Documento	Codice
Manuale del Sistema di Gestione	**MSG**

*Il sottoscritto assicura che il presente documento è copia conforme dell'originale disponibile nella bacheca elettronica di **MADE IN BIT** alla data di consegna. L'eventuale revisione aggiornata è disponibile nell'area riservata.*

Distribuito a scopo informativo e non soggetto ad aggiornamento:

Data consegna: | *Destinatario:* | *Distribuito in copia controllata:*

Rev.	Data	Descrizione modifiche	Redatto	Verificato	Approvato
01.a	*05/01/26*	*Prima emissione*	*Lilli (RSG)*	*Lilli (RSG)*	*Lilli (RSG)*

1 Sommario

È possibile interrogare il presente manuale utilizzando NotebookLM di Google inquadrando il seguente QR-Code

O richiamando il seguente link:

https://notebooklm.google.com/notebook/9aea1aa1-91c6-42d2-99f3-81e5e0bdfd6c

Si ricorda che i modelli cosiddetti di Intelligenza Artificiale possono commettere errori si consiglia quindi di controllare sempre il riferimento al testo del documento che ha originato la risposta (indicato da un numero su sfondo grigio).

1 SCOPO E CAMPO DI APPLICAZIONE

1.1 Struttura e scopo del presente manuale

Il presente Manuale descrive il Sistema di Gestione di MADE IN BIT organizzato ed attivato in conformità ai requisiti della normativa UNI EN ISO 9001:2015 (d'ora in poi ISO 9001) e UNI CEI EN ISO/IEC 27001:2024 (d'ora in poi ISO 27001) recependo la raccomandazione ISO/IEC 27017 che fornisce linee guida per i controlli di sicurezza delle informazioni applicabili alla fornitura e all'uso dei servizi cloud.

Questo Manuale ha lo scopo di descrivere la politica stabilita dalla Direzione Aziendale, di definire i criteri gestionali adottati e di fornire il riferimento per l'attuazione e la comprensione del Sistema di Gestione, nonché costituire un costante riferimento nell'applicazione e nell'aggiornamento del Sistema di Gestione stesso.

Il Manuale rappresenta il documento di riferimento che rende esplicita la volontà della Direzione Aziendale di perseguire i seguenti obiettivi in termini prioritari:

- dimostrare la capacità di erogare servizi conformi ai requisiti cogenti ed alle esigenze, espresse ed implicite, del cliente;
- garantire la sicurezza delle informazioni;
- misurare la percezione del cliente di tali capacità in modo da accrescerne la soddisfazione;
- rispondere ai cambiamenti del contesto nel quale opera ed ai rischi ad esso connessi ed alle mutevoli esigenze;
- migliorare l'organizzazione aziendale e le prestazioni di MADE IN BIT con riferimento alla politica aziendale ed alle norme ISO 9001, ISO 27001 e ISO 27017[1], per la quale mantenere la certificazione di ente terza parte;
- dimostrare alle parti interessate che esiste un Sistema di Gestione in grado di garantire il miglioramento continuo delle prestazioni e fornire risultati in linea con le attese dei differenti portatori di interesse.

Il Manuale di Gestione, dove necessario, è integrato e richiama una serie di Procedure e Istruzioni che definiscono con maggior dettaglio le modalità operative di chi partecipa alle attività all'interno del Sistema di Gestione.

1.2 Campo di applicazione

Le prescrizioni del presente Manuale, delle Procedure e delle Istruzioni in esso richiamate sono applicabili a tutte le attività e a tutte le funzioni aziendali di MADE IN BIT e disciplinano i processi necessari alla progettazione, erogazione e supporto dei servizi aziendali.

Il Sistema di Gestione si applica ai seguenti ambiti operativi:

- studio, analisi e acquisizione delle commesse;
- progettazione e sviluppo di soluzioni software;
- installazione, configurazione e gestione di sistemi hardware e infrastrutture IT;
- erogazione di servizi di assistenza tecnica e manutenzione;
- progettazione ed erogazione di attività formative;
- approvvigionamento di beni e servizi;
- gestione amministrativa e di supporto ai processi aziendali;
- gestione delle risorse umane e delle competenze;
- gestione delle infrastrutture tecnologiche e degli strumenti di lavoro.

Il presente Manuale, unitamente alle Procedure e Istruzioni richiamate, definisce lo standard organizzativo e operativo adottato da MADE IN BIT per garantire la conformità dei servizi erogati ai requisiti applicabili delle norme ISO richiamate, nonché ai requisiti cogenti e contrattuali applicabili.

Tutto il personale aziendale è tenuto ad osservare le prescrizioni del presente Manuale, delle Procedure e delle Istruzioni applicabili alla propria funzione; ne conosce i contenuti e ne condivide gli obiettivi definiti dalla Direzione Aziendale.

1.3 Presentazione dell'organizzazione

MADE IN BIT srl si propone alle aziende come fornitore globale di soluzioni software e tecnologia informatica. Grazie alla sinergia con i propri clienti, MADE IN BIT ha acquisito un patrimonio di conoscenze necessario ad affrontare, con piena padronanza, le più complesse problematiche relative alla gestione d'azienda.

Una politica aziendale dinamica e tesa a mantenere sempre i più alti livelli di conoscenza nel settore, consente a MADE IN BIT di proporsi come partner unico sia in campo software che hardware.

MADE IN BIT si propone a ciascun cliente come interlocutore attento e capace di supportarlo nell'analisi e nella progettazione di soluzioni basate sul web, nell'assistenza, nella consulenza hardware e, infine, nella formazione del personale.

La collaborazione con i clienti è preziosa perché orientata ad individuare nei minimi dettagli le loro esigenze, ottimizzando tempi e risultati delle soluzioni.

MADE IN BIT ha scelto di utilizzare per la gestione del proprio Sistema di Gestione **SQuadra** che è un'applicazione software per la gestione dei Sistemi Aziendali scelta da importanti associazioni imprenditoriali nazionali per i propri associati. SQuadra è gestito da una società terza, certificata ISO 27001, ed opera con servizi cloud differenti da quelli utilizzati da MADE IN BIT garantendo continuità nell'operatività anche in situazioni anomale per MADE IN BIT.

2 RIFERIMENTI NORMATIVI

Il presente Manuale di Gestione è stato elaborato in conformità alle norme UNI EN ISO 9001:2015 (d'ora in poi ISO 9001), UNI CEI EN ISO/IEC 27001:2024 (d'ora in poi ISO 27001) e UNI EN ISO/IEC 27017:2021 (d'ora in poi si ritiene compreso nel riferimento alla ISO 27001).

[1] Vengono utilizzate anche le indicazioni presenti nella norma ISO 27002:2022 ("Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli sulla sicurezza delle informazioni") e, con particolare attenzione al trattamento dei dati personali, nella norma ISO 27701:2021 ("Tecniche di sicurezza - Estensione a ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni sulla privacy - Requisiti e linee guida").

3 TERMINI E DEFINIZIONI

3.1 Definizioni

Di seguito si riportano le definizioni dei termini utilizzati all'interno del presente Manuale:

Termine	Definizione
Audit	Processo sistematico, indipendente e documentato per ottenere evidenze di audit e valutarle in maniera oggettiva, al fine di stabilire in quale misura i criteri di audit siano stati rispettati.
Azioni Correttive	Azione tesa ad eliminare la causa di una Non Conformità.
Cliente o Committente	Organizzazione destinataria dei prodotti o servizi offerti da MADE IN BIT.
Fornitore	Organizzazione o persona che fornisce un prodotto o servizio.
Miglioramento Continuo	Processo di accrescimento del Sistema di Gestione per accrescere la capacità di soddisfare i requisiti e ottenere miglioramenti delle prestazioni in accordo con la politica dell'organizzazione.
Non Conformità	Mancato soddisfacimento di un requisito.
Obiettivo	Fine a cui si aspira in termini di prestazioni che un'organizzazione intende conseguire.
Organizzazione	Società, esercizio, azienda, impresa, istituzione, associazione, ovvero loro parti, con o senza personalità giuridica, pubblica o privata, che abbia una propria struttura funzionale e amministrativa.
Parte Interessata	Persona o gruppo che ha un interesse, è coinvolto o influenzato nell'attività dell'organizzazione o di un sistema o nelle sue prestazioni.
Politica	Dichiarazione, da parte di un'organizzazione, delle sue intenzioni e dei suoi principi in relazione alla sua prestazione, che fornisce uno schema di riferimento per l'attività e per la definizione dei suoi obiettivi e indirizzi generali.
Prestazione	Risultati misurabili del Sistema di Gestione, conseguenti al controllo esercitato dall'organizzazione sui propri aspetti e rischi, sulla base della sua politica e dei suoi obiettivi.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in entrata in elementi in uscita. Procedimento attraverso il quale si utilizzano elementi in ingresso (risorse umane, materiali, energetiche, ecc.) per la realizzazione di un prodotto finito o di parte di esso.
Registrazione	Documento che riporta i risultati ottenuti o fornisce evidenza delle attività svolte.
Riesame	Attività effettuata per riscontrare l'idoneità, l'adeguatezza e l'efficacia di qualcosa da conseguire a intervalli stabiliti.
Sistema di Gestione	Sistema che comprende la struttura organizzativa, le attività di pianificazione, le responsabilità, le prassi, le procedure, i processi, le risorse per elaborare, mettere in atto, conseguire, riesaminare e mantenere attiva la politica e gli obiettivi.
Utente	Persona che utilizzerà i prodotti e/o servizi offerti da MADE IN BIT.

3.2 Abbreviazioni ed Acronimi

Nel Manuale del Sistema di Gestione ricorrono le seguenti abbreviazioni:

Acronimo	Descrizione
AC	Azione Correttiva
CQ	Controllo Qualità
IO	Istruzione Operativa
MD	Modello o modulo
MG	Manuale di Gestione
NC	Non Conformità
PdI	Proprietario delle Informazioni
PdP	Piano della Progettazione
PdQ	Piano qualità di Commessa
PG	Procedura Gestionale
RA	Rapporto Audit
RAP	Responsabile delle Attività di Progettazione
REC	Responsabile della Erogazione della Commessa
RP	Responsabile della Pianificazione
RSG	Responsabile del Sistema di Gestione
RSI	Responsabile del Sistema Informatico
SIA	Sistema Informativo Aziendale
SG	Sistema di Gestione
VI	Audit (Verifica Ispettiva)

4 SISTEMA DI GESTIONE

4.1 Comprendere l'organizzazione ed il suo contesto

La Direzione Aziendale ha determinato i fattori esterni ed interni rilevanti per le proprie finalità e per i propri indirizzi strategici e che influenzano le sue capacità di raggiungere i risultati attesi per il proprio Sistema di Gestione e li ha riportati nell'Analisi del Contesto effettuata su SQuadra.

L'analisi del Contesto viene effettuata con le modalità stabilite nel Manuale di SQuadra e si basa anche sui concetti presenti nei seguenti modelli teorici di riferimento:

- Business Model Canvas (per individuare il modello di business di MADE IN BIT, eventualmente suddiviso per ogni linea di business);
- Analisi SWOT che consente di individuare i fattori interni (punti di forza e punti di debolezza) ed i fattori esterni (opportunità e minacce) più significativi per MADE IN BIT.

La Direzione Aziendale valuta l'adeguatezza e l'eventuale necessità di aggiornamento dei fattori esterni ed interni rilevanti almeno una volta all'anno e fornisce tale indicazione nel Riesame della Direzione. Se necessario, la Direzione Aziendale provvede ad aggiornare l'analisi del contesto.

4.2 Comprendere le esigenze e le aspettative delle parti interessate

La Direzione Aziendale ha determinato le parti interessate rilevanti per il Sistema di Gestione ed i requisiti di tali parti interessate che sono rilevanti e significativi.

La Direzione Aziendale ha determinato le esigenze e le aspettative delle parti interessate che hanno influenza sulla capacità di MADE IN BIT di fornire con regolarità prodotti e servizi che soddisfano i requisiti del cliente e quelli cogenti applicabili e la sicurezza delle informazioni ed ha registrato tali indicazioni nell'analisi del contesto presente su SQuadra.

La Direzione Aziendale valuta l'eventuale esigenza di modifiche o integrazioni di tali informazioni e, in caso di necessità, provvede ad aggiornare le esigenze e le aspettative delle parti interessate nell'analisi del contesto su SQuadra.

4.3 Ambito di applicazione

L'ambito di applicazione della certificazione rispetto alla norma ISO 9001 e ISO 27001 (con la ISO 27017) è: "Servizi professionali di configurazione, monitoraggio, supporto continuativo sistemistico e soluzioni hardware, soluzioni software di integrazione su gestionali Passepartout, configurazione di servizi Cloud offerti dai più importanti player internazionali".

MADE IN BIT ha stabilito, documentato, attuato, tiene aggiornato e migliora con continuità un Sistema di Gestione rispondente ai requisiti delle norme ISO 9001 e ISO 27001 prese come riferimento per lo schema di certificazione.

Il Sistema di Gestione è stato progettato e realizzato interessando tutti i processi nonché il personale coinvolto nelle attività aziendali, compresi i fornitori che operano per conto di MADE IN BIT tali da poter influire sulla qualità del servizio erogato, per garantire la conformità ai requisiti specificati.

La Direzione Aziendale si pone come obiettivo quello di mettere a punto un'organizzazione orientata alla crescita del valore di MADE IN BIT nell'ottica prioritaria della tutela degli interessi dei soggetti coinvolti (parti interessate).

A tal fine ha impostato il proprio Sistema di Gestione in modo da definire i propri processi e le loro interazioni, i criteri e metodi necessari per assicurarne l'efficacia e il miglioramento mediante un effettivo monitoraggio delle prestazioni, le risorse e le informazioni necessarie.

Il Sistema di Gestione è dunque rivolto ad assicurare la soddisfazione dei portatori d'interesse di MADE IN BIT, in particolare:

- dei clienti, mediante la realizzazione di servizi adeguati alle richieste contrattuali, la proposizione di alternative migliorative sia sul piano realizzativo che dei costi di esecuzione;
- dei Soci, cercando di fare in modo che il capitale investito in MADE IN BIT dia adeguate risposte economiche ma soprattutto che l'immagine della stessa rifletta la loro volontà di "ben figurare" nei confronti di tutti;
- dei Fornitori e Consulenti, stabilendo, nel naturale rispetto del reciproco interesse economico, contatti di lavoro duraturi nel tempo, privilegiando l'affidabilità, la professionalità e la correttezza commerciale e favorendo scambi di conoscenze;
- di tutti coloro che operano in MADE IN BIT, garantendo condizioni di lavoro adeguate nel pieno rispetto delle disposizioni normative in materia di sicurezza, ed individuando le esigenze e le aspettative in termini di riconoscimenti, soddisfazione professionale e sviluppo individuale per assicurare un forte coinvolgimento e motivazione del personale.

