POLITICA

Politica e organizzazione per la Sicurezza delle Informazioni (ACN – NIS2)

Il presente documento è di proprietà di MM S.p.A. Pertanto, esso non può essere riprodotto, anche parzialmente, senza autorizzazione scritta della stessa

Tipologia di documento	*POLITICA IT*
Numero identificativo	*PL-ISMS001_POSI*
Sistema di Riferimento	*ISMS*
Titolo	*Politica e organizzazione per la Sicurezza delle Informazioni (ACN – NIS2)*
Process Owner	*CBE*
Data	*01/10/2026*
Versione	**05**
Archiviazione	*Il presente documento è archiviato e visibile nella intranet aziendale, sotto la responsabilità della DICT*
Note	

Redatto	**Verificato**	**Approvato**
DIS *CBE*	*DIS* *ITO* *ITO-EAP* *ITO-GED* *PPT* *DES SII e Facility* *DEI ING, CASA e Staff* *QUA* *CMP*	*DICT* *CSO* *AD/COO* *CDA*

Matrice delle revisioni		
Versione n°	**Descrizione**	**Data**
01	Emissione	14/07/2021
02	Aggiornamento normativa ISO/IEC 27001	21/12/2023
03	Aggiornamento per revisione organizzativa	30/05/2025
04	Verifica per adeguamento e integrazione requisiti della Direttiva NIS2 -approvata CDA	25/09/2026
05	Aggiornamento tabella approvazione (acronimi) e modifiche organizzativi e pubblicazione intranet post approvazione CDA	01/10/2026

INDICE

1. SCOPO E CAMPO D'APPLICAZIONE 6

2. ACRONIMI E DEFINIZIONI 7

2.1. Acronimi 7

2.2. Definizioni 8

3. QUADRO GENERALE DEL PROCESSO 9

4. RESPONSABILITA' E SISTEMA DI CONTROLLI 9

5. ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA (Conformità GV.RR-02 NIS2) 11

6. FASI DEL PROCESSO 11

6.1. Approccio basato sul Rischio 11

6.2. Gestione della sicurezza delle informazioni nell'Organizzazione 12

6.2.1. Politiche, Procedure e Responsabilità Operative 12

6.2.2. Organizzazione interna 12

6.2.3. Rapporti con Autorità e Gruppi Specialistici 12

6.2.4. Information Security in Project Management 12

6.2.5. Gestione degli asset 13

6.2.6. Controllo accessi 13

6.2.7. Relazioni con i fornitori 14

6.2.8. Gestione degli incidenti relativi alla sicurezza delle informazioni 15

6.2.9. Aspetti di sicurezza delle informazioni nella gestione della continuità operativa 16

6.2.10. Monitoraggio del SGSI 17

6.2.11. Gestione della sicurezza delle informazioni nei rapporti con il personale 17

6.3. Gestione della sicurezza delle informazioni nella Sicurezza fisica e ambientale 19

6.3.1. Aree sicure 19

6.3.2. Gestione degli Asset 19

6.3.3. Politica Clean Desk e Clean Screen 19

6.4. Gestione della sicurezza delle informazioni con le Tecnologie 20

6.4.1. Protezione dalle minacce informatiche 20

6.4.2. Gestione della vulnerabilità tecnica 20

6.4.3. Backup 20

6.4.4. Monitoraggio delle Attività 21

6.4.5. Sicurezza delle comunicazioni e della rete 21

6.4.6. Controlli Crittografici 22

6.4.7. Acquisizione, sviluppo e manutenzione dei sistemi 22

6.4.8. Gestione delle Configurazioni 22

6.4.9. Considerazioni sull'audit dei sistemi informativi 22
6.5. Diffusione e modifiche alla politica 22
7. ALLEGATI E RIFERIMENTI 24
7.1. Allegati 24
7.2. Riferimenti 24

1. SCOPO E CAMPO D'APPLICAZIONE

Scopo del presente documento è definire, insieme al manuale del sistema di gestione MSGSI_Manuale SGSI, i principi guida e gli obiettivi per la sicurezza delle informazioni ed elencare i punti cardine delle attività e processi svolti da MM per il raggiungimento di tali obiettivi all'interno del suo sistema di gestione per la sicurezza delle informazioni.

Per sicurezza delle Informazioni si intendono tutti quei processi volti a tutelare la Riservatezza, l'Integrità e la Disponibilità delle Informazioni conservate, trattate e trasmesse da MM, nonché tutti i processi volti a garantire la protezione dei dati personali o di business di MM dalla divulgazione, modifica o distruzione (dolosa o accidentale). La sicurezza è garantita attraverso un sistema di gestione attuato dall'Alta Direzione di MM, che attribuisce ruoli e responsabilità, prevede un insieme di processi e procedure descritte all'interno di un sistema documentale per la sicurezza, attua controlli secondo una logica basata sulla valutazione dei rischi; il sistema viene monitorato nella sua efficacia periodicamente attraverso audit interni e riesami al fine di individuare un percorso continuo di miglioramento. Gli obiettivi perseguiti nell'ambito del SGSI adottato da MM sono:

- Assicurare che il Top Management sia consapevole delle sue responsabilità nei confronti della sicurezza delle informazioni attraverso corsi di aggiornamento e attività di awareness
- L'impegno del Top Management e dell'Organo di Direzione è esteso in conformità al D.Lgs. 138/2024, garantendo l'approvazione delle misure di gestione dei rischi, lo stanziamento delle risorse finanziarie e organizzative idonee, e la partecipazione periodica a programmi di formazione e aggiornamento in materia di cybersicurezza
- Assicurare la corretta individuazione delle responsabilità nell'organizzazione di MM per la salvaguardia della sicurezza delle informazioni e la diffusione della cultura della sicurezza in tutto il personale di MM
- Assicurare la disponibilità di politiche e procedure che siano periodicamente aggiornate
- Assicurare riesami periodici e audit interni circa il corretto funzionamento del sistema di gestione
- Assicurare l'individuazione e gestione dei rischi legati alla sicurezza delle Informazioni e dei sistemi corrispondenti sia in ambito IT che OT, attraverso periodiche analisi dei rischi e piani di trattamento
- Assicurare il monitoraggio efficace ed il continuo miglioramento della Sicurezza delle Informazioni anche attraverso l'utilizzo, l'aggiornamento e la valutazione periodica di KPI e cruscotti in grado di misurare l'efficacia dei controlli effettuati
- Assicurare un'efficace prevenzione e gestione degli incidenti di sicurezza, incluse le attività di analisi e monitoraggio post-incidente
- Assicurare periodici riesami del sistema di gestione in ottica di miglioramento, attraverso audit interni e riesami della direzione
- Assicurare la verifica del rispetto dei principi regolatori e contrattuali, con particolare riferimento alla protezione dei dati personali
- Assicurare un controllo sull'attività dei fornitori in relazione alle misure di sicurezza da garantire e alla tutela dei dati di MM da trattare.

Gli obiettivi mirano a preservare la disponibilità, l'integrità e la riservatezza delle informazioni per i servizi di MM, soddisfacendo continuamente le aspettative di tutte le parti interessate interne ed esterne (cfr. MSGSI_Manuale SGSI).

Il documento illustra i controlli che MM ha implementato per gestire la sicurezza delle informazioni, in conformità con la certificazione ISO/IEC27001:2022. Vengono citati i documenti del sistema di gestione della sicurezza, che spiegano in dettaglio le procedure adottate. Gli obiettivi relativi ai processi operativi e all'efficacia dei controlli della gestione della sicurezza delle informazioni sono monitorati regolarmente.

Questo documento si applica a tutti i contesti aziendali, specialmente IT e OT, e alla protezione della sicurezza delle informazioni del Sistema di Gestione del Servizio (SMS) e dei Servizi nel Catalogo offerti dalla Direzione ICT. Nell'applicazione al Sistema di Gestione dei Servizi, si considerano politiche, standard, requisiti legali, normativi e contrattuali, con un focus sulla sicurezza delle informazioni.

