POLITICA DELLA QUALITA' E SICUREZZA DELLE INFORMAZIONI

SOMMARIO

1. Introduzione

1.1. Premesse e perimetro applicativo della norma

Lo scopo del presente documento (di seguito indicato come Politica per la Sicurezza delle Informazioni) è quello di descrivere i principi generali di sicurezza delle informazioni che l'Associazione Cyber 4.0 ha fatto propri al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione per la qualità e della Sicurezza delle Informazioni ai sensi delle norme ISO/IEC 27001:2022 e ISO 9001:2015.
Tali principi sono concretizzati nel Manuale Integrato, Procedure, Istruzioni Operative, Regolamenti e nella ulteriore documentazione, interna ed esterna, in utilizzo aziendale ai fini della tutela della sicurezza delle informazioni e in relazione alle reali esigenze derivanti dalla tipologia di attività svolte dalla Cyber 4.0 nello specifico ambito di applicazione della suddetta norma.
L'ambito di applicazione del Sistema di gestione per la qualità e della Sicurezza delle Informazioni è il seguente:

"Servizi di orientamento e formazione alle imprese ed alla Pubblica Amministrazione. Attuazione di progetti di innovazione, ricerca industriale e sviluppo sperimentale in ambito nazionale ed internazionale finalizzati alla realizzazione e/o miglioramento di nuovi prodotti, processi o servizi nell'area tematica della cybersecurity".

Presso la sede operativa di Via Ardito Desio, 60 a Roma, sono ospitati, in ambienti dotati di idonee misure di sicurezza infrastrutturali sia fisiche che logico-informatiche, sistemi ed apparecchiature di elaborazione/gestione dati.
I suddetti locali garantiscono anche i seguenti servizi strumentali (c.d. "facilities"):

- Sistema di alimentazione elettrica diretta (sistema alimentazione primario) ed indiretta (sistemi di alimentazione di back up);
- Sistema di condizionamento ambientale;
- Misure di protezione antincendio.

Quanto successivamente descritto nel presente documento e nella ulteriore documentazione di riferimento per il Sistema di Gestione della Sicurezza delle Informazioni, deve essere inteso, dunque, come applicato esclusivamente al suddetto perimetro fisico-logico nonché ai processi, risorse e/o rapporti lavorativi (Personale dipendente/Collaboratori/Terzi aventi causa) correlati e/o connessi alla debita gestione in esercizio della suddetta infrastruttura nell'ambito dei più ampi e generali scopi aziendali.

La Cyber 4.0 fonda la propria organizzazione sui seguenti principi:

- Rispetto della legislazione vigente;
- Conformità del sistema di gestione;
- Competenza, professionalità ed imparzialità del personale;
- Coinvolgimento del personale nell'implementazione e nel miglioramento del sistema di gestione per la qualità e sicurezza delle informazioni;
- Adeguatezza della struttura e delle attrezzature;
- Erogazione dei servizi nel rispetto della normativa per la certificazione, della legislazione di riferimento e dei requisiti dei clienti;
- Aggiornamento tecnico del personale e delle attrezzature;
- Adeguatezza dell'organizzazione e del sistema di gestione per la qualità e sicurezza delle informazioni alle esigenze interne e del mercato.

L'operato dell'Associazione Cyber 4.0 rispetta i seguenti principi:

- Collaborazione con gli Enti di certificazione;
- Collaborazione con le imprese e gli enti serviti.

L'Alta Direzione inoltre:

- Fa in modo di rendere disponibili le risorse necessarie a garantire l'efficacia del Sistema di Gestione per la Qualità e sicurezza delle informazioni;
- Comunica ed aggiorna ogni anno gli orientamenti, gli impegni e gli obiettivi per la qualità e la sicurezza delle informazioni;
- Convoca periodicamente specifiche riunioni, affinché ad ogni livello sia nota e condivisa la necessità di soddisfare i requisiti previsti dai contratti e capitolati e per effettuare gli aggiornamenti richiesti dall'evoluzione delle norme cogenti;
- Garantisce che gli obiettivi della politica di qualità integrata siano definiti e compatibili con il contesto e la direzione strategica della società e che comprendano la sicurezza delle informazioni;
- Garantisce l'integrazione dei requisiti di sistema di gestione integrato nei processi di business aziendali;
- Promuove l'uso dell'approccio per processi e il pensiero basato sul rischio;
- Provvede affinché le risorse necessarie per il sistema di gestione della qualità integrata siano disponibili;
- Assicura che il sistema di gestione integrato raggiunga i risultati attesi;
- Coinvolge, dirige e sostiene il personale al fine di ottenere l'efficacia del sistema di gestione;
- Promuove il miglioramento;
- Fa in modo che la Politica aziendale sia comunicata e condivisa con tutti i dipendenti.