Per mettere in atto il proprio Sistema di Gestione MADE IN BIT ha:

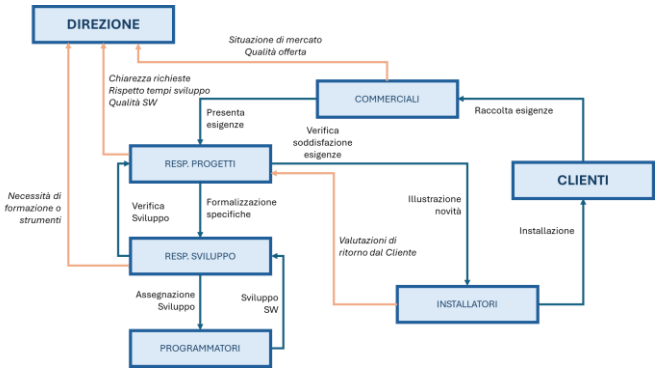
- identificato e definito i processi aziendali necessari per ottenere la conformità ai requisiti stabiliti e richiesti;
- stabilito la sequenza e le interazioni tra questi processi attraverso l'elaborazione del diagramma di flusso riportato di seguito;
- definito una propria *Politica*;
- stabilito criteri e metodi per garantire un'efficace operatività ed un adeguato controllo dei processi riportati nel presente Manuale;
- definite responsabilità e risorse necessarie per la gestione del SGI;
- individuato le risorse coinvolte nell'attuazione, il monitoraggio dei processi, provvedendo ad una adeguata formazione delle risorse umane, e la gestione dei mezzi ed apparecchiature;
- definiti appositi indicatori per la misurazione e controllo dei processi, del SGI e del suo miglioramento;
- stabilite, pianificate ed attuate azioni per il miglioramento continuo del sistema e dell'attività in genere;
- nominato un Responsabile del Sistema di Gestione (RSG) per facilitare la trasmissione delle informazioni necessarie, per il continuo monitoraggio ed analisi dei processi e per la verifica dell'attuazione delle azioni necessarie per conseguire i risultati previsti ed il miglioramento continuo del Sistema di Gestione.

4.3.1 Interazione tra i processi del Sistema di Gestione

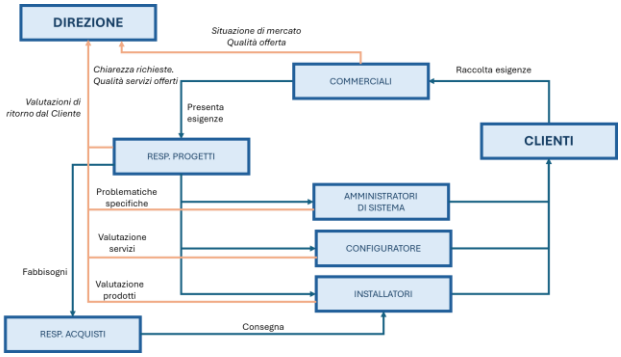
I diagrammi di flusso riportati di seguito illustrano le principali interazioni tra i processi che descrivono le attività svolte da MADE IN BIT.

Per ogni fase sono stati individuati gli elementi in ingresso e quelli in uscita, stabilendo le relazioni che legano tra loro le varie fasi.

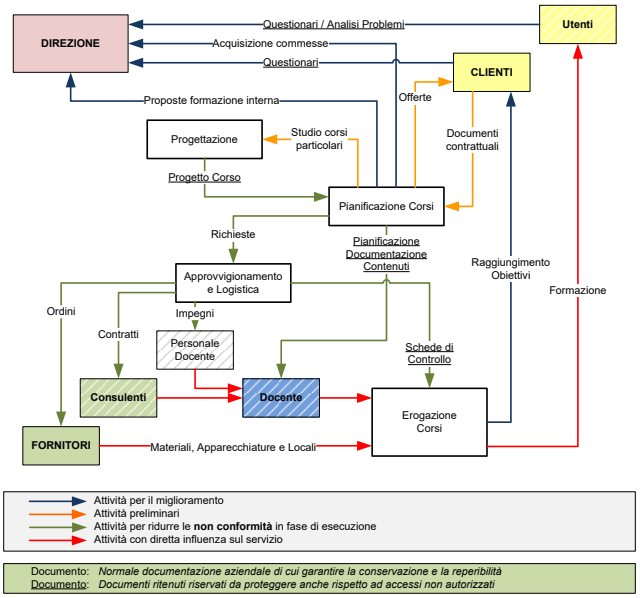
Sviluppo software



Attività sistemistiche



Attività di formazione.

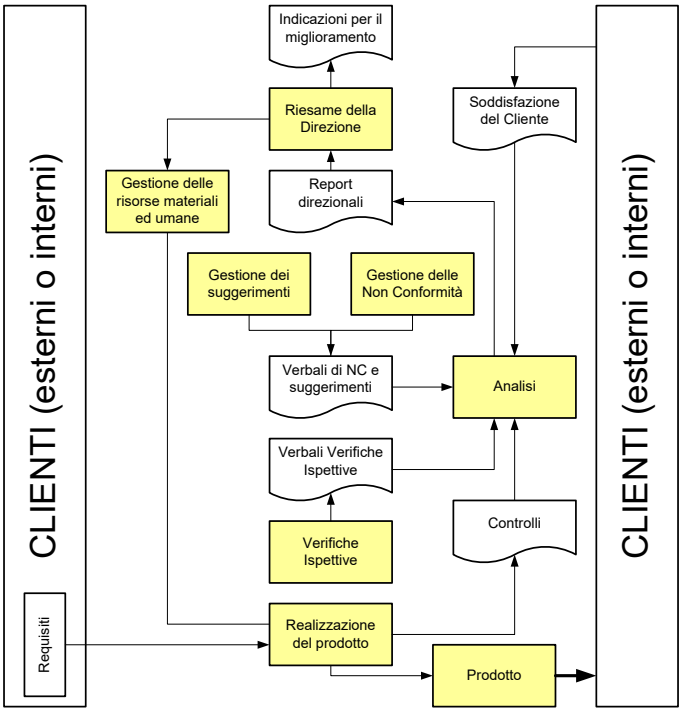


Alcuni dei processi possono essere affidati all'esterno. In questo caso essi vengono comunque tenuti sotto controllo e rimane comunque in carico a MADE IN BIT la responsabilità per la conformità a tutti i requisiti, sia del cliente sia cogenti.

Il tipo e l'estensione dei controlli da applicare al processo affidato all'esterno dipendono dall'impatto potenziale che questo ha sulla capacità di MADE IN BIT di fornire un servizio conforme ai requisiti con particolare riferimento agli aspetti cogenti.

Nel diagramma successivo viene riportato lo schema di gestione applicato ad ogni processo aziendale. Per ogni prodotto realizzato dal processo (ad esempio: progettazione di nuovi corsi da parte dell'ufficio progettazione) sono individuate le parti interessate, che ovviamente possono essere sia esterne che interne (nell'esempio: l'ufficio pianificazione), che hanno collaborato alla definizione dei requisiti e contribuiscono al loro continuo riesame (nell'esempio: adeguatezza, tempestività, ecc.) ed i controlli ai quali deve essere sottoposto il processo.

Ovviamente ogni processo è sottoposto ad Audit interno che, insieme ad una corretta gestione dei Reclami e delle Non Conformità ed indagini sulla soddisfazione del cliente (interno o esterno), permettono di tenerlo sotto controllo e di fornire elementi di valutazione per la Direzione Aziendale anche in relazione all'eventualità di interventi sull'assegnazione di risorse sia materiali che in termine di personale.



L'elenco completo di tutti i processi con l'individuazione dei portatori di interesse, del prodotto, dei requisiti, dei controlli e degli Obiettivi è descritto nella IO9.3A "Preparazione del Riesame della Direzione" ed analizzato ad ogni Riesame della Direzione per la conferma o modifica degli obiettivi per il successivo riesame.

4.4 Dati aziendali

4.4.1 Classificazione dei dati aziendali

Ogni informazione aziendale, compresi i dati personali trattati, può, in base al suo contenuto, essere classificata.

Nella Policy aziendale, nel capitolo "Classificazione delle informazioni", viene illustrata a tutti gli utenti la classificazione utilizzata in MADE IN BIT.

4.4.2 Rischi connessi al trattamento dei dati

Relativamente alla RISERVATEZZA (proprietà di un'informazione di non essere disponibile a individui, entità e processi non autorizzati) possiamo considerare i seguenti rischi:

- BASSO: I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici.
- MEDIO: I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business aziendale o sul rispetto della normativa vigente.
- ALTO: I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine). Un'eventuale loro diffusione ha elevati impatti sul business aziendale ma non sul rispetto della normativa vigente.

- CRITICO: La diffusione delle informazioni può mettere a repentaglio la sostenibilità dell'organizzazione o ha impatti elevati relativi al rispetto della normativa vigente.

Relativamente alla INTEGRITÀ (proprietà di un'informazione, di essere protetto per quanto riguarda l'accuratezza e la completezza) possiamo considerare i seguenti rischi:

- BASSO: I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie.
- MEDIO: I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'azienda. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.
- ALTO: I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'azienda. La mancanza di integrità dei dati ha elevati impatti sulle attività operative, ma non sul rispetto della normativa vigente.
- CRITICO: La mancanza di integrità delle informazioni ha elevati impatti sulle attività o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. I dati sono utilizzati per transazioni economiche, finanziarie o sanitarie.

Relativamente alla DISPONIBILITÀ (proprietà di essere accessibile e utilizzabile, entro i tempi previsti, su richiesta di un'entità autorizzata) possiamo considerare i seguenti rischi:

- BASSO: L'indisponibilità dei dati oltre i tempi stabiliti non comporta perdite rilevanti. I dati sono ricostruibili a un costo molto basso e includono gli elementi già duplicati che hanno bassi requisiti di sicurezza.
- MEDIO: L'indisponibilità dei dati oltre i tempi stabiliti comporta perdite non particolarmente rilevanti. Sono dati utilizzati nelle operazioni quotidiane per i quali esistono tuttavia delle fonti alternative o sono ricostruibili con una certa facilità.
- ALTO: L'indisponibilità dei dati oltre i tempi stabiliti comporta perdite rilevanti. Sono dati senza i quali MADE IN BIT è in grado di operare per brevi periodi di tempo. In questa categoria rientrano i dati utilizzati nei processi aziendali standard o che rappresentano un investimento significativo e sono difficili da ricostruire.
- CRITICO: L'indisponibilità dei dati oltre i tempi stabiliti comporta perdite che mettono in pericolo la sostenibilità economica e di immagine. Sono dati cruciali per l'operatività aziendale, utilizzati nei processi strategici chiave oppure obbligatori per legge.

4.4.3 Valore delle informazioni

Per definire il valore delle varie informazioni trattate si è tenuto conto dei seguenti fattori:

- Perdita di vantaggio competitivo, se un concorrente potesse disporre delle informazioni che hanno perso riservatezza.
- Perdita di ricavi a causa dell'indisponibilità delle informazioni o della loro inesattezza.
- Perdita di immagine a seguito di divulgazione di informazioni riservate, uso o alterazione delle informazioni per commettere frodi, pubblicazione di informazioni non accurate, indisponibilità delle informazioni e dei servizi informatici con impatto sui servizi offerti ai clienti.
- Impatti sugli Stakeholder (personale, clienti, fornitori, ecc.) conseguenti a perdita di fiducia in MADE IN BIT per incidenti relativi alla sicurezza delle informazioni.
- Errori decisionali in caso di dati non integri (incompleti o inesatti).
- Sanzioni determinate dai contratti o dalla normativa vigente (per esempio: la perdita di disponibilità che può causare l'interruzione dell'attività verso clienti, la perdita di riservatezza rispetto alla normativa privacy).
- Costi per ripristinare l'integrità o la disponibilità delle informazioni.

5 RESPONSABILITÀ DELLA DIREZIONE

5.1 Impegno della Direzione

La Direzione Aziendale di MADE IN BIT desidera mantenere e migliorare la propria collocazione nel mercato anche attraverso la qualità percepita dai clienti e dagli utenti relativamente ai propri prodotti e servizi. Ritiene per questo fondamentale la messa in atto del Sistema di Gestione ed il miglioramento continuo della sua efficacia. Consapevole che il proprio sistema informativo è un patrimonio aziendale, ha predisposto ed approvato la propria Politica anche in merito alla Sicurezza delle Informazioni.

Tale desiderio viene manifestato da MADE IN BIT mediante lo svolgimento delle seguenti attività:

- stabilendo e rendendo pubblica (attraverso la pubblicazione nel sito internet) la propria Politica e definendo gli obiettivi che intende raggiungere;
- definendo ruoli e responsabilità per il Sistema di Gestione ed assicurando la disponibilità delle risorse necessarie;
- effettuando periodicamente dei Riesami della Direzione allo scopo di individuare i possibili miglioramenti e definire nuovi obiettivi da raggiungere e/o modificare i parametri di misurazione di quelli già esistenti;
- comunicando e diffondendo a tutti coloro che operano per MADE IN BIT l'importanza di ottemperare ai requisiti del Sistema di Gestione.

Il raggiungimento degli obiettivi espressi nella politica aziendale è un importante compito di tutte le funzioni aziendali.

Per garantire la diffusione a tutti i livelli della politica aziendale la Direzione Aziendale, attraverso il RSG, si attiva affinché siano create occasioni di crescita professionale ed attività informative e formative al fine di rendere consapevole ogni lavoratore dell'importanza del suo comportamento.

Attenzione focalizzata ai portatori di interesse

La Direzione Aziendale di MADE IN BIT è consapevole che il successo dell'organizzazione dipende dal saper comprendere e soddisfare le esigenze e le aspettative, presenti e future, dei clienti attuali e potenziali, dei portatori di interesse in generale e degli utenti finali e dal saper prendere in considerazione quelle delle altre parti interessate.

A tal fine le esigenze e le aspettative dei potenziali clienti vengono individuate e convertite in requisiti già al momento dello studio per l'acquisizione delle commesse e quindi ottemperate in fase di realizzazione allo scopo di soddisfare i propri portatori di interesse. Nell'individuazione delle esigenze e

aspettative dei portatori di interesse vengono sempre presi in esame anche gli obblighi, inclusi quelli relativi ai requisiti legali.

5.2 Politica Aziendale

MADE IN BIT si impegna a fornire soluzioni software, servizi IT e formazione di qualità, garantendo la sicurezza delle informazioni trattate. La Direzione persegue questo impegno attraverso:

- il rispetto dei requisiti contrattuali, normativi e cogenti applicabili;
- la gestione sistematica dei rischi relativi alla qualità e alla sicurezza delle informazioni;
- il miglioramento continuo dei processi, delle competenze e delle infrastrutture;
- la protezione della riservatezza, integrità e disponibilità delle informazioni;
- la soddisfazione dei clienti e di tutte le parti interessate;
- la conformità al GDPR e alle norme ISO 9001, ISO 27001 e ISO 27017.

Ogni collaboratore è chiamato a contribuire al raggiungimento di questi obiettivi nell'ambito delle proprie responsabilità.