2. ACRONIMI E DEFINIZIONI

2.1. Acronimi

- **ACN:** Agenzia Cybersicurezza Nazionale
- **AD:** Amministratore Delegato
- **CSO:** Chief Staff Officer
- **COO:** Chief Operating Officer
- **CMP:** Compliance
- **BCP:** Business Continuity Plan
- **DIS-CBE:** Cybersecurity
- **DEI**: Demand & Delivery ING. CASA e Staff
- **DES**: Demand & Delivery SII e Facility
- **DICT:** Direzione Innovation e Information Technology
- **DIS:** Digital Strategy e Sostenibilità Digitale
- **DORU:** Direzione Organizzazione e Risorse Umane
- **DRP:** Disaster Recovery Plan
- **ITO-EAP:** Esercizio Applicativo
- **ITO-GED:** Gestione Device
- **ICT:** Information Communication Technology
- **IT:** Information Technology
- **ITO:** Information Technology Operations
- **MM:** MM S.p.A.
- **OT:** Operational Technology
- **PPT**: Protezione patrimonio, infrastruttura e TLC
- **QUA:** Qualità e Processi
- **SGS**: Sistema di Gestione dei Servizii
- **SGSI**: Sistema di gestione della sicurezza delle informazioni
- **SOC**: Security Operation Center
- **SOD**: Segregation of duties

2.2. Definizioni

- **Apparecchiature ICT:** componenti di un impianto di elaborazione dei dati, inteso come strumenti informatici e tecnologici aziendali (es. monitor, server, stampanti, ecc.) utilizzati da MM, esclusi i dispositivi mobili che non sono nella responsabilità della gestione sede ma degli utenti a cui sono assegnati
- **Attrezzature:** componenti di un impianto non ICT ma al servizio della sicurezza delle informazioni e dalla protezione degli asset aziendali
- **Disponibilità:** proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata (Fonte ISO/IEC 27000)
- **Hypertext Transfer Protocol Secure (HTTPS):** è un protocollo per la comunicazione sul web che protegge l'integrità e la riservatezza dei dati scambiati usando una comunicazione criptata
- **Impianti:** l'insieme di locali, edifici, terreni o anche di apparecchi, attrezzature, congegni, ecc., concorrenti a uno stesso scopo o indispensabili alla sicurezza delle informazioni (es condizionamento ambiente, telefonia e reti di comunicazione, elettrico, elaborazione dati)
- **Informazione:** qualsiasi comunicazione o rappresentazione di conoscenza, come fatti, dati o opinioni, in qualsiasi mezzo o forma, compresi quelli testuali, numerici, grafici, cartografici, narrativi o audiovisivi. Un'istanza di un tipo di informazione (Fonte NIST SP 800-30 Rev. 1)
- **Integrità:** proprietà di accuratezza e completezza (Fonte ISO/IEC 27000)
- **Accordo di riservatezza o Non Disclosure Agreement (NDA):** accordo che delinea informazioni, materiali o conoscenze specifiche che i firmatari si impegnano a non rilasciare o divulgare ad altre parti. (Fonte: NIST SP 800-47 Rev. 1)
- **Riservatezza:** la proprietà che le informazioni non siano rese disponibili o divulgate a persone, entità o processi non autorizzati (Fonte ISO/IEC 27000)
- **Security Operation Center (SOC):** centro che fornisce servizi finalizzati alla sicurezza dei sistemi informativi di un'azienda (SOC interno) o di clienti esterni con lo scopo di identificare, correlare, gestire ed eventualmente rispondere ad eventuali eventi di sicurezza informatica. (Fonte CSIRT)
- **Segregation of duties (SOD):** si riferisce al principio secondo cui a nessun utente devono essere concessi privilegi sufficienti per utilizzare il sistema da solo. Ad esempio, la persona che autorizza una busta paga non dovrebbe essere anche quella che la prepara. La separazione dei compiti può essere applicata staticamente (definendo ruoli in conflitto, cioè ruoli che non possono essere eseguiti dallo stesso utente) o dinamicamente applicando il controllo al momento dell'accesso (Fonte NIST SP 800-192)

3. QUADRO GENERALE DEL PROCESSO

Il Sistema di Gestione della Sicurezza delle Informazioni è basato sul modello "*Plan-Do-Check-Act*" (PDCA). All'interno di tale modello la fase Do prevede l'applicazione dei controlli di cui all'Annex A della norma ISO 27001:2022.

La Società prevede l'implementazione delle regole, dei regolamenti e delle istruzioni contenute nei documenti approvati. Questi documenti sono organizzati su più livelli per garantire sia vari gradi di specializzazione delle informazioni in essi contenute (a livello di procedure) sia l'adattabilità all'evoluzione dei sistemi informatici (a livello di policy). Le politiche e le procedure vengono adeguatamente comunicate e diffuse.

4. RESPONSABILITA' E SISTEMA DI CONTROLLI

Le modalità di gestione della sicurezza delle Informazioni sono parte integrante degli obiettivi di business di MM e vedono le responsabilità così distribuite:

- **Amministratore Delegato:**
  - Approva le Policy e le Procedure del ISMS
- **Organo di Direzione (CdA):**
  - Approva le misure e le politiche di cybersecurity risk management per la conformità NIS2; sovrintende all'efficacia dei controlli di sicurezza
  - Partecipa a programmi periodici di formazione in cybersicurezza
- **Referente per la Cybersicurezza:**
  - Assicura il coordinamento operativo per la conformità NIS2 e la gestione dei rapporti formali e delle notifiche verso ACN e CSIRT Italia
- **Chief Staff Officer (CSO):**
  - Assicura l'armonizzazione delle strategie delle Divisioni di Staff assegnate, garantendo l'efficienza e l'efficacia dell'azione operativa mediante un coordinamento trasversale capace di massimizzare la valorizzazione delle competenze delle risorse e la qualità dei servizi. Ha la responsabilità di coordinare:
    - Compliance (CMP)
    - Direzione Innovation & Information Technology (DICT)
    - Direzione Organizzazione e Risorse Umane (DORU)
    - Risk Management (RMA)
- **Direttori Strutture:**
  - Sono responsabili della gestione del rischio relativo alla sicurezza delle informazioni delle aree di propria responsabilità e pertinenza
  - Garantiscono l'applicazione del "Manuale del Sistema di Gestione della Sicurezza delle Informazioni" e della Politica sulla sicurezza delle informazioni all'interno del singolo dipartimento di appartenenza
  - Approvano politiche e procedure per il sistema di gestione, garantendone l'applicazione per la propria area di competenza. Validano le valutazioni di rischio per le informazioni che li riguardano
- **Direttore ICT:**
  - Approva il manuale del sistema di gestione per la sicurezza delle informazioni e la politica per la sicurezza delle informazioni
  - Partecipa al riesame del sistema di gestione per la sicurezza delle informazioni
  - Approva politiche e procedure per il sistema di gestione della sicurezza delle informazioni
  - È informato sugli esiti di attività di monitoraggio sull'efficacia delle misure di sicurezza applicate
- **Responsabile della sicurezza delle informazioni (DIS-CBE)**

- Definisce le policy sulla sicurezza delle informazioni e ne monitora la corretta applicazione attraverso l'elaborazione di linee guida per le strutture operative
- Supporta la definizione di politiche e procedure per la sicurezza delle informazioni
- Esegue verifiche sulla corretta applicazione delle misure di sicurezza
- Attiva la management review del sistema di gestione
- Assicura una visione strategica per la sicurezza delle informazioni, garantendo la comprensione degli scenari di rischio e assicurando, compatibilmente con le risorse stabilite dall'Organizzazione, le migliori capacità e il più aggiornato livello e qualità degli strumenti tecnologici e dei processi per fronteggiarle tali scenari
- Determina obiettivi e piani specifici per la Sicurezza delle Informazioni appropriati per i vari ambiti di attività
- Promuove la cultura della sicurezza delle informazioni assicurando la necessaria formazione e sensibilizzazione
- Presidia il corretto funzionamento del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), facilitando il miglioramento continuo
- Fornisce indirizzo per la corretta esecuzione delle attività di valutazione dei rischi
- Facilita e indirizza attività di controllo e monitoraggio, di gestione degli incidenti e di prevenzione degli stessi, in armonia con le strategie dell'organizzazione
- Definisce un manuale per il SGSI e una politica per la sicurezza delle informazioni
- Fornisce indirizzo per la definizione di politiche, procedure e controlli per la sicurezza delle informazioni
- Partecipa alla management review del SGSI