L'Alta Direzione si impegna inoltre a:

- Divulgare e promuovere la politica per la qualità e la sicurezza delle informazioni;
- Attuare la politica integrata attraverso la definizione di obiettivi di miglioramento;
- Riesaminare la politica integrata in funzione dei risultati raggiunti e delle strategie aziendali.
- Garantire la riservatezza delle informazioni attraverso la definizione puntuale delle responsabilità interne per la gestione dei servizi e delle informazioni ad essi connesse; il controllo degli accessi fisici e logici agli archivi elettronici e cartacei esclusivamente da parte di personale autorizzato e competente;
- Garantire l'integrità delle informazioni attraverso il controllo degli accessi fisici e logici agli archivi elettronici esclusivamente da parte di personale autorizzato e competente e la gestione dei back-up dei dati e delle configurazioni dei sistemi informativi;
- Garantire la disponibilità delle informazioni attraverso l'identificazione dei ruoli e delle funzioni, i diritti di accesso alle informazioni e agli assets aziendali per la gestione dei servizi al Cliente;
- A rispettare e applicare quanto indicato nella dichiarazione SOA (*Statement of Applicability*) nel rispetto del proprio campo di applicazione;
- Garantire che dipendenti, fornitori, partner, appaltatori e ogni altra terza parte coinvolta con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni, accettino gli obblighi e le responsabilità di propria pertinenza, al fine di proteggere le informazioni, i beni e le risorse di Cyber 4.0;
- che ogni accesso, di tipo fisico o informatico, sia autorizzato, controllato e monitorato sulla base dei seguenti criteri: (a) l'accesso è autorizzato al personale abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere); (b) l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati); (c) l'accesso alla struttura e ai locali è autorizzato al personale abilitato. L'accesso ai locali di Cyber 4.0 è autorizzato, controllato e monitorato in linea con la politica aziendale.

- che ogni dipendente, fornitore, associato e terza parte sia consapevole del proprio ruolo e dell'impatto delle proprie azioni sulla sicurezza delle informazioni.
- che ogni risorsa sia adeguatamente formata e addestrata sulle politiche e sulle procedure relative alla gestione della sicurezza delle informazioni.
- che i trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni inerenti la protezione delle informazioni di Cyber 4.0 o gestiti dalla stessa per conto dei propri clienti sono conformi alle leggi e ai regolamenti applicabili di natura cogente, contrattuale e volontaria.
- che ogni attività e risorsa di Cyber 4.0 o affidata da questa a terze parti, nonché ogni informazione pertinente l'ambito del SGSI, è protetta contro i problemi legati alla riservatezza, l'integrità e la disponibilità, in proporzione al loro valore e nel rispetto delle leggi vigenti.

Con l'integrazione del Sistema di Gestione per la qualità e Sicurezza delle Informazioni la Cyber 4.0 si prefigge la finalità di proteggere da tutte le minacce, interne o esterne, intenzionali o accidentali, il patrimonio informativo aziendale, ivi comprese le informazioni e i dati relativi a clienti e fornitori, oltre a mantenere e dimostrare la correttezza delle trattative con clienti e fornitori e di dare evidenza che i servizi erogati non causino direttamente o indirettamente un aumento dei rischi per i clienti.
Per il perseguimento di tali finalità, la Società ha individuato nella documentazione del Sistema di Gestione Integrato le modalità di valutazione e i criteri di gestione dei rischi, valutando gli investimenti economici che l'implementazione e il mantenimento del Sistema di Gestione potrà comportare.
Pertanto, la Direzione si impegna, nel rispetto dei requisiti cogenti, ad assicurare che:

- Le informazioni siano protette da accessi non autorizzati nel rispetto della riservatezza e siano disponibili solo agli utenti autorizzati;
- Le informazioni non vengano divulgate a persone non autorizzate a seguito di azioni deliberate o per negligenza e, nel rispetto dell'integrità, siano salvaguardate da modifiche non autorizzate;
- Vengano predisposti piani per la continuità dell'attività aziendale e che tali piani siano il più possibile tenuti aggiornati e controllati;
- Il personale riceva addestramento sulla sicurezza delle informazioni;
- Tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano riferiti a chi di dovere ed esaminati.