Finalità del Sistema di Gestione

MADE IN BIT è orientata al miglioramento continuo delle proprie capacità organizzative, tecniche e professionali, attraverso lo sviluppo delle competenze del personale, l'innovazione tecnologica e l'ottimizzazione dei processi aziendali. La Direzione ritiene che l'adozione e il mantenimento di un Sistema di Gestione conforme alle norme ISO 9001 e ISO 27001 costituiscano uno strumento essenziale per:

- garantire la soddisfazione del cliente e delle parti interessate;
- assicurare la conformità ai requisiti cogenti e contrattuali applicabili;
- gestire i rischi e cogliere le opportunità connesse ai processi aziendali;
- migliorare in modo continuo l'efficacia e l'efficienza del Sistema di Gestione.

Contesto competitivo

MADE IN BIT è consapevole di operare in un contesto competitivo:

- la crescente complessità dei servizi ICT richiede una struttura organizzativa solida, processi definiti e responsabilità chiaramente assegnate;
- l'innovazione tecnologica impone un costante aggiornamento delle competenze e degli strumenti operativi;
- la qualità dei servizi software, sistemistici, di assistenza e di formazione rappresenta un fattore competitivo determinante;
- la volontà di consolidare e ampliare la propria presenza nel mercato ICT richiede evidenza oggettiva della capacità organizzativa e della costanza delle prestazioni.

La Direzione Aziendale analizza il contesto sulla base di fattori interni quali:

- Le strategie aziendali attuali e future e le relative priorità.
- Il livello di innovazione, attuale e prevista, per MADE IN BIT.
- La struttura organizzativa per i sistemi informativi, inclusi i fornitori principali e i processi affidati all'esterno (in outsourcing o esternalizzati) e le caratteristiche delle sedi dei locali dove sono trattate le informazioni e dove sono collocati gli archivi e i sistemi informatici, inclusi quelli presso fornitori o altre parti esterne.
- Le tipologie delle informazioni trattate ed il relativo livello di protezione voluto.
- I rapporti con il personale interno (indipendentemente dalla tipologia di contratto tra le parti) e le loro competenze informatiche.
- Le aspettative delle parti interne interessate (stakeholder), ossia dei clienti attuali e potenziali, dei fornitori, del personale, degli azionisti e dei soci; tra queste aspettative vi è il rispetto dei contratti e degli accordi e la buona qualità dell'ambiente di lavoro.
- L'evoluzione: della tecnologia, della normativa applicabile, dei concorrenti ed i potenziali concorrenti e delle strategie di mercato.

Impegni operativi della Direzione Aziendale

MADE IN BIT si impegna quindi a:

- assicurare il rispetto costante delle leggi e degli altri regolamenti applicabili, la corretta applicazione delle tecnologie utilizzate;
- predisporre una struttura organizzativa dotata di metodologie di lavoro concepita in modo da prevenire carenze nei processi e capace di intervenire, per correggersi, sulle proprie modalità operative in ogni fase del ciclo produttivo, dallo studio per l'acquisizione delle commesse fino alla erogazione del servizio;
- ricercare, anche con il contributo di tutte le parti interessate, l'ottimizzazione dei processi aziendali al fine di migliorare le performance aziendali e raggiungere il massimo livello di efficacia ed efficienza compatibilmente con lo stato dell'arte;
- assicurare il costante supporto organizzativo, finanziario e operativo per migliorare il proprio Sistema di Gestione, garantendone la certificazione in relazione alle norme ISO 9001 e ISO 27001 (con l'estensione alla 27017);
- analizzare le esigenze dei clienti e degli utenti dei servizi erogati;
- tenere sotto controllo, attraverso un monitoraggio continuo ed efficace, il raggiungimento delle aspettative dei clienti e degli utenti dei servizi erogati;
- analizzare i risultati consuntivi delle commesse concluse confrontandoli con le ipotesi iniziali per una validazione delle stesse;
- assicurare che tutto il personale riceva adeguata informazione e formazione sui requisiti del Sistema di Gestione, ne condivida la politica e gli obiettivi e ne comprenda le implicazioni per quanto riguarda il proprio ruolo all'interno di MADE IN BIT e il proprio comportamento nel lavoro;
- controllare che i collaboratori e terze parti che lavorano per MADE IN BIT adottino gli stessi criteri stabiliti da MADE IN BIT;
- responsabilizzare tutto il personale al fine di renderlo consapevole dei propri obblighi e dell'importanza di ottemperare ai requisiti del cliente;
- impostare le fasi di pianificazione, controllo, monitoraggio e riesame per garantire che la politica sia rispettata e assicurare l'efficacia del Sistema di Gestione;
- effettuare verifiche, ispezioni e audit, atti ad identificare e a prevenire eventuali situazioni di Non Conformità e promuovere Azioni Correttive;
- mantenere un ruolo proattivo della Direzione Aziendale per la promozione del miglioramento continuo nelle materie interessate dal Sistema di Gestione sottoponendo a periodico riesame la politica e l'applicazione del Sistema di Gestione per valutarne la correttezza e l'efficacia.

Valore delle informazioni e impegno per la sicurezza

MADE IN BIT è consapevole che oggi viviamo in una società basata sulla conoscenza, in cui le informazioni sono un patrimonio prezioso. Le informazioni, sia relative a dati personali che ai dati aziendali, in qualsiasi forma

devono essere protette adeguatamente da tutte le minacce e le vulnerabilità, siano esse interne o esterne, intenzionali o accidentali.

La Direzione Aziendale ritiene che la salvaguardia della riservatezza, integrità e disponibilità delle informazioni siano aspetti fondamentali per assicurare, oltre la conformità legale, il mantenimento di una affidabile immagine di MADE IN BIT verso i propri dipendenti, collaboratori, clienti, fornitori e terze parti interessate.

La Direzione Aziendale è consapevole che la corretta gestione della sicurezza delle informazioni riguarda tutti gli aspetti dalla vita societaria, ed è quindi attivamente impegnata ad ottenere la partecipazione competente e responsabile di tutti i collaboratori aziendali e, per quanto possibile, dei soggetti terzi interessati.

I livelli di protezione da garantire devono essere tali da rispettare le clausole contrattuali e la normativa vigente, nonché da garantire la coerenza e il bilanciamento tra: rischio di impresa, sostenibilità economica, risultati delle analisi e valutazione del rischio, politiche e strategie aziendali, politiche e strategie dei fornitori e dei clienti, necessità di costante adeguamento al contesto in cui MADE IN BIT opera e di miglioramento dell'efficacia ed efficienza dei propri processi e controlli di sicurezza.

In particolare, il Regolamento Europeo [2016/679] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora in poi GDPR) individua i principi applicabili al trattamento dei dati (Art. 5) e obbliga il titolare a mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (Art. 24).

I principi cardine a cui attenersi per la sicurezza delle informazioni sono:

- le informazioni devono essere accessibili solo a coloro che ne hanno necessità (principio need to know) e nei tempi stabiliti;
- il personale deve essere opportunamente formato in materia di sicurezza delle informazioni e deve seguire i principi etici e comportamentali prescritti;
- i fornitori devono essere opportunamente tenuti sotto controllo attraverso misure da stabilire a seconda dei casi;
- i partner devono essere selezionati anche per la loro capacità e disponibilità a conformarsi alle regole di sicurezza di MADE IN BIT;
- per i servizi erogati, è necessario considerare i requisiti di sicurezza sin dalla contrattazione con il cliente.

Benefici attesi

La corretta applicazione del Sistema di Gestione dovrebbe garantire gli obiettivi di sicurezza delle informazioni. In particolar modo i benefici che ci si aspetta di ottenere dall'implementazione del Sistema di Gestione sono i seguenti:

- Prevenire incidenti relativi alla sicurezza delle informazioni anche per prevenire danni di immagine.
- Rendere sistematica la gestione della sicurezza informatica.
- Individuare le cause di inefficacia dei processi di gestione anche attraverso un sistema di segnalazione di Non Conformità, reclami, incidenti e quasi incidenti e di monitoraggio degli stessi e dei costi connessi.
- Determinare le conseguenze dei requisiti normativi e contrattuali.
- Comunicare ai clienti gli sforzi per l'aumento consapevole della sicurezza delle informazioni.

Sostenibilità ambientale

L'organizzazione riconosce l'importanza della sostenibilità ambientale e si impegna a promuovere pratiche responsabili nell'uso delle risorse. L'adozione di una politica per il risparmio della carta nell'uso di programmi informatici è parte integrante della strategia per ridurre l'impatto ambientale e ottimizzare i processi operativi. A tal fine i prodotti di MADE IN BIT permettono sempre la produzione di documenti digitali (WORD o EXCEL) che permettono la consultazione immediata senza bisogno di procedere alla stampa cartacea. Nei servizi di assistenza verranno privilegiati collegamenti via web al fine di evitare spostamenti fisici.

Partecipazione attiva del personale

Ciascun componente dell'organizzazione deve partecipare attivamente alla crescita dei prodotti e servizi forniti da MADE IN BIT collaborando alla definizione delle Procedure e Istruzioni e impegnandosi sia nella rilevazione che nella pronta rimozione di Non Conformità nei "processi" rispetto alle linee definite dalla documentazione per un continuo miglioramento di tutte le funzioni che partecipano alle attività di MADE IN BIT.

La Direzione Aziendale di MADE IN BIT richiama tutto il personale al perseguimento della politica ed alla completa osservanza dei contenuti del presente Manuale, delle Procedure e delle Istruzioni nell'ambito delle rispettive competenze e responsabilità, considerando fra l'altro che gli aspetti legati al raggiungimento di adeguati standard di qualità si ottengono innanzitutto da chi esegue le varie attività e non da chi le controlla.

5.2.1 Conoscenza, applicazione ed aggiornamento della politica

La Direzione Aziendale si impegna affinché la Politica sia compresa, attuata e sostenuta a tutti i livelli dell'organizzazione mediante i seguenti strumenti:

- pubblica la Politica nell'area pubblica del sito aziendale in modo che qualunque portatore di interesse possa prenderne visione;
- assegna al RSG l'autorità e l'autonomia per lo sviluppo e il coordinamento del Sistema di Gestione e la responsabilità di fornire tutti i chiarimenti eventualmente richiesti da ogni funzione di MADE IN BIT e comunque di valutare il grado di conoscenza e comprensione della Politica durante gli audit;
- assegna le responsabilità secondo le competenze specifiche di ognuno, fissando le procedure da seguire durante tutte le fasi di sviluppo dei servizi / prodotti, dall'acquisizione e definizione dei contratti, fino alla erogazione dei servizi o consegna dei prodotti;
- si occupa della formazione del personale, sia per le attività specifiche che per le problematiche connesse al Sistema di Gestione.

La politica è approvata dalla Direzione Aziendale e riesaminata almeno annualmente per assicurare che sia appropriata alle attività di MADE IN BIT.

5.2.2 Pianificazione

MADE IN BIT individua e pianifica le risorse necessarie per raggiungere gli obiettivi stabiliti.

Tale pianificazione include:

- la definizione dei processi coperti dal Sistema di Gestione;

- la definizione delle risorse necessarie per la gestione dei processi;
- la definizione delle modalità adottate per garantire il miglioramento continuativo del Sistema di Gestione.

In generale il perseguimento degli obiettivi si attua attraverso:

- L'impegno finanziario per reperire le risorse necessarie (in termini di personale e di mezzi) e l'introduzione di nuove tecnologie di gestione.
- La predisposizione della documentazione relativa alle attività delle funzioni coinvolte nei processi aziendali, in modo da avere il massimo controllo durante l'erogazione dei servizi commissionati.
- La valorizzazione delle risorse umane mediante la formazione pianificata in relazione alle esigenze e mansioni dei singoli e dell'insieme.

Gli obiettivi sono espressi in modo da individuare i risultati da raggiungere, le risorse da mettere a disposizione, indicando eventualmente anche le modalità di verifica ed i termini temporali entro i quali tali obiettivi devono essere raggiunti.

5.2.3 Obiettivi e miglioramento

Obiettivi

MADE IN BIT desidera migliorare costantemente la definizione delle esigenze dei portatori di interesse e la loro soddisfazione.

Da questo obiettivo di carattere generale e strategico discendono obiettivi specifici per le funzioni ed i livelli aventi responsabilità nell'ambito del Sistema di Gestione in funzione di:

- politica
- conformità legislativa o rispetto di eventuali prescrizioni o regolamenti sottoscritti
- sicurezza delle informazioni
- risultati del Riesame della Direzione
- opportunità tecnologiche, disponibilità di risorse finanziarie ed operative
- punti di vista delle parti interessate
- reclami o altre segnalazioni dei clienti
- grado di influenza di MADE IN BIT sui vari aspetti
- modifiche al Sistema di Gestione a seguito di anomalie, di Non Conformità, di carenze segnalate dal personale o dai consulenti o evidenziatesi nel corso delle attività e dei processi
- introduzione di miglioramenti al Sistema di Gestione.

Gli obiettivi, per ogni funzione avente responsabilità, sono stabiliti annualmente dalla Direzione Aziendale in funzione delle strategie aziendali e di quanto emerso in occasione del Riesame della Direzione. Tali obiettivi stabiliti sono comunicati alle funzioni coinvolte.

Gli obiettivi sono soggetti a revisione, condotta dal RSG di comune accordo con i vari responsabili operativi. L'esigenza di procedere alla revisione degli obiettivi è dettata dal verificarsi di una delle seguenti circostanze:

- Riesame della Direzione di MADE IN BIT.
- Esigenze di miglioramento continuo all'interno di MADE IN BIT.
- Modifiche nei processi e prodotti di MADE IN BIT.

L'elenco degli obiettivi è riportato nel verbale del Riesame della Direzione con azioni da intraprendere ed assegnazione delle responsabilità ai diversi livelli della struttura organizzativa, con la definizione dei tempi previsti e delle risorse coinvolte.

Miglioramento continuo

MADE IN BIT pianifica e gestisce i processi necessari per il miglioramento continuativo del Sistema di Gestione.

Il Responsabile del Sistema di Gestione (RSG), periodicamente e comunque in preparazione dei Riesami della Direzione, provvede ad effettuare l'analisi di tutte le Non Conformità (comprese quelle originate dai reclami dei clienti) per individuare eventuali ripetitività, l'analisi dettagliata delle Non Conformità episodiche ma rilevanti, l'analisi di eventuali incidenti relativi alla sicurezza delle informazioni, l'analisi dei verbali degli Audit Interni ed Esterni, l'analisi dei risultati delle Azioni Correttive, l'analisi delle misurazioni sui processi e sulla soddisfazione dei clienti.

5.2.4 Pianificazione del Sistema di Gestione

La Direzione Aziendale assicura che la pianificazione del Sistema di Gestione nel corso dei Riesami della Direzione sia condotta in modo da soddisfare i requisiti generali conseguendo gli obiettivi definiti.

Particolare attenzione verrà posta in caso di modifiche al sistema per garantirne l'integrità del Sistema di Gestione.