- **Responsabile Funzione Demand & Delivery (DES e DEI)**
  - Garantisce la definizione dei requisiti per i controlli di sicurezza
  - Implementa i requisiti per i controlli di sicurezza nei progetti applicativi, OT e IOT
  - Verifica e valida politiche e procedure per la sicurezza delle informazioni di propria competenza
- **Responsabile Funzione Esercizio Applicativo (ITO-EAP)**
  - Garantisce l'implementazione dei controlli di sicurezza relativi all'esercizio applicativo;
  - Verifica e valida politiche e procedure per la sicurezza delle informazioni di propria competenza
  - Assicura lo svolgimento delle attività relative al funzionamento dei controlli per la sicurezza delle informazioni legati alla componente di esercizio
  - Partecipa alla management review del sistema di gestione
- **Responsabile Funzione Gestione Device (ITO-GED)**
  - Garantisce l'implementazione dei controlli di sicurezza relativi ai sistemi di informatica individuale e unità periferiche assegnate agli utenti
  - Verifica e valida le politiche e procedure per la sicurezza delle informazioni
  - Assicura lo svolgimento delle attività relative al funzionamento dei controlli per la sicurezza delle informazioni legati alla componente di sua competenza
- **Responsabile Funzione Protezione patrimonio, infrastruttura e TLC (PPT)**
  - Garantisce l'implementazione e il funzionamento dei controlli di sicurezza nell'ambito infrastrutturale e della gestione dei sistemi per la protezione del patrimonio e TLC
  - Assicura lo svolgimento delle attività relative al funzionamento dei controlli per la sicurezza delle informazioni legati alla componente infrastrutturale, di protezione del patrimonio e TLC
  - Verifica e valida le politiche e procedure per la sicurezza delle informazioni di propria competenza
- **Direzione Organizzazione e Risorse Umane (DORU) - Responsabile Qualità e Ambiente (QUA)**

- Coinvolto come verificatore dello sviluppo delle policy sulla gestione della Sicurezza delle Informazioni ha il compito di revisionare e controllare che le policy e le misure ideate siano messe in atto

- **Responsabile Compliance (CMP)**
  - Coinvolto come verificatore dello sviluppo delle policy sulla gestione della Sicurezza delle Informazioni ha il compito di revisionare e controllare che le policy e le misure ideate siano messe in atto

5. *ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA (Conformità GV.RR-02 NIS2)*

In conformità al requisito GV.RR-02 punto 1 dell'Allegato 2 alla Determinazione ACN n. 164179 del 14 aprile 2025, MM S.p.A. ha definito, approvato e formalizzato la propria organizzazione per la sicurezza informatica. Tale organizzazione è approvata dagli Organi di Amministrazione e Direzione aziendale ed è comunicata alle strutture competenti mediante il sistema documentale aziendale, il Manuale Organizzativo, il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e le procedure operative correlate. L'organizzazione per la sicurezza informatica individua ruoli, responsabilità, poteri decisionali e linee di riporto relativamente alla gestione dei rischi cyber, alla protezione delle informazioni, alla gestione degli incidenti, alla continuità operativa e agli adempimenti previsti dal D.Lgs. 138/2024. In particolare, sono formalmente individuati:

- l'Organo di Direzione e gli Organi Amministrativi per le attività di indirizzo e supervisione
- il Direttore ICT
- il Responsabile della Funzione Cybersecurity (DIS-CBE)
- il Responsabile della Sicurezza delle Informazioni
- il Referente per la Cybersicurezza e i punti di contatto previsti dalla normativa NIS2
- i Responsabili delle strutture ICT, OT e delle funzioni operative interessate
- i soggetti incaricati delle attività di monitoraggio, prevenzione e risposta agli incidenti

I ruoli e le responsabilità sopra descritti sono documentati, comunicati e applicati nell'ambito del SGSI e sono soggetti a riesame periodico in occasione delle revisioni organizzative, dei riesami della direzione, degli audit interni o a seguito di significative variazioni del contesto di rischio, al fine di garantirne la continua adeguatezza ed efficacia.

6. *FASI DEL PROCESSO*

Durante la fase di adozione delle politiche e procedure dell'ISMS, MM svolge attività volte a ridurre i rischi associati alle minacce alla sicurezza delle informazioni, seguendo il modello di controlli stabilito dallo standard ISO 27001:2022. Queste attività sono considerate fasi di un processo orientato alla sicurezza delle informazioni.

6.1. Approccio basato sul Rischio

La gestione del rischio per la sicurezza delle informazioni è attuata da MM secondo un approccio strutturato, proporzionato e documentato, coerente con i requisiti della ISO/IEC 27001:2022 relativi alla valutazione e al trattamento dei rischi e con le misure di gestione del rischio Cyber previste dalla Direttiva NIS2 e dal relativo recepimento nazionale. In tale ambito, MM adotta un approccio *All-Hazards*, considerando sia minacce Cyber sia eventi fisici, ambientali, tecnologici, organizzativi e sulla Supply Chain, che possano compromettere la riservatezza, l'integrità e la disponibilità delle informazioni, dei sistemi IT/OT e dei servizi essenziali.

Il processo prevede l'identificazione degli asset, delle minacce, delle vulnerabilità, degli scenari di rischio, degli impatti potenziali e dei rispettivi Risk Owner; la valutazione della probabilità e della severità degli eventi, inclusi gli impatti operativi, economici, reputazionali, regolamentari e sociali; la definizione di criteri di accettazione del rischio; l'individuazione delle opzioni di trattamento, quali mitigazione, trasferimento e accettazione formalizzata del rischio residuo; nonché il monitoraggio continuo dell'efficacia delle misure adottate.

Gli esiti dell'Analisi alimentano il Piano di Trattamento dei Rischi, la selezione dei controlli applicabili, il Riesame della Dichiarazione di Applicabilità (SoA), le attività di Business Continuity, Disaster Recovery, Incident Management, gestione delle vulnerabilità, sicurezza della catena di fornitura, formazione e Cyber Hygiene, assicurando un ciclo di miglioramento continuo e una risposta tempestiva all'evoluzione del contesto delle minacce.

6.2. Gestione della sicurezza delle informazioni nell'Organizzazione

6.2.1. Politiche, Procedure e Responsabilità Operative

MM ha sviluppato delle politiche per la sicurezza delle informazioni che sono state approvate dalla Direzione e comunicate al personale e alle parti esterne interessate. Le politiche, le procedure e gli standard di sicurezza di MM sono supportati da controlli e monitoraggi continui dei livelli di conformità. All'interno di tali politiche e procedure vengono delineate responsabilità specifiche per i vari ruoli coinvolti nei processi.

Le procedure operative sono documentate, comunicate e rese disponibili a tutti gli Utenti e ai terzi che ne necessitano. In caso di modifiche ai processi aziendali o ai sistemi e tecnologie utilizzati, l'organizzazione valuta nuovamente i potenziali impatti e rischi sulla sicurezza dei dati.

6.2.2. Organizzazione interna

MM ha stabilito un quadro di riferimento organizzativo per l'attuazione, la gestione e il controllo del SGSI in azienda. Sono state definite ed assegnate le responsabilità relative alla sicurezza delle Informazioni - cfr. *MSGSI_Manuale SGSI*.