Attraverso l'attuazione di tale politica la Cyber 4.0 intende ottemperare all'impegno di conformità alla UNI CEI ISO/IEC 27001:2022 e UNI EN ISO 9001 nonché di conseguire e mantenere tali certificazioni. Per il conseguimento di tale obiettivo, la direzione si impegna a far sì che la presente politica sia diffusa, compresa e attuata non solo dal personale interno, ma anche da collaboratori esterni e fornitori che siano in qualsiasi modo coinvolti con le informazioni aziendali.
La Direzione si impegna infine a riesaminare regolarmente la politica ed eventuali modifiche o cambiamenti che la influenzino in ambito organizzativo, per accertarsi che permanga idonea all'attività e alla capacità di soddisfare i Clienti, i Fornitori e le altre parti interessate. Il riesame della stessa sarà comunque effettuato a seguito dell'annuale Riesame della Direzione.

1.2. Obiettivi del RGSI

La sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione.
In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere le seguenti proprietà delle stesse:

- **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;

- **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
- **Autenticità**: garantire la provenienza dell'informazione;
- **Non ripudio**: assicurare che l'informazione sia protetta da falsa negazione di ricezione, trasmissione, creazione, trasporto e consegna.

La mancanza di adeguati livelli di sicurezza, in termini di Riservatezza, Disponibilità, Integrità, Autenticità e Non Ripudio, può comportare, nell'ambito di una qualsiasi attività aziendale, il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.
La sicurezza delle informazioni è, quindi, un requisito fondamentale per garantire l'affidabilità delle informazioni trattate, nonché l'efficacia ed efficienza dei servizi erogati dalla Cyber 4.0.
Di conseguenza, è essenziale per la società identificare le esigenze di sicurezza sia di natura esterna che derivanti dal cogente.
Tale attività viene realizzata attingendo a diverse fonti:

- **Analisi dei rischi:** consente all'azienda di acquisire la consapevolezza e la visibilità sul livello di esposizione al rischio del proprio sistema informativo. Sulla base di tale livello sono individuate le misure di sicurezza idonee. La valutazione del rischio consiste nella sistematica considerazione dei seguenti elementi:
  - Danno che può derivare dalla mancata applicazione di misure di sicurezza al sistema informativo, considerando le potenziali conseguenze derivanti dalla perdita di riservatezza, integrità, disponibilità, autenticità e non ripudio delle informazioni;
  - Realistica probabilità di come sia possibile perpetrare un attacco alla luce delle minacce individuate.

  I risultati della valutazione aiutano a determinare quali siano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee rispetto ai propri obiettivi, in base alla definizione del livello di rischio residuo che l'azienda decide di accettare, da implementare successivamente.
- **Principi ispiratori:** Rappresentano il sistema dei valori in cui l'azienda crede con riferimento alla gestione della sicurezza del proprio sistema informativo. Si tratta delle idee di fondo che l'azienda ha maturato nei riguardi della sicurezza delle informazioni, ovvero che cosa sia giusto fare, o meno, per disporre di un sistema di gestione della sicurezza efficiente, efficace e adeguato alle proprie necessità. Il riferimento primario dei principi generali di sicurezza è lo standard ISO/IEC 27001.
- **Leggi e contratti:** nell'ambito del contesto normativo esistente, vengono fornite indicazioni su come affrontare le problematiche della sicurezza e su come gestire l'utilizzo dei sistemi informativi. Il rispetto della legislazione italiana relativa alla sicurezza serve, oltre che per limitare i rischi di un coinvolgimento dell'azienda, anche per garantire un livello minimo di sicurezza del sistema informativo da proteggere.

La presente policy, nel rispetto delle principali norme e degli standard in materia:

- Sottolinea l'importanza di garantire la sicurezza delle informazioni e degli strumenti atti al trattamento delle stesse;
- È coerente con la volontà espressa dalla società di garantire la protezione del patrimonio informativo;
- Ha come oggetto aspetti fisici, logici ed organizzativi del Sistema di Gestione della Sicurezza delle Informazioni.