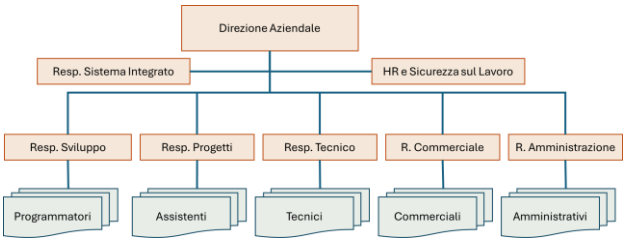
L'uso del marchio di certificazione e dei relativi riferimenti è regolato dalla documentazione dell'Ente certificante che viene reperita dai siti deputati.

5.3 Ruoli, responsabilità e autorità

5.3.1 Responsabilità ed autorità

Generalità

MADE IN BIT, al fine di garantire un corretto svolgimento delle attività, è strutturata in un insieme di funzioni descritte nell'organigramma riportato di seguito.



Le informazioni relative alle responsabilità ed autorità sono comunicate al personale interessato sia mediante la disponibilità del presente Manuale e delle Procedure di interesse sia durante gli incontri periodici di informazione e formazione sui processi aziendali.

MADE IN BIT considerando indispensabile un'adeguata competenza di tutte le risorse umane di MADE IN BIT, come descritto nel presente documento, individua e definisce le competenze necessarie ed adeguate alle attività svolte dal personale.

Responsabilità per il sistema

Le funzioni aziendali a tutti i livelli, oltre agli specifici compiti descritti nel presente Manuale, sono impegnate a:

- contribuire alla diffusione e all'applicazione dei criteri contenuti nel presente manuale;

- attenersi, nell'attività quotidiana, alle Procedure emesse;
- emettere la documentazione operativa di propria pertinenza;
- individuare, con il supporto del RSG, le necessità di addestramento del personale, sottoponendo le proposte alla Direzione Aziendale;
- segnalare al RSG le Non Conformità nelle attività di propria competenza;
- collaborare per il continuo miglioramento del sistema, attuando le Azioni Correttive di propria pertinenza;
- richiedere la modifica di procedure o di istruzioni in caso di difficile comprensione o applicazione.

L'illustrazione dei compiti e delle responsabilità, unitamente alla descrizione delle modalità esecutive, è inserita nelle singole Procedure.

5.3.2 Proprietario delle Informazioni (PdI)

Il Proprietario delle Informazioni all'interno di MADE IN BIT è rappresentato dal Datore di Lavoro.

Il PdI in funzione delle esigenze aziendali, anche avvalendosi delle applicazioni informatiche, genera l'informazione e ne determina: obiettivi e finalità; logiche di elaborazione; caratteristiche e requisiti.

In quanto proprietario, è responsabile della valorizzazione delle informazioni che sono sotto il suo controllo e della definizione dei criteri di designazione degli utenti ai quali conferire l'abilitazione all'accesso.

Ogni accesso ai dati deve infatti essere concesso o negato in conformità alle disposizioni emanate dal PdI, con il supporto del Responsabile del Sistema Informatico (RSI).

Il PdI è proprietario o ha la disponibilità dell'HW e del SW funzionali ai sistemi informativi di produzione e ha assegnato al RSI la responsabilità di assicurarne il corretto funzionamento.

Il PdI è anche il Titolare per il trattamento dei dati personali e ne garantisce la conformità al GDPR.

Il PdI deve, in particolare:

- Stabilire il livello di rischio accettabile.
- Riesaminare periodicamente ed in concomitanza con modifiche organizzative o novità tecnologiche l'adeguatezza e la validità del SGI per la sicurezza delle informazioni.
- Valutare i nuovi servizi da proporre agli Stakeholder in base all'evoluzione tecnologica anche analizzando le proposte dei competitor.
- Nominare il Responsabile del Sistema di Gestione (RSG) e fornirgli l'autorità e le risorse necessarie.
- Nominare il Responsabile del Sistema Informatico (RSI) e fornirgli risorse sufficienti a sviluppare, implementare, far funzionare e mantenere i sistemi informativi di produzione.

5.3.3 Responsabile del Sistema di Gestione (RSG)

Al RSG, è conferita per delega dalla Direzione Aziendale l'autorità e la libertà organizzativa per predisporre il Sistema, assicurarne la conoscenza e condivisione da parte di tutto il personale, garantirne l'adeguatezza e sorvegliarne lo sviluppo per individuare ed analizzare le aree ritenute in grado di causare problemi rilevanti ai fini della qualità, promuovere o proporre soluzioni a detti problemi e verificare l'attuazione delle soluzioni adottate.

RSG ha il compito di riferire alla Direzione Aziendale sulle prestazioni del sistema e sulle esigenze di miglioramento.

5.3.4 Responsabile del Sistema Informatico (RSI).

Assicura il corretto funzionamento dei sistemi informatici aziendali e garantisce la protezione dei dati con il supporto degli specialisti. Svolge il ruolo di Amministratore di Sistema per MADE IN BIT[2].

5.3.5 Responsabile della Pianificazione (RP).

Coordina le fasi di studio e acquisizione delle commesse, analizza i requisiti del cliente e ne verifica la fattibilità.

5.3.6 Responsabile delle Attività di Progettazione (RAP).

Coordina le attività di progettazione e sviluppo, assicurando la conformità agli elementi in ingresso e l'approvazione degli output progettuali.

5.3.7 Responsabile dell'Erogazione della Commessa (REC).

Gestisce l'esecuzione operativa della Commessa, assicurando il rispetto dei requisiti contrattuali, dei tempi e degli standard aziendali.

6 PIANIFICAZIONE

MADE IN BIT pianifica il Sistema di Gestione assicurando che sia in grado di conseguire i risultati attesi e di migliorare in modo continuo.

6.1.1 Azioni per affrontare rischi e opportunità

La Direzione, in occasione del Riesame, identifica e valuta i rischi e opportunità relativi a qualità del servizio e sicurezza delle informazioni sulla base dell'analisi per Processo, registrata su SQuadra e presente fra gli elementi di ingresso, e definisce le azioni da intraprendere individuando e registrando su SQuadra responsabilità, tempi e criteri di verifica dell'efficacia.

MADE IN BIT adotta un approccio sistematico alla gestione dei rischi e delle opportunità, differenziato per le due dimensioni del Sistema di Gestione:

- Per la qualità del servizio: i rischi e le opportunità sono identificati per ciascun processo aziendale, valutati in termini di probabilità e impatto sulla conformità del servizio, e registrati nell'analisi per processo su SQuadra. Le azioni di trattamento sono definite con responsabilità, tempi e criteri di verifica.
- Per la sicurezza delle informazioni: la valutazione dei rischi segue una metodologia specifica di valutazione del rischio (descritta nell'Appendice ISO 27001 del manuale di SQuadra), basata sull'identificazione degli asset informativi, delle minacce e delle vulnerabilità, e sulla valutazione dell'impatto su riservatezza, integrità e disponibilità.

[2] Per Amministratori del sistema si intendono quelle figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. Non rientrano invece quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software. Non rientrano neppure gli amministratori dei singoli personal computer che non devono contenere dati personali.

Le valutazioni dei rischi e delle opportunità, le azioni di trattamento, le responsabilità e i tempi previsti sono registrati su SQuadra e costituiscono elementi in ingresso per il Riesame della Direzione.

Dichiarazione di Applicabilità (SoA).

I risultati della valutazione dei rischi alimentano la Dichiarazione di Applicabilità presente su SQuadra, in cui, per tutti i controlli previsti dall'Appendice A della norma ISO 27001 con l'indicazione, per ciascuno, dell'applicabilità o della non applicabilità (con relativa giustificazione)

La Dichiarazione di Applicabilità è gestita dal RSI, approvata dalla Direzione e riesaminata in occasione di ogni aggiornamento significativo della valutazione dei rischi.

6.1.2 Obiettivi e pianificazione per il loro raggiungimento

Sono definiti obiettivi misurabili negli indicatori delle prestazioni registrati su SQuadra dove vengono raccolte anche le valutazioni periodiche con indicazione del responsabile, del tipo di monitoraggio e criteri di valutazione, della frequenza di controllo prevista, del valore rilevato rispetto all'obiettivo prefissato.

6.1.3 Pianificazione delle modifiche

Ogni modifica significativa (processi, infrastrutture, applicazioni, fornitori, requisiti clienti o normativi) è pianificata (scopo e potenziali conseguenze, integrità del Sistema di Gestione, disponibilità di risorse, eventuale riassegnazione delle responsabilità) e valutata prima dell'attuazione, considerando impatti su qualità, continuità operativa e sicurezza, e mantenendo adeguate evidenze documentate.

7 SUPPORTO

L'Organizzazione assicura il supporto necessario per l'efficace funzionamento del Sistema di Gestione, determinando e rendendo disponibili risorse, competenze, consapevolezza, comunicazione e informazioni documentate.

7.1 Gestione delle risorse

7.1.1 Messa a disposizione delle risorse

MADE IN BIT ha individuato e messo a disposizione le risorse necessarie (persone, infrastrutture, strumenti HW/SW, ambienti di lavoro, servizi cloud/fornitori) per:

- attuare e tenere aggiornato il Sistema di Gestione e migliorare in modo continuativo la sua efficacia; per tali attività ha incaricato il RSG;
- mantenere aggiornate, rispetto all'evoluzione delle metodologie e delle tecniche, le strumentazioni;
- ottenere ed incrementare la soddisfazione dei clienti, rispettando i requisiti definiti in fase contrattuale; per tali attività MADE IN BIT ha individuato le funzioni responsabili dei processi relativi alla valutazione dei requisiti definiti dal cliente in fase contrattuale, alla valutazione delle informazioni di ritorno dai clienti e dagli utenti che permettono di determinarne il livello di soddisfazione e alla valutazione delle Azioni Correttive necessarie ad incrementarne la soddisfazione.

Le risorse particolari necessarie per lo svolgimento del servizio vengono individuate valutando la tipologia e le caratteristiche del servizio da erogare e sono riportate nei MD8.4A "*Piani di Qualità della Commessa*" (PdQ).

MADE IN BIT provvederà ad assicurare, attraverso un'adeguata sensibilizzazione ed informazione, che le attività eventualmente affidate a personale o società esterne vengano condotte secondo criteri compatibili con il Sistema di Gestione di MADE IN BIT.

7.1.2 Risorse umane

Le risorse umane di MADE IN BIT sono impiegate nei seguenti ambiti:

- progettazione e sviluppo software;
- installazione, configurazione e gestione di sistemi hardware e infrastrutture IT;
- servizi di assistenza tecnica e manutenzione;
- progettazione ed erogazione di attività formative;
- attività amministrative, commerciali e di supporto ai processi aziendali.

La Direzione Aziendale assicura che siano rese disponibili risorse adeguate in termini di numero, competenze e responsabilità per garantire la conformità dei servizi erogati e il corretto funzionamento del Sistema di Gestione.

7.1.3 Infrastrutture

MADE IN BIT individua, mette a disposizione e mantiene le infrastrutture necessarie per garantire la conformità dei servizi erogati.

Rientrano tra le infrastrutture:

- postazioni di lavoro attrezzate per sviluppo software e attività amministrative;
- server, reti, sistemi di backup e dispositivi di sicurezza informatica;
- strumenti hardware e software per attività di installazione, configurazione e assistenza tecnica;
- ambienti di test e sviluppo;
- strumenti per il monitoraggio e la diagnostica;
- locali per attività formative, ove previste;
- strumenti di comunicazione e collaborazione interna ed esterna.

Le infrastrutture sono oggetto di manutenzione, aggiornamento e verifica periodica per garantirne l'efficienza e l'adeguatezza.

7.1.4 Ambiente di lavoro

MADE IN BIT tiene sotto controllo l'ambiente di lavoro, inteso come le condizioni di lavoro in cui opera il personale. Specifiche attività e/o programmi di miglioramento sono avviati per garantire che l'ambiente di lavoro abbia una positiva influenza sulle motivazioni, soddisfazione e sul rendimento finale del personale.

Tali condizioni comprendono fattori fisici, sociali, psicologici ed ambientali.

MADE IN BIT ritiene opportuno un ambiente di lavoro confortevole per i propri dipendenti; a tal fine gli uffici sono ampli, luminosi e dotati di aria condizionata e comunque si cerca di garantire l'ergonomia di tutte le strutture utilizzate dai dipendenti.

Per creare un ambiente di lavoro accettabile MADE IN BIT prende in considerazione:

- metodi di lavoro che salvaguardino il benessere del personale;
- norme di comportamento che proteggono la salute dei lavoratori;

- l'ergonomia;
- l'illuminotecnica ed il microclima.

Per quanto riguarda l'ambiente di lavoro in relazione alle caratteristiche del servizio erogato, in fase di pianificazione del Servizio, sono valutate le eventuali condizioni ambientali dei locali presso i quali verrà erogato il servizio.

7.1.5 Risorse per il monitoraggio e la misurazione

MADE IN BIT ha determinato e reso disponibili le risorse necessarie per il monitoraggio, la misurazione, la verifica e il controllo dei propri prodotti e servizi, al fine di assicurare risultati validi, affidabili e coerenti con i requisiti applicabili.

In particolare l'uso di SQuadra permette di avere in un unico ambiente tutte le informazioni sullo stato del sistema e permette una pianificazione delle scadenze.

7.1.6 Conoscenza organizzativa

La Direzione Aziendale ha determinato la conoscenza necessaria per il funzionamento dei propri processi e per conseguire la conformità nei servizi offerti e la sicurezza delle informazioni ed ha attribuito la responsabilità di definire tali conoscenze indicandole nell'analisi dei processi e nelle schede nominative del personale.

Tale conoscenza deve essere mantenuta e messa a disposizione, nella misura necessaria per cui sono predisposte idonee Istruzioni Operative quando ritenuto necessario a rendere alcune modalità operative patrimonio di MADE IN BIT.

Nell'affrontare le esigenze e tendenze di cambiamento, (determinato ad esempio dall'introduzione di una nuova legislazione o dall'aggiornamento di una normativa esistente, in caso di introduzione di nuove funzionalità nel programma, in caso di variazione di una modalità lavorativa, ...) l'organizzazione considera la propria conoscenza attuale e determina come acquisire o accedere ad ogni necessaria conoscenza aggiuntiva e aggiornamenti richiesti.

La conoscenza organizzativa è la conoscenza specifica dell'organizzazione, maturata generalmente attraverso l'esperienza. Queste informazioni sono utilizzate e condivise al fine di conseguire gli obiettivi dell'organizzazione.

La conoscenza organizzativa può essere basata su:

- risorse interne (per esempio proprietà intellettuale; conoscenze maturate con l'esperienza; lezioni apprese da insuccessi o da progetti che hanno avuto successo; acquisizione e condivisione di conoscenze ed esperienze non documentate; risultati dei miglioramenti ottenuti nei processi, prodotti e servizi);
- risorse esterne (per esempio norme, fonti accademiche, conferenze, raccolta di conoscenze da clienti o fornitori esterni, supporto di consulenti, ecc.).

7.2 Competenza

MADE IN BIT determina le competenze necessarie per il personale che svolge attività che influenzano le prestazioni e la qualità dei servizi ICT erogati (analisti, sviluppatori, sistemisti, help desk, formatori).