I processi operativi sono separati per evitare conflitti di responsabilità, riducendo il rischio di uso improprio o modifiche non autorizzate degli asset dell'organizzazione - vedere MSGSI_Manuale SGSI e PL-ISMS002_AL_Politica per gli accessi logici.

6.2.3. Rapporti con Autorità e Gruppi Specialistici

Le attività concernenti la sicurezza delle Informazioni vengono coordinate dai rappresentanti delle diverse Strutture dell'organizzazione di MM in base ai ruoli ricoperti e alle attività svolte.

Le attività relative alla sicurezza delle informazioni includono l'instaurazione e il mantenimento di contatti con le autorità competenti in ambito protezione e sicurezza dei dati (ad esempio, Garante), nonché con gruppi specialistici o altre associazioni professionali frequentate da esperti della sicurezza delle informazioni (ad esempio, Clusit). Questo è fondamentale per garantire un aggiornamento continuo sull'evoluzione degli scenari di rischio esterni e delle contromisure. Tale attività consente di affrontare con maggiore preparazione eventuali incidenti di sicurezza e assicurare una risoluzione più tempestiva di tali incidenti e delle problematiche sottostanti, come indicato nel MSGSI_Manuale SGSI.

Nel caso di violazioni di dati personali, nel rispetto della normativa vigente e della politica di gestione dei data breach - vedi *IO045_DBS_Gestione Data Breaches per i Sistemi Informatici*, le comunicazioni all'Autorità di controllo dovranno avvenire entro i termini di 72 ore dal momento dell'avvenuta conoscenza del caso, pena l'esposizione dell'azienda al rischio di ingenti sanzioni, richieste di danni e perdita di immagine.

6.2.4. Information Security in Project Management

MM definisce una strategia per la sicurezza delle Informazioni adeguata, completa e strutturata, articolata sui seguenti contenuti:

- raggiungimento degli obiettivi di sicurezza in tutti gli ambiti tramite misure ed interventi omogenei e coerenti;
- approccio Security by Design alla sicurezza delle informazioni, valutando i requisiti di sicurezza delle informazioni all'interno di tutti i nuovi progetti;
- utilizzo delle valutazioni sul rischio informatico per stabilire la maturità e l'efficacia dei controlli di sicurezza;
- attribuzione di priorità ai controlli di sicurezza che hanno come scopo la prevenzione delle minacce, rispetto a quelli con finalità di mitigazione degli impatti derivanti dagli incidenti;
- distribuzione delle misure di sicurezza su diversi livelli, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità");
- garanzia che l'implementazione di ogni controllo di sicurezza includa le modalità ed i meccanismi adeguati a verificarne l'efficacia e la corretta attuazione nel tempo.

MM si impegna a sostenere con risorse adeguate l'attuazione del Sistema di Gestione per la Sicurezza delle Informazioni e il suo miglioramento continuo, al fine di raggiungere tutti gli obiettivi fissati e soddisfare tutti i requisiti identificati.

6.2.5. Gestione degli asset

La gestione degli asset segue procedure basate sullo schema di classificazione di MM, il quale identifica categorie di asset, rischi e misure di sicurezza per mitigarli. MM mantiene un inventario dei beni con l'indicazione della proprietà - fare riferimento al documento *PG-ISMS017_GCVA_Gestione Ciclo vita asset*. Tali inventari includono i dispositivi assegnati agli Utenti (ad esempio laptop, smartphone). La responsabilità dell'aggiornamento del registro degli asset ricade sulle funzioni responsabili degli stessi, come indicato nel *MOIT_MOIT Manuale Organizzativo IT*.

MM ha implementato misure di sicurezza per la gestione dei rischi derivanti dall'uso di dispositivi mobili, al fine di garantire che le Informazioni non siano compromesse, e valuta i possibili rischi derivanti dallo svolgimento di un'attività lavorativa in un ambiente non protetto da parte degli Utenti e di terzi. A tal scopo sono implementati controlli che riguardano la politica 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.

Al termine del periodo di impiego e/o di collaborazione, gli Utenti e i terzi devono riconsegnare i beni a loro assegnati da MM.

L'organizzazione documenta e attua apposite regole per il corretto uso delle Informazioni e dei beni di MM contenenti le Informazioni o adibiti al trattamento delle stesse - cfr. *RG-ISMS012_RUSI_Regolamento* uso strumenti informatici consegnato ai dipendenti e collaboratori durante la fase di Onboarding del nuovo personale.

MM definisce le procedure necessarie allo smaltimento sicuro dei supporti media quando non più necessari, al fine di prevenire qualsiasi divulgazione non autorizzata delle informazioni

- cfr. *PG-ISMS017_GCVA_Gestione Ciclo vita asset*.

MM, inoltre, attua misure di sicurezza necessarie a proteggere le Informazioni accessibili, trattate o memorizzate presso i c.d. siti di telelavoro. Sono definite le condizioni di sicurezza per il telelavoro vedi *PL-ISMS006_SISW_Politica per la sicurezza delle informazioni in Smart working*.

6.2.6. Controllo accessi

MM adotta una politica di controllo degli accessi conforme alle norme aziendali relative alla sicurezza delle informazioni, come delineato nella politica *PL-ISMS002_AL_Politica per gli accessi logici*. MM ha formalizzato e implementato procedure per la gestione degli account utente che garantiscono la sicurezza delle informazioni durante le fasi di creazione, aggiornamento e cancellazione degli account stessi. Tali procedure includono processi per garantire che tutte le richieste di creazione di account siano correttamente autorizzate dai responsabili delle informazioni o da loro delegati e processi per monitorare gli account non più necessari al fine della loro cancellazione. Richieste ed autorizzazioni sono opportunamente tracciate.

Per le utenze privilegiate sono previsti particolari controlli che consistono nella limitazione degli accessi ai casi di necessità, previa autorizzazione, con livelli di privilegi non eccedenti e con tracciamento degli accessi effettuati. Gli Utenti titolari di account privilegiati utilizzano un account separato (cioè non privilegiato) per lo svolgimento delle normali funzioni aziendali.
I vari gruppi di sistemi informatici, di servizi e di Utenti sono distinti secondo criteri basati sulla necessità di accedere ai dati da parte degli utenti (ad esempio, le credenziali di ciascun Utente consentono l'accesso solo ai sistemi per i quali si è ricevuta autorizzazione).

Gli Utenti accedono solo alle applicazioni e ai servizi per i quali hanno ricevuto una specifica autorizzazione. L'accesso remoto ai sistemi e alle applicazioni interne è disciplinato da adeguati controlli di autenticazione e crittografia. L'accesso alla rete e ai servizi di rete è consentito solo agli Utenti e ai terzi specificamente autorizzati.
L'accesso fisico e logico alle funzionalità di monitoraggio e di configurazione è limitato ad alcuni Utenti.
L'accesso alle utilità ed agli strumenti di sistema che sono in grado di superare i controlli di sicurezza esistenti è limitato al personale della Direzione ICT autorizzato.

L'accesso ai sistemi operativi, alle basi dati ed alle applicazioni avviene mediante meccanismi di log-on sicuri.
I titolari di un nuovo account ricevono una password, da modificare al primo login, comunicata insieme all'account in accordo con la password policy contenuta nel Regolamento - vedi *RG-ISMS012_RUSI_Regolamento* uso strumenti informatici. Le password devono essere custodite dagli utenti in maniera riservata, modificate secondo le Password Policy e ogniqualvolta vi sia un sospetto di compromissione.

6.2.7. Relazioni con i fornitori

Con l'obiettivo di assicurare la protezione delle Informazioni di MM accessibili ai fornitori, MM concorda con il fornitore, nel contratto, i requisiti per garantire la sicurezza delle Informazioni al fine di limitare i rischi associati all'accesso non autorizzato, alla divulgazione non autorizzata e alla perdita di disponibilità e integrità. Tali Informazioni, infatti, potrebbero essere compromesse dal fornitore a causa di una gestione inadeguata.

