi con ambiti di competenza complementari (es. processo di gestione delle violazioni dei dati personali) e prevede una progressiva escalation di coinvolgimento dei livelli aziendali proporzionale all'impatto dell'evento e delle azioni di contenimento e rimedio.

La segnalazione degli eventi relativi alla sicurezza delle informazioni deve essere effettuata il più velocemente possibile attraverso appropriati canali gestionali conosciuti e formalizzati, che internamente si realizzano attraverso strumento di ticketing o e-mail aziendale, verso terze parti attraverso lo strumento concordato o definito dai termini di legge (es. PEC istituzionale). Oltre agli eventi, devono essere segnalati anche tutti i punti di debolezza relativi alla sicurezza delle informazioni; deve essere richiesto a tutto il personale e ai collaboratori che utilizzano i sistemi informativi ed i servizi aziendali di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato.

Come parte iniziale del processo di reazione, c'è la valutazione e la classificazione degli eventi relativi alla sicurezza delle informazioni: gli eventi devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni o meno. In caso si trattasse di incidente, deve essere innescato il processo di risposta: si deve rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure che devono essere documentate e rese note a tutti i collaboratori.

Parte integrante del processo di reazione è la raccolta delle evidenze: devono quindi essere definite e applicate opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che sono impiegate come evidenze.

Il processo di gestione degli incidenti deve prevedere che la conoscenza acquisita dall'analisi delle informazioni relative all'incidente sia utilizzata per ridurre la probabilità o l'impatto di incidenti futuri.

A tal fine, all'interno del Gruppo Mastrotto è stata adottata la seguente documentazione a cui poter fare riferimento:

- P7014G – Procedura di Gestione degli incidenti di sicurezza delle informazioni;

- P7015G – Regolamento interno per l'utilizzo del sistema informatico.

5.13. Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

5.13.1. Continuità della sicurezza delle informazioni

La continuità della sicurezza delle informazioni deve essere garantita anche dai sistemi per la gestione della continuità operativa.

Per assicurare che l'obiettivo sia raggiunto si devono implementare i controlli di seguito descritti.

Devono essere innanzitutto definiti i requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri; questi devono essere espressi in modo formale.

Successivamente è necessario stabilire, documentare, attuare e mantenere i processi, le procedure e i controlli per garantire che il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa sia messo in atto.

Per garantire il processo di aggiornamento e di miglioramento continuo, è necessario verificare ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti ed attuati.

5.13.2. Ridondanza

Deve essere garantita la disponibilità delle strutture per l'elaborazione delle informazioni.

Per garantire che l'obiettivo sia raggiunto è necessario che i sistemi utilizzati per l'elaborazione delle informazioni siano realizzati con una ridondanza sufficiente a soddisfare i requisiti di disponibilità.

5.13.3. Disaster Recovery e ripristinabilità dati

Devono essere effettuati salvataggi complessivi dei dati con lo scopo di ripristinare gli stessi in caso di perdita o alterazione non autorizzata dei dati.

La ripristinabilità dei dati di backup deve essere verificata almeno annualmente, affinché i dati salvati siano effettivamente utilizzabili nel caso di necessità di ripristino. I tempi di ripristino dei dati devono rientrare nei tempi di ripresa dei servizi, secondo le necessità di business

Le linee guida di mantenimento della storicità dei dati devono assolvere sia le valutazioni relative alla continuità del business sia i requisiti di compliance (es. GDPR).

5.14. Compliance

5.14.1. Conformità ai requisiti cogenti e contrattuali

Devono essere evitate le violazioni a obblighi cogenti o contrattuali relativi alla sicurezza delle informazioni e di qualsiasi requisito di sicurezza.

Per garantire che l'obiettivo sia raggiunto, per ogni sistema informativo e per l'azienda in generale, si devono esplicitamente definire, documentare e mantenere aggiornati tutti i requisiti cogenti e contrattuali pertinenti, oltre all'approccio stesso che l'azienda adotta per soddisfarli.

Le registrazioni devono essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità ai requisiti cogenti, contrattuali e di business

Devono essere garantiti il rispetto della normativa sulla privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti, per quanto applicabile.

I controlli crittografici devono essere utilizzati in conformità a tutti gli accordi, alla legislazione e ai regolamenti pertinenti.

6. Diffusione

Il presente documento, nella versione aggiornata in vigore, è pubblicato sulla Intranet Aziendale.

7. Revisione e aggiornamento

La Politica deve essere periodicamente rivista con cadenza non superiore ai 12 mesi e, laddove necessario, aggiornata. Deve essere inoltre rivista a fronte di cambiamenti normativi, organizzativi o di altri eventi possono avere impatto sulla sicurezza delle informazioni.

L'Ufficio ICT, con il supporto del Responsabile del governo degli aspetti di Sicurezza delle Informazioni, previa validazione e autorizzazione con il GCFO, è Responsabile per la manutenzione delle versioni aggiornate del presente documento.