1.3. Termini e definizioni

- **Asset o Bene**: qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale che immateriale (es. beni fisici, software, informazioni e dati, ...).
- **Autenticità**: proprietà per la quale è garantito che l'identità di un soggetto o di una risorsa è quella dichiarata; l'autenticità si applica ad entità quali utenti, processi, sistemi ed informazioni.

- **Disponibilità**: proprietà per la quale le informazioni sono rese accessibili ed utilizzabili su richiesta di un'entità autorizzata.
- **Integrità**: proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata.
- **Non ripudio**: capacità di dimostrare che un'azione o un evento hanno avuto luogo, in modo che questo evento od azione non possano essere ripudiati successivamente.
- **Riservatezza**: proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Hardening**: insieme di azioni atte ad analizzare le funzionalità di un sistema operativo/applicazione al fine di individuare la configurazione ottima che permetta di innalzare il livello di sicurezza e ridurre il rischio residuo connesso alle debolezze dei sistemi.

1.4 Riferimenti normativi

1.4.1. Vigenti norme di legge

"Codice in materia di protezione dei dati personali"
REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

1.4.2. Norme standardizzazione comunitarie ed internazionali di riferimento

- UNI EN ISO 9001:2015 Sistemi di gestione per la qualità. Requisiti
- UNI CEI EN ISO/IEC 27001:2017 Tecnologie informatiche, tecniche di sicurezza, sistemi di gestione della sicurezza dell'informazione. Requisiti.
- UNI CEI ISO-IEC 27002 Tecniche per la sicurezza. Raccolta di prassi sui controlli per la sicurezza delle informazioni.

1.4.3. Documenti del SGSI

L'elenco generale dei documenti comprensivo della eventuale categoria di classifica è conservato nell'archivio qualità e sicurezza delle informazioni.

1.4.4. Documenti del Sistema di Gestione per la Qualità e Sicurezza delle informazioni

- Manuale Qualità Integrato
- Procedure
- Istruzioni
- Moduli
- SOA (*Statement of Applicability)*

2. Policy

2.1. Principi generali

I principi generali ai quali la Cyber 4.0 ispira la sua Politica di Gestione della Sicurezza delle Informazioni, nello specifico perimetro applicativo della norma sono articolati nelle seguenti tematiche:

- Identificazione, classificazione e gestione delle risorse
- Gestione sicura degli accessi logici
- Norme comportamentali per la gestione sicura delle risorse aziendali
- Personale e Sicurezza
- Gestione degli eventi anomali e degli incidenti
- Gestione della sicurezza fisica
- Aspetti contrattuali connessi alla sicurezza delle informazioni

- Gestione della Business Continuity
- Monitoraggio, tracciamento e verifiche tecniche
- Ciclo di vita dei sistemi e dei servizi
- Rispetto della normativa

2.1.1. Miglioramento continuo

Al fine di perseguire il miglioramento continuo, la Direzione si impegna ad individuare gli strumenti, le modalità, le tecniche e le risorse umane che siano ritenuti a tal fine necessari, e che abbiano, quindi, il fine ultimo di accrescere la qualità del lavoro congiuntamente al benessere di tutti coloro che lavorano nell'azienda e la soddisfazione dei Clienti.
Al fine di verificare l'effettivo miglioramento aziendale, la Direzione stabilisce degli obiettivi misurabili e quantificabili, meritatamente agli aspetti che, di volta in volta, ritiene cruciali per la propria società, e si impegna a controllarne l'andamento per poter, in sede di Riesame da parte della Direzione, proporre ed attuare idonee azioni di miglioramento.