In particolare, i requisiti in materia di sicurezza delle Informazioni sono definiti e concordati con ciascun fornitore che abbia la possibilità di accedere, trattare, archiviare, comunicare informazioni di MM o fornire componenti di infrastrutture informatiche di MM. Tali accordi con i fornitori devono prevedere disposizioni relative alla gestione dei rischi per la sicurezza delle Informazioni.

MM monitora, controlla e sottopone regolarmente ad audit i servizi di fornitura per quanto riguarda gli aspetti relativi alla sicurezza di Informazioni sensibili o critiche. Particolare attenzione è data agli aspetti di sicurezza che i fornitori si devono impegnare a far rispettare nei confronti di altri eventuali subfornitori nella catena delle forniture legate al servizio. Gli accordi con i fornitori includono i requisiti per affrontare i rischi relativi alla sicurezza delle Informazioni associati ai servizi e ai prodotti della filiera di fornitura per l'ICT.

In linea con i requisiti di sicurezza della catena di approvvigionamento (D.Lgs. 138/2024), MM definisce criteri minimi di sicurezza informatica per la qualificazione dei propri fornitori di beni e servizi ICT e OT. I contratti includono clausole stringenti sull'obbligo di notifica immediata di incidenti da parte del fornitore e sulla trasparenza nella gestione delle vulnerabilità e delle patch.

Tali accordi, qualora prevedano il trattamento di dati personali di cui MM è titolare, dovranno includere un incarico ai fornitori come responsabili del trattamento (art. 28 GDPR). Tale incarico, controfirmato dal fornitore, deve elencare le misure tecniche e organizzative ritenute adeguate ai fini del rispetto della normativa sulla privacy e delle policy e procedure emanate, in materia, da MM. Il rispetto degli accordi potrà essere monitorato da MM riservandosi, contrattualmente, il diritto di audit.

Gli audit sono effettuati internamente dalla funzione preposta DIS, la cui responsabilità è indicata nel manuale organizzativo aziendale.

Inoltre, MM gestisce le modifiche alle disposizioni regolanti la prestazione di servizi da parte dei fornitori, incluse la manutenzione e il miglioramento di politiche, procedure e controlli vigenti sulla sicurezza delle Informazioni, tenendo conto della criticità delle Informazioni aziendali, dei sistemi e processi coinvolti e della ridefinizione dei rischi.

Le misure tecniche ed organizzative previste da norme e leggi nazionali ed internazionali in vigore devono essere integrate nei piani di sicurezza informatica delle terze parti, inoltre, le migliori *best practices* nazionali e internazionali devono essere considerate come riferimento per l'implementazione di misure specifiche.

In caso di trasferimento di Informazioni verso qualsiasi entità esterna, è necessario mantenere la sicurezza delle Informazioni trasferite.
In caso di trasferimento di Informazioni verso parti esterne, devono essere formalizzati degli accordi e/o clausole contrattuali appositi e, in caso il trasferimento o la condivisione riguardi dati che sono ritenuti critici per il business o da tutelare ai sensi della normativa vigente, devono essere formalmente stipulati degli accordi di riservatezza o di non divulgazione.

MM, in fase di stesura di contratto con i fornitori e per tutta la durata contrattuale, identifica, controlla, regolamenta e documenta gli obblighi e i patti di riservatezza o di non divulgazione a tutela delle esigenze aziendali di protezione delle Informazioni.

I patti di riservatezza e non divulgazione sono volti a garantire il più possibile la tutela delle Informazioni organizzative e, inoltre, informano i firmatari del loro obbligo di proteggere, utilizzare e non divulgare le Informazioni ricevute. Questi devono riflettere le necessità aziendali per la protezione delle Informazioni e devono essere riesaminati periodicamente.

I fornitori, in considerazione della specificità di ogni tipo di servizio e della tipologia di fornitore, sono sottoposti a particolari verifiche in fase di valutazione delle offerte tecniche circa le modalità con le quali il fornitore offre possibilità di avere visione e comprensione del programma di sicurezza per la tutela delle informazioni da questo gestite, della sua evoluzione in caso di cambiamenti e delle possibilità offerte al cliente di interagire, avere spiegazioni, garanzie e possibilità di verifica diretta cfr.*PL-ISMS004_STP_Gestione della sicurezza delle informazioni nei rapporti con i fornitori*.

6.2.8. Gestione degli incidenti relativi alla sicurezza delle informazioni

MM minimizza le conseguenze e l'impatto di eventuali violazioni della sicurezza delle Informazioni all'interno dell'azienda, andando ad attuare tutte le azioni necessarie per contrastare l'incidente e contenere gli impatti prodotti da quest'ultimo al fine di ripristinare prontamente la situazione antecedente la violazione. A tal riguardo, MM ripartisce ruoli e responsabilità e adotta le procedure di gestione necessarie a garantire una risposta rapida, efficace e ordinata agli incidenti di sicurezza. MM, inoltre, sviluppa e attua procedure formali di gestione degli incidenti relativi alla sicurezza delle Informazioni.

Ove richiesto dalle normative vigenti MM segnalerà eventuali incidenti di rilevanza per gli organi preposti (ACN)

Gli Utenti che utilizzano sistemi e servizi informatici annotano e riferiscono il più velocemente possibile mediante appositi canali di gestione tutti i casi riscontrati o sospetti di criticità nella sicurezza dei sistemi o servizi informatici.

Tutti gli Utenti sono formati e sensibilizzati sull'obbligo di riferire il più velocemente possibile qualsiasi evento relativo alla sicurezza delle Informazioni e delle procedure per la relativa comunicazione e agli stessi vengono comunicati i contatti della persona a cui tali eventi vengono riportati.

Nel caso di incidenti classificati come "significativi" ai sensi del D.Lgs. 138/2024, MM S.p.A. provvede all'inoltro formale delle notifiche obbligatorie verso il CSIRT Italia (ACN) rispettando le tempistiche di legge (pre-notifica entro 24 ore, notifica dettagliata entro 72 ore, e relazione finale entro un mese).

Successivamente alla loro comunicazione e raccolta, gli eventi relativi alla sicurezza delle Informazioni vengono valutati al fine di stabilire se essi debbano essere classificati come incidenti relativi alla sicurezza delle Informazioni. In quest'ultimo caso, MM reagisce come previsto nelle procedure documentate prevedendo eventuali escalation in funzione del livello di severità dell'incidente. L'obiettivo primario della risposta a tali incidenti è sempre il ripristino di un "livello di sicurezza normale" e il conseguente avvio del necessario processo di recupero.

La raccolta oltreché in maniera reattiva (identificazione di eventi di sicurezza mediante "Notifica" da parte dei soggetti segnalanti o mediante il processo di Gestione degli Incidenti di Sicurezza – cfr PG-ISMS015_GIS_Gestione Incidenti Sicurezza) può avvenire in maniera proattiva (allarmi dalle piattaforme di monitoraggio delle infrastrutture IT/OT).

L'esperienza acquisita dall'analisi e dalla risoluzione degli incidenti di sicurezza delle Informazioni è impiegata per ridurre la probabilità o la portata di futuri problemi. MM elabora ed applica le procedure necessarie all'identificazione, alla raccolta, all'acquisizione e alla conservazione delle Informazioni che possano servire come prova in tal senso, servendosi di Piattaforme di Monitoraggio e sistemi di registrazione/tracciatura degli eventi di sicurezza

6.2.9. Aspetti di sicurezza delle informazioni nella gestione della continuità operativa

MM eroga servizi essenziali a un grande numero di Utenti e le interruzioni di tali servizi possono avere impatti gravi sul business e sulla salute e sicurezza dei clienti.

Sono quindi implementate misure di sicurezza tecniche ed organizzative al fine di evitare o ridurre al minimo possibile il rischio di interruzione dei servizi derivante da minacce e vulnerabilità - intenzionali, accidentali o ambientali - legate alle Informazioni.