In particolare l'organizzazione:

- definisce per ciascun ruolo le competenze richieste in termini di istruzione, esperienza, abilità tecniche e capacità organizzative;
- assicura che il personale sia competente sulla base di adeguata formazione, addestramento o esperienza;
- pianifica interventi di formazione, aggiornamento tecnico e affiancamento operativo ove necessario;
- valuta l'efficacia delle azioni intraprese;
- conserva informazioni documentate a supporto delle competenze (titoli di studio, certificazioni tecniche, curriculum, registrazioni formative).

Particolare attenzione è rivolta a:

- aggiornamento continuo in ambito tecnologico (software, cybersecurity, infrastrutture IT);
- sviluppo delle competenze relazionali del personale di assistenza e formazione;
- aggiornamento normativo e gestionale per il personale amministrativo.

La competenza è assicurata tramite formazione, affiancamento ed esperienza ed è documentata su SQuadra.

7.3 Consapevolezza

MADE IN BIT assicura che tutto il personale sia consapevole:

- della Politica per il Sistema di Gestione;
- degli obiettivi aziendali;
- del proprio ruolo e delle proprie responsabilità;

delle implicazioni derivanti dal mancato rispetto delle procedure del Sistema di Gestione (qualità del servizio, tempi, sicurezza dei dati).

La consapevolezza è promossa attraverso riunioni periodiche, comunicazioni interne e momenti formativi dedicati.

Addestramento

MADE IN BIT basa la propria organizzazione sulle capacità operative e gestionali del personale, per cui si preoccupa di formare ed istruire adeguatamente tutte le risorse a disposizione.

In particolare sono stati individuati i seguenti tipi di addestramento:

- formazione sui processi del Sistema di Gestione: è rivolta a tutto il personale aziendale e ad ogni nuovo assunto con funzioni che hanno influenza sul Sistema di Gestione stesso;
- formazione tecnico–operativa: è rivolta al personale di nuova assunzione, con particolare attenzione per coloro che non hanno esperienza specifica e al personale che deve cambiare mansione;
- aggiornamenti rivolti a tutto il personale.

La formazione avviene in occasione dell'assunzione, del trasferimento o cambiamento di mansione, dell'introduzione di nuove apparecchiature o nuove tecnologie.

Sistema disciplinare

In caso di violazioni potrà essere avviato il processo disciplinare per intraprendere provvedimenti nei confronti del personale che ha commesso una violazione della sicurezza delle informazioni.

Il processo disciplinare dovrà prevedere una risposta progressiva, che prenda in considerazione fattori quali: la natura e la gravità della violazione e il suo

impatto sull'azienda, se si tratta o meno di un primo reato o di una recidiva, se il trasgressore è stato debitamente istruito, la legislazione pertinente, i contratti aziendali e altri fattori se richiesti.

A fronte di una violazione RSI provvederà alla raccolta di tutte le evidenze anche al fine di potenziali azioni legali e disciplinari.

Sarà cura del RSI valutare, peraltro, l'opportunità di riconoscimenti in caso di condotte eccezionali (proposte, suggerimenti, segnalazioni, ecc.) riguardo alla sicurezza delle informazioni.

7.4 Comunicazione

L'efficace circolazione delle informazioni all'interno ed all'esterno dell'organizzazione, inclusa la gestione di comunicazioni su incidenti e disservizi, rappresenta un elemento chiave per promuovere la motivazione del personale nei confronti del Sistema di Gestione, favorire il processo di miglioramento continuo, creare consenso nei confronti delle attività di MADE IN BIT da parte della comunità esterna.

Il piano delle principali comunicazioni è inserito su SQuadra con l'indicazione di:

- Chi comunica.
- Con chi comunica.
- Cosa comunica.
- Come comunica.
- Quando comunica.

Comunicazioni interne

MADE IN BIT ritiene fondamentale coinvolgere tutto il personale nel perseguimento degli obiettivi. A tal fine il RSG assicura la diffusione, attraverso la "pubblicazione" nell'area dedicata del Server aziendale del presente manuale e degli estratti dei Riesami della Direzione contenenti gli obiettivi e le indicazioni relative alle modalità di raggiungimento degli obiettivi individuati, dei risultati raggiunti e di eventuali altre informazioni riguardanti l'efficacia del Sistema di Gestione stesso. È sempre cura del RSG attivarsi per raccogliere segnalazioni da parte di tutto il personale sul Sistema di Gestione.

Le modalità operative utilizzate di MADE IN BIT e descritte nel presente Manuale e nelle Procedure, consentono di assicurare comunicazioni efficaci (indipendentemente dal fatto che esse siano in forma scritta o verbale) tra i diversi livelli e funzioni all'interno dell'organizzazione.

Comunicazioni esterne

MADE IN BIT ritiene fondamentale comunicare con i clienti / utenti al fine di individuare i possibili problemi e le possibili soluzioni. A tal fine, all'inizio di ogni servizio viene consegnato il modulo MD10.1A "Reclami e Suggerimenti" che permette di inviare segnalazioni che verranno indirizzate direttamente all'attenzione del RSG che provvederà a gestirle, qualora significative, come NC.

7.5 Informazioni documentate

7.5.1 Generalità

In sintesi la documentazione è strutturata sui livelli gerarchici seguenti:

- Manuale del Sistema di Gestione (il presente documento), concernente le prescrizioni generali del Sistema di Gestione che rappresentano il livello attuativo della Politica aziendale (contenuta nel Manuale stesso) e delle prescrizioni della norma ISO 9001 e ISO 27001.
- Procedure, concernenti prescrizioni generali che individuano e definiscono le modalità di gestione e di attuazione di processi aziendali.
- Istruzioni che descrivono dettagli delle modalità esecutive di alcune attività specifiche, per le quali non sono state predisposte delle procedure o a completamento delle procedure esistenti.
- Moduli, documenti redatti per garantire la conformità al processo e ai requisiti stabiliti dall'organizzazione.
- Registrazioni, documenti che riportano i dati relativi alla gestione del Sistema di Gestione. La modulistica viene utilizzata per effettuare le registrazioni ovvero quei documenti che, una volta compilati, forniscono l'evidenza oggettiva della realizzazione delle attività in conformità a quanto stabilito dal Sistema di Gestione. Essi comprendono ad esempio: verbali, rapporti, maschere di inserimento dati su supporto informatico, ecc.

Fra le Registrazioni assumono particolare importanza:

- Piani della Progettazione (PdP) che permettono la definizione dei dati e requisiti di base, le apparecchiature necessarie, la documentazione di supporto, le attività da svolgere, le tempistiche, le responsabilità e le interfacce tra eventuali gruppi diversi coinvolti nel processo.
- Piani Qualità di Commessa (PdQ) che recepiscono i requisiti del Contratto e definiscono le modalità applicative del SG alla specifica Commessa.

7.5.2 Gestione dei documenti

La documentazione del Sistema di Gestione prodotta da MADE IN BIT è gestita, in accordo con la PG7.5A *"Gestione documentazione e registrazioni"*, assicurando che:

- i documenti siano identificati e sia garantito l'aggiornamento dello stato di revisione corrente;
- sia garantita l'identificazione e la leggibilità dei documenti;
- i documenti siano emessi secondo un iter prestabilito e siano approvati prima della loro emissione per garantire l'adeguatezza degli stessi;
- i documenti siano riesaminati e quando necessario aggiornati e riapprovati;
- sia garantita una gestione controllata delle modifiche, che devono essere identificate;
- siano disponibili edizioni appropriate dei documenti necessari in tutti i luoghi ove si svolgono attività essenziali per la corretta applicazione del Sistema di Gestione;
- siano eventualmente distribuiti in forma controllata;
- vengano prontamente rimossi da tutti i centri di emissione o di utilizzazione documenti (anche quelli di origine esterna) non validi e/o superati, o venga comunque evitato un loro uso indesiderato;
- siano adeguatamente identificati i documenti superati conservati per motivi legali e/o di conservazione delle conoscenze;
- sia disponibile l'elenco aggiornato di tutti i documenti in vigore del Sistema di Gestione.

La conoscenza di tali documenti da parte di tutti è necessaria per garantire l'applicazione del Sistema di Gestione. È compito di ognuno verificare lo stato di validità dei documenti disponibili nel sistema informativo provvedendo ad eliminare o correttamente identificare eventuali documenti superati.

I documenti del Sistema di Gestione sono soggetti a vincoli di riservatezza e pertanto ne è proibita la diffusione non autorizzata a persone non facenti parte dell'organizzazione.

La distribuzione esterna dei documenti è decisa dal RSG e riguarda generalmente il presente Manuale che potrà essere consegnato a clienti attuali o potenziali, all'ente di certificazione o ad altri enti che ne facessero richiesta.

7.5.3 Gestione delle registrazioni

Si considera documentazione di registrazione qualunque informazione che certifichi e dimostri la conformità dei servizi, materiali o attività, alle prescrizioni contrattuali, alle leggi e alle normative applicabili o che attesti che i responsabili, nel corso delle proprie attività, hanno effettuato le verifiche di loro competenza.

I documenti di registrazioni sono elaborati in tutte le attività per le quali risulta necessario dare evidenza della conformità e dell'efficace applicazione del Sistema di Gestione.

I documenti non dovranno subire alcuna manomissione o deterioramento in modo da garantire, per tutto il periodo di conservazione, la leggibilità ed il loro stato originale. Dovranno essere prese tutte le precauzioni, da parte dei responsabili dell'archiviazione, per evitare smarrimenti delle registrazioni.

Tutti i documenti di registrazione dovranno essere consultabili, su richiesta, da parte delle funzioni aziendali autorizzate. I documenti dovranno essere consultabili su richiesta da parte degli Enti di Certificazione e, quando previsto dal contratto, anche da parte del cliente o di un suo rappresentante.

I documenti di registrazione sono gestiti secondo la relativa PG7.5A "*Gestione documentazione e registrazioni*" che definisce le modalità per:

- identificarli e correlarli al processo cui si riferiscono;
- raccoglierli e archiviarli;
- garantire che siano adeguatamente protetti;
- assicurare che siano facilmente rintracciabili e consultabili (reperibili);
- conservarli per un tempo predefinito;
- eliminarli.

La procedura PG7.5A "*Gestione documentazione e registrazioni*" fornisce, inoltre, specifiche indicazioni per la gestione delle registrazioni in formato elettronico con particolare riferimento alle modalità da adottare per:

- l'archiviazione;
- la protezione;
- la gestione delle Firme.

Alcune informazioni sono archiviate su SQuadra di cui detengono le credenziali per l'accesso unicamente RSG e RSI. Le informazioni sulla sicurezza dei dati archiviati su SQuadra sono riportate nel Manuale del prodotto.

8 ATTIVITÀ OPERATIVE

8.1 Pianificazione della erogazione del servizio

I servizi erogati e i prodotti forniti da MADE IN BIT sono gestiti attraverso commesse o contratti, ciascuno pianificato e controllato in modo sistematico.

Per ogni incarico o contratto l'organizzazione:

- analizza i requisiti del cliente, contrattuali e normativi applicabili;
- valuta i rischi e le opportunità connessi all'erogazione del servizio;
- definisce le risorse necessarie (umane, tecnologiche e infrastrutturali);
- stabilisce le responsabilità e le modalità operative;
- individua le attività di monitoraggio e i criteri di accettazione.

La pianificazione può assumere forma diversa in funzione della tipologia di servizio:

- **Progetti di sviluppo software** → pianificazione delle fasi di analisi, progettazione, sviluppo, test, rilascio e assistenza post-avviamento;
- **Progetti sistemistici** → pianificazione di installazione, configurazione, collaudo e messa in esercizio;
- **Servizi di assistenza continuativa** → definizione di SLA, modalità di presa in carico e gestione delle richieste;
- **Attività formative** → pianificazione dei contenuti, delle modalità di erogazione e delle risorse didattiche.

Per le commesse di particolare complessità o rilevanza può essere predisposto un Piano della Qualità della Commessa (MD8.4A), che recepisce i requisiti contrattuali e definisce:

- modalità applicative del Sistema di Gestione;
- documentazione specifica da produrre;
- eventuali attività di verifica, validazione o collaudo;
- criteri di accettazione del servizio.

Durante l'erogazione del servizio sono attuate attività di controllo dello stato di avanzamento, verifica tecnica e riesame periodico, al fine di garantire il rispetto dei requisiti concordati e il raggiungimento degli obiettivi previsti.

Le modifiche ai requisiti o alle condizioni contrattuali sono riesaminate, valutate e formalmente gestite prima della loro attuazione.

8.1.1 Acquisizione delle commesse

Determinazione dei requisiti relativi alle commesse

MADE IN BIT opera in modo tale che per ogni attività tutti i requisiti applicabili siano correttamente determinati (quelli precisati dal cliente, quelli non precisati dal cliente ma comunque necessari, quelli attesi dagli utenti, quelli cogenti, quelli stabiliti da MADE IN BIT stessa).

Queste operazioni sono svolte preliminarmente durante il processo di pianificazione delle commesse e quindi in fase di ristudio in caso di acquisizione della Commessa stessa.

8.2 Riesame dei requisiti relativi alle commesse

L'attività di studio e acquisizione della Commessa viene coordinata dal RP e vede il coinvolgimento delle funzioni che contribuiscono alla formulazione dell'offerta e di quelle interessate alla eventuale successiva erogazione del servizio oggetto della Commessa.

Lo scopo dello studio è garantire che:

- le caratteristiche del servizio/prodotto siano chiaramente definite: vincoli legislativi, documentazione da produrre, verbalizzazioni da compilare, ecc.;
- eventuali scostamenti del contratto rispetto a quanto indicato in sede di offerta siano risolti;
- MADE IN BIT abbia la capacità di soddisfare i requisiti della Commessa.

Le fasi nelle quali l'attività di esame si articola sono:

- preliminare all'emissione dell'offerta, mirata:
  - alla verifica del recepimento da parte di MADE IN BIT di tutte le prescrizioni del cliente e delle aspettative degli utenti;
  - all'analisi delle richieste del cliente / utenti e alla verifica della capacità di soddisfarle, da parte di MADE IN BIT, in termini di competenze, risorse, mezzi e tempi;
  - alla verifica della fattibilità della Commessa;
  - alla verifica della fattibilità della nuova Commessa in considerazione delle capacità organizzative di MADE IN BIT;
  - alla verifica della documentazione prodotta in sede di studio della Commessa.
- preliminare alla firma del contratto o all'accettazione di un ordine, mirata:
  - ad un riesame della Commessa con l'eventuale elaborazione di un nuovo studio tecnico di fattibilità;
  - al riesame del contratto o dell'ordine stesso.
- preliminare all'accettazione delle eventuali modifiche proposte dopo la firma del contratto o l'accettazione dell'ordine.

I documenti contrattuali e gli elaborati dello studio della Commessa saranno gli elementi di riferimento per l'elaborazione della documentazione di pianificazione delle commesse.

Nella procedura PG8.1A "*Studio e acquisizione delle commesse*" vengono descritte le modalità stabilite da MADE IN BIT per la definizione dell'offerta e del contratto e per eventuali modifiche richieste dal cliente in corso d'opera.