2.1.2. Obiettivi generali del SGQ

L'esistenza di un SGSI ha come obiettivo primario il raggiungimento e mantenimento di un livello qualitativo in continuo miglioramento nell'ambito del ciclo di erogazione del servizio a favore dell'utenza finale.
In particolare, la Politica aziendale, intesa non soltanto come insieme di metodologie ma anche come comportamento manageriale, è diventata una leva strategica in tutte le attività orientate al cliente sia attraverso il migliore impiego delle risorse umane che finanziarie che tecnologiche.
È per questa ragione che l'associazione si propone:

- l'obiettivo di garantire la completa soddisfazione delle aspettative del cliente attraverso l'erogazione di servizi di qualità e sicurezza delle informazioni frutto degli standard definiti nel proprio Sistema di Gestione Integrato;
- di sviluppare e mantenere un SGSI conforme agli standard di riferimento quale strumento per realizzare gli obiettivi, rispettare gli impegni assunti, promuovere il miglioramento continuo dei processi aziendali, garantire il rispetto dei requisiti cogenti per i prodotti ed i servizi correlati;
- di adottare un sistema di gestione del rischio, al fine di garantire che per tutti i servizi forniti il rischio residuo sia ridotto al minimo;
- di impegnare tutte le energie e capacità a disposizione nell'ascoltare le indicazioni, suggerimenti, desideri del cliente;
- di focalizzare ogni attività sui bisogni del cliente per soddisfarlo meglio e più velocemente in modo da affermare una posizione di leader nel mercato;
- di consolidare il rapporto con i partner al fine di assicurare ai clienti prodotti di maggior valore, sicuri, affidabili, di alto livello tecnologico a prezzi ragionevoli;
- di fornire prodotti e servizi aderenti a tutti i requisiti imposti dalle disposizioni legislative vigenti in materia;
- di diffondere nell'organizzazione cultura e metodologie appropriate in modo che chiunque vi lavori sia costantemente in grado di erogare il miglior servizio atteso al cliente;
- di assicurare un alto livello di soddisfazione di tutti i dipendenti attraverso la ricerca della massima lealtà e senso di responsabilità;
- di incoraggiare il personale ed il management affinché possa realizzare le proprie attitudini, interessi e predisposizioni e sviluppi le proprie competenze tecniche ed organizzative.

La Direzione inoltre si impegna affinché:

- gli obiettivi così definiti vengano compresi, accettati ed attuati a tutti i livelli dell'organizzazione;
- gli obiettivi della politica integrata siano definiti e compatibili con il contesto e la direzione strategica della società;

- il sistema di gestione per la qualità e sicurezza delle informazioni raggiunga i risultati attesi;
- il personale sia coinvolto, diretto e sostenuto al fine di ottenere l'efficacia del sistema di gestione della qualità sicurezza delle informazioni;
- venga promosso il miglioramento.

2.1.3. Obiettivi operativi per l'anno di riferimento

L'Alta Direzione provvede poi su base annuale alla definizione e diffusione di un Piano contenente gli obiettivi per l'anno di riferimento che declinano in dettaglio gli obiettivi generali coinvolgendo i pertinenti livelli e le relative funzioni aziendali nell'ambito dell'Organizzazione con il fine di aumentare/migliorare il livello di soddisfazione del Cliente e delle ulteriori Parti interessate.
La mancanza di adeguati livelli di qualità del servizio, può comportare, nell'ambito di una qualsiasi attività aziendale, il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.
La Qualità sicurezza delle informazioni è, quindi, un requisito fondamentale per garantire l'affidabilità, l'efficacia e l'efficienza dei servizi erogati da Cyber 4.0. Di conseguenza, è essenziale per l'associazione identificare le esigenze qualitative sia nei rapporti inter-aziendali (dipendenti/collaboratori) che nei rapporti con l'esterno (utenti/fornitori).
I risultati della valutazione aiutano a determinare quali siano le azioni necessarie per gestire i rischi individuati, le procedure e le misure più idonee rispetto ai propri obiettivi.
La presente Politica, nel rispetto delle principali norme e degli standard in materia:

- sottolinea l'importanza di garantire la Qualità sicurezza delle informazioni del servizio e degli strumenti atti al raggiungimento e mantenimento della stessa;
- è coerente con la volontà espressa dall'associazione di garantire la soddisfazione dell'utente finale di detti servizi;
- ha come oggetto aspetti fisici, logici ed organizzativi del Sistema di Gestione Integrato.