I sistemi di Business Continuity (BCMS) e Disaster Recovery (DR) di MM S.p.A. sono allineati ai requisiti dello standard ISO 22301 e alla normativa NIS2, prevedendo test periodici (almeno annuali) di ripristino dell'operatività dei servizi critici IT e OT/SCADA.
e la revisione delle strategie di gestione delle crisi da parte dell'Organo di Direzione.

- definisce le norme per la gestione della sicurezza delle Informazioni e della continuità operativa in situazioni impreviste (ad es. durante una crisi o una calamità).
- definisce un piano di continuità operativa (Business Continuity Plan o BCP) e il piano di disaster recovery (Disaster Recovery Plan o DRP), al fine di assicurare la continuità operativa in caso di eventi avversi di interruzione del servizio o in caso di calamità naturali.

All'interno del piano di continuità dell'azienda MM definisce modalità e tempi di ripristino dei sistemi in caso di eventi avversi. Se le cause degli eventi avversi non sono di natura ICT la responsabilità della gestione dei piani di continuità e il ripristino alle condizioni di normale funzionamento sono affidate alle Direzioni competenti (Facility e/o Direzioni Operative).

- prevede e attua controlli periodici della continuità e della sicurezza delle Informazioni al fine di garantire che il BCP e il DRP siano strumenti validi ed efficaci in caso di situazioni critiche.

- effettua analisi periodiche biennali, in assenza di cambiamenti sulla infrastruttura tecnologica, con il business di MM per valutare l'impatto di un evento informatico eccezionale sulla continuità di business

L'approccio di MM alla gestione della sicurezza delle Informazioni e della continuità operativa e la relativa attuazione (i.e. obiettivi di controllo, controlli, politiche, processi e procedure per la sicurezza delle Informazioni, procedure per la continuità operativa) sono oggetto di revisione tramite audit interni ed esterni coordinati da DIS-CBE, la quale definisce per ciascun contesto IT e OT i processi e le aree di controllo sottoposte ad audit in funzione dei nuovi requisiti provenienti da DICT e di nuove normative o regolamenti applicabili e si occupa di redigere un Programma di Audit, nel quale sono riportati il contesto, i processi e le aree di controllo da verificare, i Team esterni o interni di audit che avranno in carico l'esecuzione dell'audit e le date in cui questi si terranno.

Dal momento che MM dispone di due DataC TIER 4 geograficamente distanti tra loro, dove sono ubicati i server nonché i terminali dei sistemi di comunicazione interni ed esterni, tali per cui eventi naturali disastrosi (terremoto, esondazioni, ecc.) di una magnitudine sufficiente ad interessare una parte importante della città di Milano con conseguenze su entrambe le sale CED risulta fortemente improbabile, si è convenuto di non predisporre in modo generalizzato sistemi ridondati a tempo di ripristino 0 per far fronte a un blocco derivante da evento disastroso.

6.2.10. Monitoraggio del SGSI

Le politiche, le procedure e gli standard di sicurezza di MM sono affiancati dal controllo e dal monitoraggio continuo dei livelli di compliance.

MM adotta strumenti di monitoraggio e controllo volti a:

- valutare le prestazioni in termini di efficacia ed efficienza del sistema di gestione per la sicurezza delle Informazioni;
- identificare le aree di debolezza al fine di comprenderne le cause e poter intervenire con opportune azioni correttive finalizzate al miglioramento continuo;

All'interno di politiche e procedure sono attribuite responsabilità per i diversi ruoli coinvolti nei processi.

6.2.11. Gestione della sicurezza delle informazioni nei rapporti con il personale

La sicurezza delle Informazioni può essere influenzata negativamente da comportamenti e attività svolte dalle persone nelle proprie attività lavorative: la persona, le sue competenze e la sua consapevolezza circa le modalità sicure per lo svolgimento delle sue attività costituisce un anello importante per la sicurezza delle informazioni.

Per tale ragione sono previsti controlli per la sicurezza delle informazioni legati alla gestione del rapporto con il dipendente, nelle fasi di selezione, assunzione, formazione, ed anche nella fase che segue l'interruzione del rapporto lavorativo.

Durante il processo di selezione e screening dei candidati viene svolta una valutazione rispetto a requisiti di etica e capacità professionale e di aderenza alle competenze richieste in base al ruolo.

Nella fase di assunzione sono formalizzati gli elementi di sicurezza ai quali il dipendente dovrà attenersi per la protezione del patrimonio informativo, che formano parte integrante del contratto sottoscritto fra l'azienda e il dipendente. Durante l'impiego sono assicurati costanti aggiornamenti sui temi della sicurezza delle informazioni.

DICT implementa processi di:

- informazione, intesa come il complesso di attività dirette a fornire conoscenze utili alla identificazione, alla riduzione dei rischi per la gestione della sicurezza delle Informazioni;
- formazione, intesa come il processo educativo attraverso il quale trasferire a dipendenti, collaboratori e altri soggetti le conoscenze e le procedure utili all'acquisizione di competenze per lo svolgimento sicuro dei rispettivi compiti nella gestione delle Informazioni (sviluppatori, tecnici ICT, amministrazione, gestione del personale, ecc.);
- consapevolezza, intesa come il complesso di attività dirette a sensibilizzare personale e collaboratori sui potenziali rischi di sicurezza associati a specifici comportamenti e fenomeni (social engineering, phishing, ecc.).

Al termine dell'impiego e/o ad ogni sua variazione vengono tutelati gli interessi aziendali definendo i doveri relativi alla sicurezza delle Informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro; tali obblighi vengono comunicati al personale o ai collaboratori e resi effettivi. Le conseguenze degli inadempimenti e le violazioni del dipendente rispetto alle norme aziendali, comprese quelle in tema di sicurezza delle informazioni, sono disciplinate sulla base dei rispettivi contratti applicati.

Tale Politica costituisce il quadro di riferimento per la definizione degli obiettivi di sicurezza delle informazioni, per l'assegnazione delle responsabilità, per l'attuazione dei controlli organizzativi, tecnici e procedurali e per il miglioramento continuo del sistema di gestione.

MM richiede al personale, ai collaboratori e ai soggetti terzi che operano sotto il controllo dell'organizzazione il rispetto dei requisiti applicabili in materia di sicurezza delle informazioni, inclusi requisiti normativi, regolamentari, contrattuali, di protezione dei dati personali, di continuità operativa e di cybersecurity, con particolare riferimento al GDPR, alla normativa NIS2 applicabile e agli standard del SGSI.

La Politica per la sicurezza delle Informazioni e le relative procedure operative sono comunicate al personale mediante canali aziendali ufficiali, attività formative, campagne di awareness e strumenti documentali disponibili sulla intranet aziendale. MM verifica periodicamente che il personale sia consapevole dei propri obblighi, delle responsabilità assegnate e delle conseguenze derivanti dal mancato rispetto delle prescrizioni di sicurezza.

Il personale contribuisce al miglioramento continuo del SGSI attraverso la corretta applicazione delle politiche e procedure aziendali, la tempestiva segnalazione di eventi, anomalie, vulnerabilità o incidenti di sicurezza, nonché la partecipazione ai programmi di formazione, sensibilizzazione, verifica periodica dell'efficacia dei controlli e riesame delle misure applicate.

6.3. Gestione della sicurezza delle informazioni nella Sicurezza fisica e ambientale

6.3.1. Aree sicure

Tutte le apparecchiature sono protette con meccanismi di limitazione, autorizzazione e controllo degli accessi. I controlli degli accessi non sono disattivati e restano in sicurezza in caso di guasto all'alimentazione o al sistema di controllo- cfr. *PG-ISMS003_SICF_Politica per la sicurezza fisica e ambientale*.

MM ha implementato misure di protezione dei locali, degli uffici e degli impianti da calamità naturali, incidenti o attacchi malevoli.

I documenti e le altre Informazioni sono conservati in luoghi chiusi a chiave quando non utilizzati. Per tale ragione, gli Utenti hanno accesso ad armadi sicuri in cui custodire tali documenti di lavoro.