Informazioni relative all'approvvigionamento

Il Responsabile della Pianificazione (RP) analizza i contratti, gli ordini e le richieste dei clienti per definire le necessità di approvvigionamento relative a tutti i servizi erogati da MADE IN BIT, inclusi:

- sviluppo software (licenze, strumenti, framework, consulenze specialistiche);
- progettazione e gestione di sistemi hardware e infrastrutture IT;
- servizi di assistenza tecnica e manutenzione;
- attività formative;
- supporto amministrativo e logistico.

Le richieste di acquisto, noleggio o locazione di materiali, apparecchiature, software, infrastrutture, locali aziendali o esterni, nonché l'impiego di consulenti o personale specializzato, vengono effettuate considerando i tempi necessari per garantire la corretta pianificazione e realizzazione dei servizi.

Tutte le informazioni contenute nei documenti per l'approvvigionamento devono essere complete, chiare e non ambigue, in modo da:

- definire con precisione i beni, i servizi o le risorse da acquisire;
- consentire la selezione del fornitore più idoneo;
- facilitare la tracciabilità tra requisiti, fornitori e consegne;
- garantire la conformità ai requisiti contrattuali, normativi e di qualità.

Le informazioni documentate relative all'approvvigionamento sono conservate secondo le modalità previste dal Sistema di Gestione.

Verifica dei prodotti approvvigionati

In relazione alle caratteristiche dei materiali e delle apparecchiature acquistati o noleggiati viene verificata dal REC la conformità ai requisiti dell'ordine.

La prestazione di eventuali Consulenti viene valutata dal REC alla fine di ogni Commessa.

8.3 Progettazione

8.3.1 Generalità

MADE IN BIT progetta ogni intervento, sia esso relativo allo sviluppo di soluzioni software, alla progettazione ed erogazione di attività formative, oppure all'installazione e configurazione di sistemi hardware e infrastrutture IT. Per ciascuna tipologia di intervento, il processo di progettazione segue le modalità definite nella Procedura PG8.3A "*Gestione della progettazione*".

8.3.2 Pianificazione della progettazione

All'interno di MADE IN BIT è stato individuato il Responsabile delle Attività di Progettazione (RAP), dotato di adeguata professionalità, che ha il compito di coordinare tutte le attività legate alla progettazione collaborando, ove già individuato, con il Responsabile dell'Erogazione della Commessa (REC).

Quando si presentano nuove commesse, MADE IN BIT pianifica e tiene sotto controllo la progettazione del Servizio da realizzare con le modalità definite nella Procedura Gestionale PG8.3A "*Gestione della Progettazione*".

Il processo di progettazione è pianificato attraverso l'elaborazione di un Piano di progettazione (PdP) in modo da stabilire:

- la definizione dei dati e dei requisiti di base e l'elencazione delle Normative cogenti;
- le attività da svolgere (fasi della progettazione e attività di riesame, verifica e validazione);
- le tempistiche complessive e per le varie attività con relative interazioni;
- le responsabilità per le varie attività;
- le interfacce tra eventuali gruppi diversi coinvolti nel processo di progettazione con l'obiettivo di stabilire adeguati canali di comunicazione tali che le informazioni risultino chiare, tempestive e continuamente aggiornate per quanto necessario a garantire il corretto svolgimento del servizio.

Il Piano di Progettazione viene aggiornato con il progredire della progettazione.

8.3.3 Elementi in ingresso alla progettazione

MADE IN BIT definisce, documenta e riesamina gli elementi in ingresso alla progettazione e sviluppo dei servizi ICT (sviluppo software, soluzioni sistemistiche, personalizzazioni applicative e attività formative), secondo quanto previsto dalla Procedura PG8.3A *"Gestione della Progettazione"*.

Gli elementi in ingresso alla progettazione comprendono, ove applicabili:

- requisiti funzionali, tecnici e prestazionali definiti dal cliente;
- requisiti contrattuali e capitolati tecnici;
- requisiti cogenti e normativi applicabili (es. normativa su protezione dei dati, sicurezza informatica, requisiti di settore);
- standard tecnici, linee guida interne e best practice di riferimento;
- requisiti relativi all'integrazione con sistemi esistenti o infrastrutture del cliente;
- vincoli tecnologici, architetturali e di sicurezza;
- risorse disponibili (hardware, software, ambienti di sviluppo e test);

- esperienze pregresse, segnalazioni di criticità e lezioni apprese da progetti analoghi;
- requisiti di usabilità, affidabilità, manutenibilità e performance, ove pertinenti;
- per le attività formative: obiettivi didattici, destinatari, modalità di erogazione e prerequisiti.

Gli elementi in ingresso sono riesaminati al fine di verificarne:

- completezza;
- chiarezza;
- coerenza interna;
- assenza di conflitti tra requisiti;
- fattibilità tecnica ed organizzativa.

Eventuali ambiguità o carenze vengono chiarite con il cliente prima dell'avvio delle attività di progettazione.

Le informazioni documentate relative agli elementi in ingresso sono conservate secondo le modalità previste dal Sistema di Gestione.

8.3.4 Controlli sulla progettazione

Verifica della progettazione

Ad ultimazione di ogni fase della progettazione e con le modalità specificate nella Procedura PG8.3A "*Gestione della Progettazione*", sono effettuate delle verifiche per garantire che gli elementi in uscita dalla progettazione siano compatibili con i relativi requisiti in ingresso.

La verifica sarà effettuata dal RAP.

Tale verifica potrà comportare la valutazione di ipotesi alternative secondo le modalità descritte nella Procedura PG8.3A "*Gestione della Progettazione*".

Riesame della progettazione

In corrispondenza di fasi importanti della progettazione, in accordo con quanto pianificato nel PdP e con le modalità specificate nella Procedura PG8.3A "*Gestione della Progettazione*", sono effettuati riesami della progettazione finalizzati al raggiungimento dei seguenti obiettivi:

- valutare la capacità dei risultati della progettazione di ottemperare ai requisiti;
- individuare tutti i problemi e proporre le azioni necessarie;
- valutare gli scostamenti dall'obiettivo ed analizzare anche soluzioni alternative.

A tali riesami partecipano tutti i rappresentanti delle funzioni coinvolte nelle varie fasi di progettazione, comprese quelle interdisciplinari e, se ritenuto opportuno, i rappresentanti della Committenza.

Validazione della progettazione

L'attività di validazione della progettazione e sviluppo si applica a tutte le tipologie di servizi erogati da MADE IN BIT:

- sviluppo software;
- progettazione e gestione di sistemi hardware e infrastrutture IT;
- servizi di assistenza tecnica;
- attività formative.

La validazione deve essere completata prima della messa in esercizio o erogazione del servizio al cliente.

Essa consiste in:

- **Verifica dei requisiti** – confronto tra gli elementi in uscita della progettazione e gli elementi in ingresso, per assicurare che tutti i requisiti siano soddisfatti;
- **Analisi delle esperienze pregresse** – riesame delle difficoltà, criticità e problematiche emerse in servizi o progetti analoghi, per identificare ulteriori requisiti o accorgimenti necessari;
- **Test, simulazioni e collaudi** – esecuzione di prove pratiche sui sistemi, software, infrastrutture o moduli formativi, utilizzando, se necessario, personale interno come tester, al fine di verificare la conformità delle soluzioni progettuali;
- **Conferma dei criteri di accettazione** – verifica che i criteri di accettazione definiti siano adeguati, realistici e misurabili.

Per i progetti software o sistemistici, la validazione può includere: test funzionali, test di integrazione, simulazioni in ambiente di collaudo, verifica di sicurezza, performance e affidabilità.

Per i progetti software, la validazione comprende obbligatoriamente non solo le verifiche di rispondenza funzionale (test di integrazione, simulazioni in ambiente di collaudo), ma anche rigorose attività di verifica della sicurezza dell'architettura e del codice. MADE IN BIT assicura il rispetto dei principi di 'Security by Design' mantenendo una segregazione logica e fisica tra gli ambienti di Sviluppo, Test e Produzione.

Prima di ogni rilascio in ambiente operativo, il codice viene sottoposto a controlli di sicurezza sistematici (es. code review orientate alla rilevazione di vulnerabilità comuni, scansioni di vulnerability assessment automatizzate) in base al modello MD8.5A "*Checklist Secure Coding per Add-on Software Gestionale*" al fine di garantire l'assenza di falle critiche.

Per i servizi formativi, la validazione può includere: simulazioni di sessioni didattiche, verifica dei materiali e delle modalità di erogazione.

Tutte le attività di validazione sono documentate e approvate dal Responsabile delle Attività di Progettazione (RAP), ove opportuno in stretta sinergia con il RSI, e costituiscono base per l'avvio dell'erogazione del servizio o rilascio del prodotto.

8.3.5 Elementi in uscita dalla progettazione

Gli elementi in uscita dalla progettazione e sviluppo dei servizi ICT (sviluppo software, soluzioni sistemistiche, assistenza tecnica e attività formative) sono approvati dal Responsabile delle Attività di Progettazione (RAP) prima del rilascio, secondo le modalità specificate nella Procedura PG8.3A "*Gestione della Progettazione*".

Gli elementi in uscita sono elaborati in modo da:

- soddisfare tutti i requisiti definiti negli elementi in ingresso;
- fornire indicazioni complete e chiare per l'approvvigionamento di risorse, la realizzazione, l'erogazione e il supporto dei servizi;
- includere o richiamare i criteri di accettazione e verifica dei risultati;
- definire responsabilità, modalità operative, strumenti e infrastrutture necessari per l'implementazione;
- garantire la tracciabilità tra requisiti in ingresso, attività svolte e risultati ottenuti;
- per i progetti software e sistemistici: includere documentazione tecnica, specifiche funzionali, diagrammi architetturali, piani di test, criteri di collaudo e requisiti di sicurezza;

- per i servizi formativi: includere programmi didattici, materiali, strumenti di verifica e modalità di erogazione.

Gli output della progettazione costituiscono la base per l'esecuzione controllata delle attività, la verifica della conformità dei servizi erogati e la misurazione della soddisfazione del cliente.

Tutte le informazioni documentate relative agli elementi in uscita sono conservate e gestite secondo le procedure previste dal Sistema di Gestione.

8.3.6 Modifiche della progettazione

MADE IN BIT gestisce le modifiche della progettazione in modo da garantire che tutte le modifiche della progettazione siano riesaminate (con la valutazione degli effetti di tali modifiche) verificate ed approvate prima della loro attuazione, secondo i canoni e gli standard previsti per la progettazione originaria.

8.4 Controllo qualità dei prodotti e servizi forniti all'esterno

8.4.1 Generalità

Tutti i prodotti e servizi vengono controllati prima di essere forniti o erogati ai clienti.

Qualifica dei fornitori

MADE IN BIT effettua, in accordo con la Procedura PG8.4B "*Valutazione e qualifica dei fornitori e consulenti*", una qualifica dei fornitori di beni e servizi che possono influenzare la qualità dei processi e dei servizi erogati.

Gli elementi di valutazione comprendono:

- esperienza del fornitore in servizi o prodotti analoghi;
- confronto delle prestazioni rispetto alla concorrenza in termini di qualità, prezzo, tempi di consegna/esecuzione e capacità di risolvere eventuali problemi;
- verifica di referenze, certificazioni e conformità normativa applicabile;
- capacità tecnica e logistica, infrastrutture disponibili e localizzazione;
- requisiti relativi alla sicurezza nella gestione delle informazioni e rispetto della privacy;
- disponibilità del fornitore a collaborare per la gestione di rischi, modifiche o criticità.

Note sui fornitori qualificati

I fornitori qualificati sono inseriti nell'elenco dei Fornitori Qualificati di MADE IN BIT, da cui si attinge per l'approvvigionamento.

L'esclusione di un fornitore comporta la sospensione di ogni rapporto fino a quando non sarà nuovamente qualificato. Per poter essere riutilizzato, il fornitore deve dimostrare di aver adottato Azioni Correttive efficaci rispetto alle carenze riscontrate.

Monitoraggio e riesame

MADE IN BIT monitora periodicamente le prestazioni dei fornitori e consulenti qualificati, verificando:

- rispetto dei requisiti contrattuali;
- qualità dei beni e servizi forniti;
- puntualità delle consegne;
- efficacia delle Azioni Correttive implementate;
- eventuali cambiamenti di processo o di organizzazione del fornitore che possano influire sui servizi erogati.

I risultati del monitoraggio sono documentati e utilizzati per aggiornare la qualifica e la lista dei fornitori.

8.4.2 Tenuta sotto controllo delle attività di erogazione del servizio

Tutte le attività operative relative ai servizi erogati da MADE IN BIT – inclusi sviluppo software, progettazione e gestione di sistemi hardware, assistenza tecnica, attività formative e attività amministrative – sono gestite in conformità alla Procedura PG8.4A "*Gestione della Commessa*".

L'esecuzione dei servizi è affidata al personale preposto, che opera secondo le indicazioni e le responsabilità definite dal REC.

Il REC assicura che le attività siano svolte in condizioni controllate, conformemente alle procedure e istruzioni documentate, e in luoghi idonei alle specifiche attività, sia che vengano eseguite da personale interno sia da fornitori o consulenti esterni.

Le attività di controllo comprendono:

- verifica della conformità dei processi agli elementi di progettazione e agli standard di qualità definiti;
- monitoraggio delle tempistiche, dei progressi e dei risultati intermedi e finali;
- controllo dei requisiti normativi, contrattuali e interni applicabili;
- gestione delle Non Conformità e implementazione di Azioni Correttive;
- registrazione delle informazioni documentate a supporto della tracciabilità e della qualità del servizio.

Tutte le verifiche e i controlli vengono documentati e archiviati secondo quanto previsto dal Sistema di Gestione, a garanzia della consistenza, affidabilità e conformità dei servizi erogati e dei prodotti forniti.

8.5 Controlli sul Sistema di Gestione della Sicurezza delle Informazioni

Tutti i controlli proposti nell'Appendice A dalla Norma ISO 27001 sono stati analizzati utilizzando SQuadra con le modalità riportate nell'Appendice ISO 27001 del relativo Manuale d'uso.

Tutti i controlli sono stati considerati nella stesura del presente Manuale. Inoltre:

- Gli elementi rivolti agli utenti sono stati riportati nella IO8.5A "*Policy e Prescrizioni per gli incaricati del trattamento dati*".
- Gli elementi che riguardano gli aspetti tecnologici e specialistici sono stati riportati nella istruzione IO8.5B "*Sicurezza delle informazioni*".
- Gli elementi che possono interessare chi tratta i dati personali per conto del Titolare sono riportati nei contratti stipulati, ai sensi dell'Art. 28 del GDPR, con i Responsabili.

Per gli eventuali elementi di controllo considerati non significativi per l'attuale gestione delle informazioni viene riportata, su SQuadra, la motivazione.

Tutti i controlli, salvo specifica indicazione, vengono applicati a MADE IN BIT nel suo complesso considerando che le minacce sono rivolte a tutta

l'organizzazione, non ad una parte di essa. Le minacce possono sfruttare criticità dei singoli asset, ma le motivazioni dei malintenzionati, la possibilità di fare errori e gli eventi naturali sono comuni a tutta l'organizzazione e non specifici di un singolo asset.