2.1.4. Principi generali della Qualità sicurezza delle informazioni

I principi generali ai quali la Cyber 4.0 ispira la sua Politica integrata, sono i seguenti:

- assicurare che i requisiti dei Clienti (esigenze implicite ed esplicite) siano ben definiti e parte fondamentale delle soluzioni proposte;
- assicurare che le caratteristiche del servizio offerto siano improntate al principio di massima informativa e trasparenza;
- assicurare processi di delivery e maintenance chiari ed in costante miglioramento;
- erogare agli enti ed imprese servite un servizio in linea con le performance espresse;
- assicurare ad ogni livello aziendale una condotta rispettosa degli impegni presi;
- aggiornamento tecnico del personale e delle attrezzature;
- ricordare sempre che l'unica ragione dell'esistenza dell'Associazione Cyber 4.0, come Centro di Competenza ad alta specializzazione, è nella qualità delle relazioni e nella qualità dei servizi offerti agli enti ed imprese serviti.

In base a tali principi, nell'ambito del proprio SGSI, Cyber 4.0:
si impegna:

- verso gli enti e le imprese servite, a fornire prodotti e servizi rispondenti ai requisiti cogenti e di qualità sicurezza delle informazioni elevata, a dimostrare trasparenza ed affidabilità, ad assicurare la qualità del servizio a prezzi competitivi, attraverso l'analisi ed il contenimento dei costi;
- verso i fornitori, a favorire una proficua "alleanza" in modo da poter essere parte attiva nella definizione delle prestazioni e delle caratteristiche del prodotto, ed a fornire il supporto necessario

per la comprensione e definizione dei requisiti del Cliente e dei requisiti cogenti pertinenti il servizio erogato;
- verso i dipendenti a favorire lo spirito di iniziativa, incoraggiare la crescita professionale, assicurare rapporti professionali proficui e sereni, garantire un ambiente di lavoro sicuro nel quale tutti possano essere soddisfatti;
- a favorire la crescita dell'Associazione, assicurando adeguata redditività e stabilità finanziaria, elementi imprescindibili per l'affermazione della Politica per la qualità sicurezza delle informazioni.

si prefigge di:

- sviluppare tecniche di servizio pensate e realizzate per venire incontro alle esigenze del cliente, per anticiparne le aspettative, e fornire soluzioni che creino valore per il cliente;
- operare una selezione sistematica di nuovi prodotti/servizi di alto livello tecnologico;
- velocizzare la distribuzione di servizi mediante l'adozione degli strumenti tecnici più innovativi ed affidabili, rendendo più efficiente l'organizzazione, utilizzando tutte le potenzialità necessarie.

2.1.5. Struttura responsabile del mantenimento del sistema di gestione

La struttura responsabile del sistema di gestione deve farsi promotrice, al fine di rendere la politica generale coerente con l'evoluzione del contesto aziendale, delle eventuali azioni da intraprendere a fronte del verificarsi di eventi quali:

- nuove minacce o modifiche a quelle considerate nelle precedenti attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo e legislativo;
- risultati di analisi sui costi, impatti, efficacia ed efficienza del sistema di gestione.

Di seguito, si riporta, per ciascuna tematica, l'obiettivo e le linee guida definite dalla Cyber 4.0.

2.2. Identificazione, classificazione e gestione delle risorse

Obiettivo: *garantire la piena conoscenza delle informazioni gestite dalla Cyber 4.0 e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.*

- Deve esistere ed essere mantenuto aggiornato, nel corso del tempo, un sistema di censimento di tutti i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione);
- Ogni risorsa (bene materiale/immateriale) deve essere direttamente associabile ad una Funzione aziendale responsabile.
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati. La criticità delle informazioni deve essere valutata in maniera quanto più oggettiva possibile, attraverso l'utilizzo di adeguate metodologie di lavoro.
- Le modalità di gestione ed i sistemi di protezione per le informazioni e gli asset su cui risiedono devono essere coerenti con il livello di criticità identificato.

2.2.1. Documentazione di Sistema

- Politica della sicurezza delle informazioni
- Elenco e piano di continuità operativa
- Classificazione Informazioni

2.3. Gestione sicura degli accessi logici

Obiettivo: *garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti.*

- L'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti. La comunicazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio.
- L'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinato al superamento di una procedura di identificazione ed autenticazione degli stessi.
- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione.
- È necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso.
- I sistemi che costituiscono l'infrastruttura devono essere opportunamente protetti e segregati, in modo da minimizzare la possibilità degli accessi non autorizzati.