Vengono inoltre correttamente attuate tutte le procedure relative alla sicurezza sul lavoro.

6.3.2. Gestione degli Asset

Le apparecchiature ICT/OT/IoT indicate negli inventari degli asset – vedi *PG-ISMS017_GCVA_Gestione Ciclo vita asset* - sono collocate e conservate in modo sicuro al fine di minimizzare sia i rischi derivanti da minacce sia i pericoli ambientali o gli accessi non autorizzati *PG-ISMS003_SICF_Politica per la sicurezza fisica e ambientale*. Adeguati livelli di protezione sono, inoltre, previsti per le apparecchiature non custodite.

Sono altresì previsti meccanismi di controllo e registrazione degli accessi assieme a meccanismi di rilevamento delle intrusioni (sistemi di allarme) e di presidio (sistemi di videosorveglianza) nel rispetto delle normative vigenti in materia di privacy.

Le apparecchiature ICT sono sottoposte ad appropriata manutenzione al fine di assicurarne l'Integrità e la continua disponibilità.

Le apparecchiature ICT non sono trasferite all'esterno senza autorizzazione. MM ha adottato delle misure di sicurezza in grado di far fronte ai possibili rischi derivanti dallo svolgimento delle attività al di fuori delle sedi MM. Prima di procedere alla dismissione o al riutilizzo delle apparecchiature ICT che contengono supporti di memorizzazione, viene assicurato dalla funzione preposta che siano stati preventivamente rimossi software coperti da licenza e Informazioni classificate diversamente da pubbliche.

Le apparecchiature ICT sono protette da eventuali cali o interruzioni di potenza causati da guasti alle strutture di supporto.

I cavi elettrici e i cavi delle telecomunicazioni a supporto dei servizi informatici o di trasporto dati sono protetti da eventuali intercettazioni o danneggiamenti.

6.3.3. Politica Clean Desk e Clean Screen

MM adotta la clean desk and clear screen policy *cfr. PL-ISMS011_CDCS_Politica clean desk clean screen*.
All'interno di tutti i luoghi di lavoro ove vengono trattati dati aziendali, si deve applicare la politica di schermo e scrivania puliti, ossia devono essere adottate sia una politica di "scrivania pulita" per i documenti e i supporti di memorizzazione rimovibili, sia una politica di "schermo pulito" per i servizi di elaborazione delle Informazioni.

6.4. Gestione della sicurezza delle informazioni con le Tecnologie

6.4.1. Protezione dalle minacce informatiche

MM adotta servizi di Threat Intelligence per identificare e mitigare tempestivamente minacce e vulnerabilità, con l'obiettivo di prevenire potenziali rischi futuri. A tal fine, mantiene operativi servizi che garantiscono un accesso immediato a tali informazioni e riceve report periodici provenienti dal Security Operation Center (SOC), da piattaforme di monitoraggio esterno gestite da fornitori affidabili e dalle autorità competenti nella divulgazione delle informazioni sulle minacce informatiche. Questo approccio consente una migliore identificazione delle specifiche vulnerabilità negli ambienti target, come descritto nella procedura *PG-ISMS018_GVUL_Procedura di Gestione delle Vulnerabilità*. Sulla base di queste informazioni di Threat Intelligence, MM implementa controlli adeguati a rilevare, prevenire e riparare eventuali danni ai sistemi informatici in caso di eventi avversi, quali l'accesso non autorizzato o l'installazione di malware.

Oltre all'installazione di sistemi di protezione degli Endpoint e dei Server (es. EDR), vengono anche adottate le seguenti misure riportate nella procedura *PL-ISMS020-RET_Politica Protezione Reti*:

- Firewall che costituiscono un sistema di difesa perimetrale;
- Soluzioni di ripristino dei dati tramite sistemi di backup che permettono di riattivare i sistemi con un tempo variabile a seconda della criticità;
- Rete di dati a fibra ottica ridondata con doppi circuiti per garantire la comunicazione in caso di manomissioni;
- Segmentazione della rete al fine di contenere la propagazione di malware, virus, o altri attacchi;
- Pianificazione di Vulnerability Assessment sulla rete perimetrale;
- Sistemi di protezione dei server pubblici;
- Sistema di web filtering per la navigazione sicura;
- Sistemi di applicazioni specifiche orientate al controllo di attività sospette;
- Monitoraggio costante dei Data Center per prevenire il traffico anomalo;
- Regole di autenticazione formalmente documentate.

A tali controlli viene affiancata un'attività mirata e volta a fornire agli Utenti l'opportuna formazione in materia di Cybersecurity.

6.4.2. Gestione della vulnerabilità tecnica

MM ha sviluppato e attua adeguati processi di gestione delle patch, che includono controlli relativi al monitoraggio e test delle patch prima dell'installazione.

Sono adottati sistemi e procedure per garantire un rapido contenimento degli effetti delle vulnerabilità quando le patch definitive non sono immediatamente disponibili. Nei casi in cui i sistemi siano obsoleti e le patch non più reperibili, si ricorre al Virtual Patching e alla segregazione dell'applicativo come soluzioni alternative.

6.4.3. Backup

Tutti i dati e le Informazioni aziendali presenti nei server sono sistematicamente sottoposti a backup tramite salvataggio periodico.

Le procedure operative verificano che il backup sia completato positivamente. I dati sottoposti a backup sono archiviati in luoghi sicuri e al riparo dai rischi ambientali.

I supporti di backup sono collocati ad una distanza tale da consentire che siano disponibili in caso di grave guasto presso le sedi di MM e non siano compromessi qualora si verificasse una calamità naturale nella zona.

6.4.4. Monitoraggio delle Attività

MM monitora in modo continuativo la rete e i sistemi per individuare comportamenti anomali che possano determinare un rischio per la sicurezza delle informazioni e intraprende le azioni necessarie a prevenire o gestire eventuali incidenti di sicurezza.

Per raggiungere questo obiettivo, sono implementate, dalla funzione di competenza indicata nel manuale organizzativo, attività di controllo utilizzando strumenti per la scansione del traffico di rete. Attraverso configurazioni appropriate si attivano i log di accesso ai server e alle applicazioni critiche (audit log ovvero accessi, disconnessioni e tentativi di accesso non riusciti). Questi dati vengono raccolti e analizzati mediante eventi segnalati dai sistemi di Endpoint Protection. Le informazioni sono quindi convogliate verso strumenti di gestione degli eventi di sicurezza informatica (SIEM) per una gestione efficace.

MM mantiene sotto controllo processi di Change Management che garantiscono l'inalterabilità del codice sorgente, così come controlli che garantiscono che non venga superata la capacità elaborativa mettendo a rischio la disponibilità dei dati e la continuità dei servizi.

I sistemi di ticketing conservano i log track dei malfunzionamenti in un sistema dedicato.

6.4.5. Sicurezza delle comunicazioni e della rete

I servizi di rete comprendono la fornitura di accesso a Internet, servizi di rete locale (LAN) e soluzioni avanzate per la gestione della sicurezza di rete, come firewall e sistemi di rilevamento delle intrusioni (IDS) o di prevenzione delle intrusioni (IPS). I dettagli tecnico operativi sono illustrati nel documento *PL-ISMS-RET_Politica Protezione Reti*.

La rete di MM è gestita e controllata in modo da proteggere le Informazioni presenti nei sistemi e nelle applicazioni. Al fine di realizzare questo obiettivo, MM stabilisce le procedure di gestione degli apparati di rete, gestisce in maniera sicura le connessioni dei sistemi alla rete MM, utilizza sistemi di Content Filtering che permettono l'accesso solo ai siti autorizzati dall'azienda.

I meccanismi di sicurezza, i livelli di servizio e le norme di gestione di tutti i servizi di rete sono, inoltre, identificati e inclusi nei contratti di servizio.

Le connessioni da remoto effettuate tramite PC aziendali utilizzano un sistema di rete privata virtuale (VPN) basato su IPSec. I meccanismi di autenticazione per questi dispositivi adottano un sistema a due fattori e impiegano un tunnel criptato per le comunicazioni, con idonei controlli di registrazione e monitoraggio.