Durante la gestione del Sistema, MADE IN BIT stratifica l'esperienza - tecnica, operativa e gestionale - accumulata durante l'esercizio del SGI stesso che, documentata in modo oggettivo e dettagliato, determina un progressivo affinamento della impostazione e modalità di utilizzo del sistema.

Le modalità di attuazione degli elementi di controllo vengono definite ed aggiornate dal RSI, sulla base dell'esperienza e in base al rapporto costo dell'implementazione / mitigazione del rischio, tenendo conto anche di fattori non esclusivamente monetari, quali la cogenza di disposizioni legislative o la perdita di immagine.

RSI valuta anche lo stato dei controlli utilizzando le apposite funzionalità di SQuadra. Lo stato dei controlli rappresenta un elemento di ingresso per il Riesame della Direzione.

8.6 Continuità operativa

8.6.1 Obiettivi di continuità

MADE IN BIT riconosce che la continuità nell'erogazione dei propri servizi (sviluppo software, assistenza tecnica, formazione) e nella disponibilità delle informazioni costituisce un elemento essenziale per la soddisfazione dei clienti, il rispetto degli obblighi contrattuali e la sostenibilità dell'organizzazione.

La Direzione Aziendale ha pertanto stabilito che i processi critici dell'organizzazione devono essere protetti da interruzioni attraverso la definizione di adeguate misure di prevenzione, risposta e ripristino, proporzionate alla dimensione e alla complessità dell'organizzazione. Le informazioni principali sono riportate nella IO8.6 "Continuità operativa".

8.6.2 Minacce e misure di continuità

MADE IN BIT ha identificato le principali minacce che possono determinare l'interruzione dei servizi o la perdita di dati quali, ad esempio: il guasto dei sistemi informatici (server, storage, apparati di rete), l'attacco informatico (ransomware, intrusione, denial of service), l'indisponibilità prolungata dei locali aziendali (evento naturale, incendio, allagamento), la perdita di personale chiave e l'indisponibilità di fornitori critici.

Per ciascuna minaccia, il RSI ha registrato SQuadra (Minacce), in accordo con la Direzione, le misure di prevenzione e di ripristino adeguate, che comprendono: le procedure di backup dei dati e dei sistemi, con verifica periodica della capacità di ripristino (test di restore); la ridondanza delle infrastrutture critiche, ove economicamente sostenibile; le modalità di lavoro alternative (accesso remoto, utilizzo di postazioni secondarie); le procedure di comunicazione verso i clienti e le parti interessate in caso di interruzione; le procedure di escalation e di attivazione del piano di emergenza. Viene anche registrato il Responsabile, la data dell'ultima verifica e la periodicità con la quale devono essere effettuati i test periodici per verificarne l'efficacia e l'adeguatezza.

Qualora un test dia esito negativo, il RSI definisce le Azioni Correttive necessarie con i relativi tempi e responsabilità.

L'elenco delle minacce è riesaminato almeno annualmente in occasione del Riesame della Direzione e ogni volta che si verifichino modifiche significative nelle infrastrutture, nei servizi erogati, nei requisiti contrattuali o nel contesto delle minacce stesse.

8.6.3 Impatto sulla continuità operativa per i vari Trattamenti

La Direzione Aziendale definisce con il supporto del RSI, per ogni trattamento, nel Registro dei Trattamenti (che MADE IN BIT ha deciso di utilizzare per documentare tutti i trattamenti effettuati e non solo quelli oggetto del GDPR), i parametri di continuità, gli impatti e la criticità con i relativi tempi di intervento necessari (vedi l'Appendice ISO 27001 – Impatto sulla continuità del Manuale di SQuadra).

Tali i dati sono riportati e riesaminati almeno annualmente.

8.7 Servizi cloud

8.7.1 Specificità dei servizi cloud

MADE IN BIT utilizza provider globali (come AWS, Azure o Google Cloud) che assicurano elevate garanzia di sicurezza "del cloud" ma spetta a MADE IN BIT assicurare la sicurezza "nel cloud" come indicato nella procedura PG8.5A "*Servizi in cloud*".

MADE IN BIT utilizza SQuadra per la gestione dei servizi cloud (vedi Manuale d'uso di SQuadra Appendice ISO 27017) per:

- effettuare la valutazione del servizio prima di offrirlo ai propri clienti;
- effettuare revisioni periodiche per valutare l'adeguatezza del servizio cloud anche rispetto all'evoluzione della tecnologia;
- per definire i livelli di SLA offerti ai propri clienti (comunque inferiori a quelli garantiti dal fornitore);
- definire chi può accedere al servizio con le relative credenziali;
- registrare i clienti del servizio (indicando, in particolare, la mail ed il livello di SLA offerto);
- predisporre mail standard per invii ai clienti:
  - delle informazioni essenziali relative alla valutazione iniziale;
  - delle informazioni essenziali relative alla rivalutazione periodica;
  - di specifiche informazioni (ed esempio in caso di problematiche legate al servizio).

RSI potrà inviare mail ai clienti anche in condizioni di emergenza grazie al servizio offerto da SQuadra.

La gestione delle credenziali tramite SQuadra è necessaria in quanto ogni persona deve avere accesso unicamente ai servizi necessari quindi è necessario creare tante credenziali quanti sono gli utenti anche al fine di poter analizzare i LOG.

Relativamente alle password:

- è necessario non utilizzare la stessa password per più utenti per evitare che una eventuale compromissione si estenda ad altri servizi;
- le password devono essere adeguatamente complesse per renderne difficile l'aggiramento;
- le non deve essere necessario memorizzarle scrivendole in chiaro;

La possibilità, per ogni utente abilitato di visualizzare tramite l'applicazione di SQuadra tutte le proprie credenziali di accesso risolve questa problematica.

Quando i Clienti operano con Mexal su server dedicati gli unici dati disponibili sono quelli ai quali si potrebbe comunque accedere dal programma e per i quali MADE IN BIT è già nominata responsabile ai sensi dell'Art. 28 del GDPR.

Quando invece i Clienti utilizzano il server sul quale si appoggia MEXAL anche per altri servizi chi ha accesso come amministratore (necessario per la gestione di MAXAL) può accedere anche ad altre informazioni e quindi è necessario tenere traccia nominativa dei log.

9 VALUTAZIONE DELLE PRESTAZIONI

9.1 Monitoraggio e misurazione

9.1.1 Soddisfazione del cliente

MADE IN BIT tiene sotto controllo la percezione che il cliente e gli utenti hanno sulla soddisfazione dei requisiti raccogliendo le informazioni di ritorno da chi eroga il servizio o ha contatti con i clienti / utenti. In particolare vengono raccolte informazioni relative a:

- **Sviluppo personalizzazioni software**: Capacità di comprendere le sue esigenze e tradurle in soluzioni funzionanti. Gli elementi chiave sono: la chiarezza e completezza dell'analisi dei requisiti iniziali (il cliente si è sentito ascoltato e ha capito cosa sarebbe stato realizzato?), la corrispondenza tra quanto concordato e quanto effettivamente rilasciato, la qualità tecnica del software (stabilità, assenza di bug, prestazioni), l'usabilità della soluzione per gli utenti finali, il rispetto dei tempi di consegna concordati, la gestione delle varianti in corso d'opera (quanto è stata flessibile e trasparente MADE IN BIT nel gestire le modifiche richieste dal cliente durante lo sviluppo), la qualità della documentazione rilasciata (manuale utente, note di rilascio), l'efficacia della fase di collaudo e avviamento (il passaggio in produzione è stato gestito bene?), la reattività nel correggere i difetti segnalati dopo il rilascio e se il cliente ritiene che il costo sostenuto sia proporzionato al risultato ottenuto.
- **Attività sistemistica**: Disponibilità, rapidità e affidabilità. Gli elementi da analizzare sono: il rispetto dei tempi di intervento concordati (SLA), la rapidità nella presa in carico delle segnalazioni (quanto tempo passa tra l'apertura del ticket e il primo contatto?), l'efficacia risolutiva al primo intervento (il problema è stato risolto definitivamente o il cliente ha dovuto richiamare?), la competenza tecnica percepita del personale (il tecnico sapeva cosa fare?), la chiarezza nella comunicazione durante l'intervento (il cliente è stato informato su cosa stava succedendo, sui tempi stimati, sulle cause del problema?), la proattività (MADE IN BIT segnala criticità o propone miglioramenti prima che il cliente li chieda?), la disponibilità e cortesia del personale, la qualità dell'assistenza remota rispetto a quella on-site, e l'affidabilità complessiva dei sistemi gestiti nel tempo (il cliente percepisce un miglioramento della stabilità della propria infrastruttura?).
- **Formazione sugli applicativi:** Esperienza didattica e utilità percepita. Gli elementi da valutare sono: la pertinenza dei contenuti rispetto alle reali esigenze operative dei partecipanti (il corso ha trattato argomenti utili per il mio lavoro quotidiano?), il livello di approfondimento (né troppo elementare né troppo avanzato per il pubblico), la competenza e la capacità comunicativa del docente, la chiarezza delle spiegazioni e degli esempi utilizzati, la qualità e completezza dei materiali didattici forniti (sono utilizzabili anche dopo il corso come riferimento?), l'organizzazione logistica (orari, durata, comfort dell'aula o qualità della piattaforma online), l'equilibrio tra teoria e pratica (c'è stata possibilità di esercitarsi?), la capacità del docente di adattare il programma alle domande e ai bisogni emersi in aula, e — aspetto fondamentale — il trasferimento effettivo delle competenze: dopo il corso, il partecipante si sente in grado di applicare quanto appreso?
- **Trasversalmente**: Qualità della comunicazione complessiva con MADE IN BIT (facilità di contatto, chiarezza nelle risposte, tempestività), la disponibilità a consigliare MADE IN BIT ad altri, l'intenzione di riutilizzare i servizi in futuro e la percezione complessiva del rapporto qualità-prezzo.

I dati raccolti servono come elementi di ingresso per il Riesame della Direzione.

Reclami

Una fonte di informazioni relative alla soddisfazione dei clienti / utenti sono i reclami.

Le segnalazioni, pervenute dai clienti / utenti durante l'esecuzione dei servizi, sono gestite direttamente dal referente per la Commessa; per quelle pervenute dopo l'esecuzione del servizio, vengono invece consegnate al RSG che individua il responsabile per la gestione del reclamo.

Il RSG, in collaborazione col responsabile incaricato, verifica le condizioni contrattuali in essere con il cliente per la valutazione della fondatezza del reclamo (identificazione del requisito contrattuale eventualmente non rispettato e delle funzioni aziendali e non, coinvolte, individuazione ed analisi delle cause che hanno generato il reclamo del cliente / utente).

Nel caso in cui si possa già escludere una responsabilità diretta di MADE IN BIT il RSG comunica il risultato negativo della valutazione aziendale con le opportune giustificazioni al cliente / utente.

In caso di fondatezza del reclamo, o di non manifesta infondatezza, il RSG si riserva di approfondire le cause e provvede con sollecitudine ad informare il cliente / utente in relazione all'analisi in corso ed ai tempi necessari per le verifiche. Se viene appurata la responsabilità di MADE IN BIT il reclamo viene accettato e viene aperta una Non Conformità.

Il RSG concorda con il cliente / utente il programma di intervento (modalità e tempi) mentre un'ulteriore comunicazione al cliente / utente sarà effettuata nel momento in cui gli interventi relativi al reclamo sono conclusi. Il Responsabile del trattamento, coordina l'intervento coinvolgendo le funzioni necessarie.

In caso di evidente responsabilità di un Consulente o di un Fornitore, il RSG, valuta le azioni inerenti la qualifica dello stesso.

L'analisi statistica dei reclami effettuata dal RSG permette di elaborare i dati raccolti che saranno oggetto di riflessione e valutazione durante il Riesame della Direzione e può dare origine ad Azioni Correttive. Questa analisi viene effettuata su tutti i reclami, siano questi stati accettati o no, i reclami non accettati possono, infatti, se ripetitivi, essere comunque indicativi di deficienze interne al sistema.

9.2 Audit interni

Generalità

Gli Audit rappresentano uno strumento fondamentale per la corretta attuazione ed il continuo miglioramento del Sistema di Gestione. Essi

costituiscono il mezzo per l'esame sistematico delle attività aziendali che hanno influenza sui servizi erogati. La loro esecuzione viene pianificata nel corso dei Riesami della Direzione al fine di analizzare periodicamente tutti i processi aziendali tenendo presenti i risultati delle precedenti Audit.

Gli Audit dovranno analizzare la conformità di tutti gli aspetti del Sistema di Gestione ma in particolare dovranno concentrarsi su aspetti specifici indicati sempre dalla Direzione nel corso dei Riesami.

MADE IN BIT conduce normalmente l'attività di audit del Sistema di Gestione su tutte le attività che hanno influenza sui servizi erogati, con l'intento di:

- verificare la corretta applicazione di quanto pianificato nel Manuale di Gestione e nelle Procedure;
- valutare l'efficacia del Sistema di Gestione nel conseguire gli obiettivi fissati;
- individuare le carenze del Sistema di Gestione;
- verificare il raggiungimento degli obiettivi definiti dal Riesame della Direzione;
- verificare il rispetto delle prescrizioni legali e delle altre prescrizioni contrattuali;
- verificare le richieste espresse dai responsabili di funzione relativamente ad attività e/o personale di loro competenza.

Responsabilità e competenze per gli Audit

Gli Audit sono effettuati da personale, interno o esterno, adeguatamente addestrato e diverso da quello che ha effettuato le attività oggetto di verifica, secondo le modalità definite nella Procedura PG9.2A *"Audit"*. Per ogni audit viene individuato un responsabile che deve conoscere le problematiche connesse all'oggetto, deve avere capacità e competenze tecniche nelle attività sottoposte a verifica, deve essere formato ed avere specifica esperienza relativa alla conduzione ed all'esecuzione degli audit, deve avere l'autorità di prendere le decisioni finali.

Attuazione degli Audit

Il RSG, in accordo con le indicazioni contenute nella PG9.2A "Audit", deve assicurare:

- La disponibilità della documentazione di riferimento.
- L'eventuale preparazione di liste di riscontro.
- L'assegnazione dell'incarico a personale competente come sopra indicato.
- La notificazione delle date e dei tempi per la verifica al Responsabile dell'area sottoposta a verifica.

Ogni verifica prevederà, anche in forma molto sintetica:

- la redazione del piano della verifica (se diverso da quello attuato nella visita precedente o se è modificato il personale sottoposto a verifica);
- la registrazione nei documenti predisposti delle evidenze e delle eventuali Non Conformità;
- la redazione del rapporto nel quale verranno riportati, sempre in maniera molto sintetica, osservazioni sulle Non Conformità, giudizio sulla conformità e capacità del sistema a conseguire gli obiettivi;
- un giudizio sulla conoscenza del Sistema Gestione.

Il Rapporto, compilato a conclusione dell'attività a cura del gruppo di verifica, viene illustrato ai Responsabili delle funzioni coinvolte.