2.4. Norme comportamentali per la gestione sicura delle risorse aziendali

Obiettivo: *garantire che i dipendenti e collaboratori della Cyber 4.0 adottino modelli di comportamento volti a garantire adeguati livelli di sicurezza delle informazioni.*

- Gli ambienti di lavoro e le risorse aziendali devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate.
- Devono essere definite delle procedure per la gestione ed utilizzo delle informazioni sia su supporto digitale che su supporto cartaceo.
- I sistemi informatici aziendali devono essere impiegati da dipendenti e da collaboratori secondo procedure approvate.

2.4.1. Normativa nazionale

Codice in materia di tutela dei dati personali
REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

2.5. Personale e sicurezza

Obiettivo: *garantire che il personale che opera per conto della Cyber 4.0 (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.*

- Nelle fasi di selezione ed inserimento del personale nella Cyber 4.0 devono essere valutati i livelli di conoscenza degli obiettivi e delle problematiche di sicurezza aziendale in funzione delle attività che dovranno essere svolte.
- Durante la permanenza nella Cyber 4.0 il personale deve ricevere un'adeguata e continuativa formazione inerente alle tematiche di sicurezza dei dati.
- Le modalità di chiusura del rapporto di lavoro con la Cyber 4.0 deve essere coerente con gli obiettivi di sicurezza aziendale.

Tutti i dipendenti della Cyber 4.0, inoltre, sentono che il raggiungimento degli obiettivi di Qualità sicurezza delle informazioni dipende fortemente dal loro coinvolgimento e dal modo in cui essi svolgono le proprie attività. La piena partecipazione richiede che ciascuno venga opportunamente addestrato, messo in condizioni di assumersi le proprie responsabilità ed acquisisca piena familiarità con la documentazione per la qualità sicurezza delle informazioni e le procedure operative stabilite in sede aziendale.
L'attivazione del processo di miglioramento continuo non può prescindere dal coinvolgimento di tutto il personale.

Tutte le persone che lavorano e/o collaborano con Cyber 4.0 sono impegnate a rispettare i seguenti principi:
1. **Riservatezza**: per assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non

autorizzate;
2. **Integrità**: per salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità**: per assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta e salvaguardia quindi il patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati, riducendo i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.);
4. **Controllo**: per assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Privacy**: per garantire la protezione ed il controllo dei dati personali.

2.6. Gestione degli eventi anomali e degli incidenti

Obiettivo: *garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.*

- Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza e secondo adeguate procedure, eventuali problematiche legate alla sicurezza delle informazioni.
- Gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e no, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure.
- Deve esistere un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerentemente con le reali problematiche riscontrate.

2.7. Gestione della sicurezza fisica

Obiettivo: *prevenire l'accesso non autorizzato alle sedi ed ai singoli locali dell'associazione e garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestite le informazioni.*

- Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite:
  - L'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni elaborate;
  - La definizione dei livelli adeguati di protezione;
  - La predisposizione di un ciclo periodico di verifiche e controlli.
- Deve essere garantita la sicurezza delle apparecchiature tramite:
  - La definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni;
  - La messa a disposizione delle risorse necessarie al loro funzionamento;
  - La predisposizione di un adeguato livello di manutenzione;
  - La predisposizione di un ciclo periodico di verifiche e controlli.

2.8. Aspetti contrattuali connessi alla sicurezza delle informazioni

Obiettivo: *assicurare la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti, in accordo con le caratteristiche specifiche della relazione che la Cyber 4.0 deve instaurare con le terze parti stesse.*

- Gli accordi con le terze parti e con gli outsourcer che accedono alle informazioni e/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza.

- Gli accordi con terze parti e con gli outsourcer, ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali ("normativa privacy").

2.8.1. Normativa nazionale

Codice in materia di tutela dei dati personali
REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

2.9. Gestione della Business Continuity

Obiettivo: *garantire la continuità dell'attività svolta dalla Cyber 4.0 e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze sia all'interno che all'esterno del contesto aziendale.*

- Devono essere attentamente identificati e valutati, in termini di probabilità di accadimento e possibili conseguenze, tutti gli eventi da cui può dipendere un'interruzione della continuità del business.
- Deve essere predisposto un piano di continuità che permetta all'organizzazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative sulla missione aziendale.
- Devono essere preparate, validate e opportunamente divulgate tutte le procedure operative ed organizzative necessarie per assicurare l'implementazione del piano di continuità.
- Devono essere periodicamente effettuati i test per tutti i componenti del piano di continuità.
- Deve essere assicurato il mantenimento e l'aggiornamento dei piani e delle procedure di cui ai punti precedenti al fine di garantire l'efficacia del sistema nel tempo a fronte di eventuali cambiamenti organizzativi/tecnologici.