Per garantire la protezione dei dati aziendali, è fondamentale mantenere la sicurezza delle informazioni scambiate sia all'interno dell'azienda sia con qualsiasi entità esterna, indipendentemente dal mezzo di comunicazione utilizzato. Nel caso di trasferimento di informazioni al di fuori della sede di lavoro tramite supporto fisico, è necessario seguire regole specifiche e ottenere previa autorizzazione.

Gli utenti sono tenuti ad archiviare, processare o trasferire le informazioni di MM esclusivamente tramite apparecchiature di proprietà di MM o configurate e gestite da quest'ultimo. Inoltre, devono conservare i documenti ad uso aziendale nelle apposite infrastrutture aziendali di archiviazione, al fine di garantire la custodia centralizzata delle informazioni e l'esecuzione dei backup necessari. Questo requisito si applica sia ai computer personali, sia agli altri dispositivi mobili di connessione (ad esempio, smartphone, supporti di memorizzazione esterna ecc.).

L'utilizzo della posta elettronica e di altri strumenti di messaggistica elettronica come mezzo per lo scambio di dati è regolamentato nel documento *RG-ISMS012_RUSI_Regolamento* sull'uso degli strumenti informatici.

6.4.6. Controlli Crittografici

MM ha stabilito una Politica sull'uso dei controlli crittografici e la gestione delle chiavi, consultabile nel documento *PL-ISMS007_CCR_Politica dei controlli crittografici e gestione delle chiavi*, allo scopo di garantire l'impiego corretto ed efficace della crittografia.
Particolare enfasi è posta sui processi di gestione delle chiavi.

6.4.7. Acquisizione, sviluppo e manutenzione dei sistemi

Le informazioni relative ai servizi applicativi che transitano su reti pubbliche sono protette contro attività fraudolente, divulgazione e modifiche non autorizzate. Questa protezione è garantita attraverso l'implementazione di controlli crittografici e l'utilizzo di protocolli di accesso e navigazione sicuri come HTTPS

DIS ha stabilito linee guida rigorose per l'adozione di tecniche di sviluppo sicuro di software e sistemi, applicandole in tutte le attività di sviluppo svolte all'interno dell'organizzazione. In questo contesto, la sicurezza delle informazioni è integrata a ogni livello dell'architettura (dati, applicazioni e tecnologia), mantenendo un equilibrio tra le necessità di sicurezza e quelle di accessibilità.

MM supervisiona e monitora l'attività di sviluppo dei sistemi quando questa viene affidata a terzi. MM ha sviluppato, ove possibile, procedure specifiche per la manutenzione e il controllo dei codici sorgente di programma e delle librerie eseguibili sviluppati internamente ed esternamente. MM gestisce le modifiche apportate ai sistemi durante il loro ciclo di vita attraverso l'utilizzo di procedure formali di gestione delle modifiche, garantendo un approccio coerente alle fasi di avvio, esecuzione e gestione delle modifiche necessarie alle varie applicazioni e ai sistemi software. In caso di modifica delle piattaforme operative, MM procede alla revisione e al collaudo delle applicazioni aziendali critiche per prevenire eventuali conseguenze negative sulle operazioni dell'organizzazione o sulla sicurezza delle informazioni.

Il collaudo delle funzionalità di sicurezza viene eseguito durante la fase di sviluppo. MM implementa processi di collaudo per i nuovi sistemi informatici, gli aggiornamenti e le nuove versioni.

Qualora le funzionalità di sicurezza di un determinato prodotto non soddisfino i requisiti indicati, MM valuta i rischi che il prodotto può generare, ed effettua i necessari controlli prima di procedere all'acquisto dello stesso.

MM utilizza di ambienti separati per lo sviluppo & test e per la produzione, in modo da ridurre il rischio di accessi o modifiche non autorizzate al codice sorgente e/o configurazioni. MM assicura inoltre che all'interno dell'ambiente di test non siano presenti dati reali.

6.4.8. Gestione delle Configurazioni

Il processo di gestione del cambiamento traccia i requisiti di configurazione per le applicazioni, come indicato nel documento *PG-ITSIC004_PCM_Processo Change Management*. La documentazione relativa alle configurazioni adottate è disponibile presso i responsabili della gestione dei rispettivi asset, secondo il principio di ownership.

Le configurazioni dei servizi gestiti da terze parti sono definite contrattualmente, disponibili presso il fornitore e monitorate da MM secondo le modalità contrattuali previste.

6.4.9. Considerazioni sull'audit dei sistemi informativi

Le attività di audit che implicano il controllo dei sistemi informatici sono attentamente programmate e realizzate nel rispetto delle procedure di sostituzione previste da MM, al fine di ridurre eventuali interruzioni accidentali dell'attività aziendale.

6.5. Diffusione e modifiche alla politica

La politica per la sicurezza delle Informazioni, e il corpo documentale del sistema di gestione in essa richiamato, è conosciuto in quanto diffuso a tutti i livelli aziendali, ed è applicato da tutto il personale e i collaboratori di MM.

I rischi per la sicurezza delle informazioni relativi al Sistema di Gestione dei Servizi e per i Servizi devono essere valutati e documentati con cadenza regolare secondo quanto previsto nella procedura *PG-SISM002_GRD Gestione Riesame Direzione del SMS e ISMS*.

La politica per la sicurezza delle Informazioni è oggetto di revisione in sede di riesame della DICT al fine di verificarne contenuti e coerenza con gli obiettivi aziendali. La revisione è periodica, almeno su base annuale, al fine di riflettere le eventuali modifiche apportate ai regolamenti interni di MM o per adeguarsi agli standard internazionali in materia di sicurezza delle Informazioni.

7. ALLEGATI E RIFERIMENTI

7.1. Allegati

- N.A.

7.2. Riferimenti

- ISO/IEC 27001:2022
- Decreto Legislativo 4 settembre 2024, n. 138 (NIS2 recepimento nazionale).
- ISO/IEC 20000-1:2018 - Information Technology Service Management
- NIST Cybersecurity Framework v2.0
- MSGSI_Manuale SGSI
- MOIT_MOIT Manuale Organizzativo IT
- PL-ISMS002_AL_Politica per gli accessi logici
- PG-ISMS003_SICF_Politica per la sicurezza fisica ambientale
- PL-ISMS004_STP_Politica Gestione della sicurezza delle Informazioni nei rapporti con i fornitori
- PL-ISMS005_LOG_Politica di gestione dei log
- PL-ISMS006_SISW_Politica per la sicurezza delle informazioni in smartworking
- PL-ISMS007_CCR_Politica dei controlli crittografici e gestione delle chiavi
- PL-ISMS009_BKP_Politica di Backup
- PL-ISMS010_SBD_Politica di Security by Design
- PL-ISMS011_CDCS_Politica Clean Desk e Clean Screen
- RG-ISMS012_RUSI_Regolamento uso strumenti informatici
- PG-ISMS015_GIS_Gestione Incidenti Sicurezza
- PG-ISMS017_GCVA_Gestione Ciclo vita asset
- PG-ISMS018_GVUL_Gestione Vulnerabilità
- PG-ISMS013_AdR_Metodologia di analisi dei rischi per la sicurezza delle informazioni
- DC-SMS016 _PDCS_Piano di Disponibilità e Continuità del Servizio
- PG-ITSIC004_PCM_Processo Change Management
- PL-ISMS-RET_Politica Protezione Reti
- PG-SISM002_GRD Gestione Riesame Direzione del SMS e ISMS
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
- D.Lgs 4 settembre 2024, n. 138 Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148
- Determinazione ACN n. 164179 del 14 aprile 2025 – Specifiche di base per l'adempimento agli obblighi del D.Lgs. 138/2024
- Allegato 2 ACN – Misure di sicurezza per i soggetti essenziali, controlli GV.PO e GV.RR