2.10. Monitoraggio, tracciamento e verifiche tecniche

Obiettivo: *garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.*

- I sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, hardware e software, implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato.
- A fronte dei risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative.
- Devono essere pianificate attività periodiche di audit del sistema di gestione della sicurezza delle informazioni.

2.11. Ciclo di vita dei sistemi e dei servizi

Obiettivo: *assicurare che gli aspetti di sicurezza siano inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.*

- Nella fase di progettazione e sviluppo devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere eseguite le seguenti azioni:
  - Inclusione dei requisiti di sicurezza nelle specifiche funzionali dei servizi e sistemi;
  - Adozione di best practice per la manutenzione del software;
  - Gestione controllata della documentazione.
- Nella fase di esercizio devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere eseguite le seguenti azioni:
  - Adozione di procedure di backup e restore;
  - Adozione di procedure di dismissione controllata dei sistemi;

  - Network security: segregazione delle reti, monitoraggio dei gateway (firewall).
- Nella gestione dei servizi devono essere opportunamente considerati gli aspetti di sicurezza. In particolare, devono essere eseguite le seguenti azioni:
  - Monitoraggio dei sistemi e servizi;
  - Gestione utenze;
  - Performance monitoring.

2.12. Rispetto della Normativa

Obiettivo: *garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni di reputazione.*

- Tutti i requisiti normativi e contrattuali in materia di sicurezza del sistema informativo e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'associazione e sui sistemi informativi.
- I responsabili delle diverse aree devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta la documentazione relativa alla sicurezza delle informazioni siano applicati e rispettati.
- Il mancato rispetto di quanto indicato in questo documento, e in tutti gli altri che da esso discendono, sarà gestito in ottemperanza a quanto previsto nel CCNL oppure, nel caso di inadempienze di terze parti, secondo i rapporti contrattuali in essere.

2.12.1. Documentazione di Sistema

- Condizioni Generali di contratto
- Condizioni Particolari di contratto Hosting, Domini, Mail

3. Definizione dei ruoli e delle responsabilità

3.1. Struttura responsabile gestione sicurezza delle informazioni

La struttura responsabile del sistema di gestione della sicurezza delle informazioni dovrà farsi promotrice, al fine di rendere la politica generale di sicurezza coerente con l'evoluzione del contesto aziendale, delle eventuali azioni da intraprendere a fronte del verificarsi di eventi quali:

- Nuove minacce o modifiche a quelle considerate nelle precedenti attività di analisi del rischio;
- Significativi incidenti di sicurezza;
- Evoluzione del contesto normativo e legislativo in materia di sicurezza delle informazioni;
- Risultati di analisi sui costi, impatti, efficacia ed efficienza del sistema di gestione perla sicurezza delle informazioni.

3.2. Management e Funzione SEC

Il Management (Direzione) è la funzione aziendale apicale a cui competono, con il supporto della struttura responsabile del sistema di gestione della sicurezza delle informazioni (RGSI), le decisioni di massimo livello riguardo alle tematiche di sicurezza.
In particolare, ha la responsabilità di supportare e garantire, mediante le funzioni aziendali subordinate, l'applicazione delle politiche generali del Sistema di Gestione della Sicurezza delle Informazioni, di definire le politiche idonee di gestione del rischio e di supportare costantemente il processo di sensibilizzazione sulle tematiche di sicurezza.

Il presente documento è revisionato annualmente in occasione della riunione per la redazione del Riesame della Direzione.

La Direzione si impegna inoltre a:

- **divulgare** e promuovere la politica per la qualità sicurezza delle informazioni
- **attuare** la politica per la qualità sicurezza delle informazioni attraverso la definizione di obiettivi di miglioramento
- **riesaminare** la politica per la qualità sicurezza delle informazioni in funzione dei risultati raggiunti e delle strategie aziendali