Il rapporto può contenere la programmazione di eventuali ulteriori visite ispettive per verificare che eventuali Non Conformità emerse siano state risolte.

La valutazione dei risultati degli Audit e l'autorizzazione alle eventuali Azioni Correttive è di competenza del RSG che, in tal caso, deve provvedere a coinvolgere il personale dell'area verificata per la pianificazione e l'attuazione delle Azioni Correttive.

L'attuazione delle Azioni Correttive richieste viene verificata, per valutare gli effetti da queste ottenuti e decidere di conseguenza se applicarne altre.

L'analisi della documentazione di registrazione degli Audit costituisce elemento fondamentale in fase di Riesame della Direzione.

9.3 Riesame della Direzione

9.3.1 Generalità

Il Sistema di Gestione adottato da MADE IN BIT è sottoposto, con cadenza annuale, al riesame complessivo, eseguito nel corso della riunione di Riesame della Direzione alla quale partecipano la Direzione Aziendale, il Responsabile Sistema di Gestione, il Responsabile del Sistema Informatico ed altri Responsabili di volta in volta individuati in relazione ad eventuali specificità.

Il Riesame della Direzione si pone l'obiettivo di analizzare lo stato di avanzamento del programma di implementazione del sistema stesso e di valutare l'idoneità, l'adeguatezza nel tempo e l'efficacia del Sistema di Gestione nel conseguimento degli obiettivi espressi e nel rispetto delle norme adottate.

Tale riesame prevede:

- l'analisi dei documenti predisposti per il Riesame;
- l'analisi delle informazioni documentate richieste dalle Norme di interesse;
- l'analisi delle informazioni gestite con strumenti software;
- il Riesame vero e proprio nel quale, per ogni "sezione", vengono analizzati i seguenti elementi:
  - Cosa era stato definito nel Riesame precedente: Opportunità di miglioramento ed esigenze di modifica del sistema e Responsabilità, Risorse e Tempi previsti per le Azioni.
  - Efficacia delle azioni intraprese.
  - Opportunità di Miglioramento ed esigenze di modifica del Sistema.
  - Responsabile, Risorse e Tempi previsti per le Azioni definite.
- la verbalizzazione dei risultati e la diffusione ai partecipanti e agli interessati.

9.3.2 Elementi in ingresso per il Riesame

Il Riesame della Direzione è effettuato sulla base di informazioni di partenza che comprendono:

- analisi dello stato di avanzamento del programma di implementazione del Sistema di Gestione e valutazione di efficacia, idoneità ed adeguatezza del sistema stesso;
- adeguatezza dell'analisi del contesto, delle opportunità/rischi per fattori interni e esterni e degli obiettivi del Sistema di Gestione;
- analisi dei risultati delle azioni intraprese a seguito dei precedenti riesami ed il livello di conseguimento degli obiettivi fissati da MADE IN BIT nel periodo precedente attraverso la valutazione dei rispettivi parametri;
- analisi degli audit interni e/o di parte terza;
- stato dei controlli sulla sicurezza delle informazioni;
- analisi delle minacce e degli incidenti;
- analisi dei reclami e delle informazioni di ritorno dal cliente e degli utenti;

- esame delle Non Conformità rilevate e l'andamento delle stesse nel tempo, nonché delle Azioni Correttive definite di volta in volta e la loro efficacia per la risoluzione delle problematiche eventualmente riscontrate;
- andamento dei programmi di addestramento e formazione, l'analisi critica della disponibilità di risorse e la rivalutazione delle risorse umane aziendali in ottica del Sistema di Gestione;
- analisi critica della disponibilità di apparecchiature e locali;
- verifica della corretta individuazione degli indicatori per i vari processi;
- verifica delle prestazioni dei processi;
- esame della qualifica dei Fornitori e dei Consulenti in base alla valutazione dei risultati relativi alle prestazioni dei Fornitori;
- valutazione sugli oneri imprevisti;
- analisi delle richieste di aggiornamento o modifica del Sistema di Gestione pianificate in relazione a variazioni organizzative e/o esigenze interne / esterne che potrebbero avere effetti sul sistema stesso;
- necessità di aggiornamento della Politica;
- valutazione delle opportunità e delle raccomandazioni per il miglioramento;
- eventuali contributi forniti dal personale e/o dai Consulenti.

Il Responsabile del Sistema di Gestione, è responsabile della preparazione preventiva della documentazione necessaria per supportare le attività di riesame.

9.3.3 Elementi in uscita dal Riesame

La Direzione Aziendale analizza gli elementi in ingresso presentati dal RSG ed utilizza l'attività di riesame come strumento per evidenziare opportunità di miglioramento indicando e pianificando futuri obiettivi, valutando anche l'adeguatezza e l'idoneità della Politica, la corretta individuazione e valutazione degli indicatori, l'idoneità della struttura e delle risorse di MADE IN BIT.

I risultati e le conclusioni emerse sono documentati dal RSG su SQuadra riportando raccomandazioni e/o richieste di azioni derivanti dal Riesame della Direzione e relative ai seguenti aspetti:

- miglioramento dell'efficacia del Sistema di Gestione e dei suoi processi;
- miglioramento dei servizi connessi ai requisiti del cliente;
- esigenza di risorse e formazione delle risorse umane;
- modifiche a procedure e controlli del Sistema necessarie per rispondere ad eventi interni o esterni.

Per ogni obiettivo dovranno essere indicati:

- Responsabile per il raggiungimento dell'obiettivo;
- Risorse necessarie;
- Tempi previsti (con eventuale pianificazione di step intermedi).

Estratti del riesame possono essere distribuiti alle funzioni che hanno partecipato alla riunione e a quelle interessate alle decisioni prese.

10 MIGLIORAMENTO

10.1 Gestione delle Non Conformità e Azioni Correttive

10.1.1 Non conformità

Per Non Conformità si intende il mancato soddisfacimento di un requisito, quale:

- Normativa di riferimento.
- Accordi volontari, impegni sottoscritti e contratti.
- Norme, procedure ed istruzioni e qualsiasi altra responsabilità volontaria prevista dal Sistema di Gestione.
- Limiti di legge o limiti interni.
- Servizi non conformi ai relativi requisiti.

Classificazione delle Non Conformità

Le Non Conformità sono così suddivise:

- NC di Sistema: sono le NC rilevate sul Sistema di Gestione che si riferiscono a difformità rispetto a quanto riportato nelle Norme per le quali è certificato o rispetto alle prescrizioni contrattuali.
- NC Documentali: sono quelle relative a carenze nella definizione dei requisiti rispetto ai quali misurare la conformità di uno specifico servizio e carenze nella registrazione del livello qualitativo raggiunto dal servizio che lasciano indeterminata la conformità del servizio.
- NC di Processo: sono relative ad inadempienze nell'applicazione delle regole del Sistema di Gestione di MADE IN BIT che possono indurre incertezza circa la conformità del servizio.

Attività di sorveglianza

La sorveglianza delle attività aziendali ha per oggetto tutti i processi operativi e di supporto di MADE IN BIT, inclusi sviluppo software, progettazione e gestione di sistemi hardware e infrastrutture IT, servizi di assistenza tecnica, attività formative e attività amministrative.

I risultati della sorveglianza vengono confrontati con gli standard e gli indicatori di qualità definiti, in coerenza con la Politica Aziendale e gli Obiettivi aziendali.

La pianificazione del controllo tiene conto della tipologia e dell'impatto dei processi sul servizio erogato e sull'efficacia del Sistema di Gestione. Il monitoraggio viene effettuato secondo frequenze stabilite da requisiti normativi, contrattuali o di sistema, con modalità adeguate al tipo di processo.

Gli strumenti e le modalità di monitoraggio includono, a titolo esemplificativo:

- **Analisi dei dati di performance dei servizi software** (bug, tempi di sviluppo, completamento delle milestone, test superati);
- **Monitoraggio dei sistemi hardware e infrastrutture IT** (disponibilità, sicurezza, integrità dei dati, manutenzione e aggiornamenti);
- **Verifica dei servizi di assistenza tecnica** (SLA rispettati, tempi di risposta e risoluzione, feedback dei clienti);
- **Controllo dei processi amministrativi** (accuratezza documentale, rispetto delle procedure, tempi di esecuzione);
- Analisi dei questionari e feedback relativi ai servizi formativi;
- **Analisi delle Non Conformità** rilevate nei vari processi;
- **Ispezioni periodiche** relative all'applicazione delle Procedure e Istruzioni.

Le attività di sorveglianza e monitoraggio sono pianificate, regolate e gestite dal Responsabile del Sistema di Gestione (RSG).

Il personale incaricato è responsabile dell'esecuzione delle attività di monitoraggio secondo quanto definito nel Sistema di Gestione. I risultati ottenuti sono documentati e utilizzati per:

- valutare l'efficacia dei processi;
- rilevare opportunità di miglioramento;
- supportare decisioni correttive;
- garantire la conformità ai requisiti contrattuali, normativi e interni.

Gestione delle NC

Chiunque rilevi una Non Conformità lo comunica al RSG (verbalmente o tramite e-mail), che provvederà a registrarla nel "*Registro delle Non Conformità"* come indicato nella Procedura PG10.1A *"Gestione delle Non Conformità"*.

Ove necessario le azioni da intraprendere ed i tempi di trattamento sono concordate con il REC.

In seguito alla decisione relativa al trattamento ritenuto più opportuno per la Non Conformità rilevata, il responsabile del trattamento provvede a svolgere le seguenti attività:

- applicare le azioni relative al trattamento della Non Conformità;
- comunicare la corretta attuazione della risoluzione della Non Conformità al responsabile della registrazione;
- richiedere la verifica del corretto trattamento al responsabile della verifica.

Ai fornitori / Consulenti può essere contrattualmente richiesto il loro impegno per gestire le Non Conformità e rispettare quanto previsto da MADE IN BIT nel presente Manuale di Gestione.

Analisi dei dati

In preparazione del Riesame della Direzione il RSG raccoglie ed analizza i dati appropriati per dimostrare l'adeguatezza e l'efficacia del Sistema di Gestione e per valutare dove possa essere realizzato il miglioramento continuo dell'efficacia del sistema stesso.

10.1.2 Azioni Correttive

Le Azioni Correttive sono volte all'eliminazione delle cause che hanno determinato Non Conformità con lo scopo di prevenire il loro ripetersi. Le Azioni Correttive devono intendersi come la ricerca e l'eliminazione delle cause dei difetti stessi a prescindere dal trattamento della singola Non Conformità.

MADE IN BIT, al fine di migliorare continuamente il proprio Sistema di Gestione, ha assegnato al RSG la responsabilità di raccogliere tutte le informazioni circa la possibilità di attuare Azioni Correttive. Tutto il personale è invitato a segnalare al proprio responsabile ogni suggerimento; sarà il responsabile a valutare l'opportunità di proporre l'Azione Correttiva al RSG.

Il RSG, inoltre, periodicamente e comunque in preparazione dei Riesami della Direzione provvede ad effettuare l'analisi statistica di tutte le Non Conformità (comprese quelle originate dai Reclami dei clienti) per individuare eventuali ripetitività indotte da carenze o mal funzionamenti del Sistema di Gestione, l'analisi dettagliata delle Non Conformità episodiche ma rilevanti, l'analisi di tutti i nuovi verbali di audit interni o esterni e proposte di miglioramento da essi scaturiti, l'esame delle registrazioni, l'analisi delle misurazioni della soddisfazione del cliente, ecc.

Le Azioni Correttive sono gestite dal RSG in accordo con le prescrizioni della PG10.1B "*Azioni Correttive*".

10.1.3 Gestione degli Incidenti di Sicurezza delle Informazioni e Data Breach

A differenza delle Non Conformità qualitative o documentali, gli eventi e le anomalie che minacciano la riservatezza, l'integrità o la disponibilità delle informazioni richiedono un processo di escalation dedicato, rapido e rigidamente strutturato. Chiunque rilevi o abbia il fondato sospetto di un incidente di sicurezza (es. infezione da malware, l'accesso non autorizzato a sistemi o dati, la perdita o il furto di dispositivi contenenti dati aziendali o dei clienti, l'infezione da malware o ransomware, la violazione di dati personali - data breach, la compromissione di credenziali di accesso, l'indisponibilità prolungata di servizi informatici, l'alterazione non autorizzata di dati, la divulgazione non autorizzata di informazioni riservate e la violazione delle politiche di sicurezza da parte del personale.) deve darne immediata notifica al Responsabile del Sistema Informatico (RSI) e agli Amministratori di Sistema, bypassando le normali procedure di registrazione delle Non Conformità al fine di azzerare i tempi di latenza.

Processo di gestione degli incidenti

MADE IN BIT per la gestione degli incidenti di sicurezza delle informazioni, utilizza SQuadra (software fornito in modalità SaaS da terza parte che si appoggia su Cloud non utilizzati da MADE IN BIT e quindi tendenzialmente non compromesso in caso di incidente a MADE IN BIT).

Le modalità di gestione sono descritte nel Manuale d'uso di SQuadra nell'Appendice ISO 27001 / Gestione Incidenti.

La registrazione degli incidenti è articolata nelle seguenti fasi:

a) Rilevazione e segnalazione. Tutto il personale è tenuto a segnalare tempestivamente al RSI qualsiasi evento sospetto o anomalia che possa configurare un incidente di sicurezza. La segnalazione può avvenire verbalmente, tramite e-mail o attraverso gli strumenti di comunicazione interna. Il RSI provvede alla registrazione dell'evento nel Registro degli incidenti di sicurezza. Nei locali è esposto il QR-CODE con il quale chiunque può segnalare un evento sospetto indicando la minaccia che si è verificata e una breve nota. In automatico verrà aperto un nuovo incidente su SQuadra e verrà inviata una mail al Responsabile della prima azione prevista dal piano di continuità. Il RSI ha accesso ad un link nel quale può vedere gli incidenti ancora aperti e avere l'elenco delle attività previste dal piano per la continuità con i contatti per i vari responsabili delle azioni.

b) Valutazione e classificazione. Il RSI, eventualmente con il supporto dell'amministratore di sistema e del RSG, valuta l'evento, ne verifica la natura e la gravità e lo classifica. La classificazione relativamente alla Sicurezza delle Informazioni prevede tre livelli: minore (impatto limitato, gestibile con interventi ordinari), significativo (impatto rilevante su operatività o su dati sensibili, che richiede un intervento coordinato) e grave (impatto critico che richiede escalation immediata alla Direzione e, se del caso, notifica alle autorità competenti). Vengono anche valutati i rischi privacy (da "Non significativo" a "Altissimo" – con necessità di comunicazione sia al Garante che agli interessati). Per gli incidenti significativi e gravi, il RSI informa immediatamente la Direzione Aziendale.

c) Contenimento e risposta. In funzione della gravità, il RSI coordina le azioni di contenimento necessarie a limitare l'estensione dell'incidente e a prevenire ulteriori danni. Le azioni possono includere: l'isolamento dei sistemi compromessi, la revoca o la modifica delle credenziali coinvolte, il blocco degli accessi non autorizzati, l'attivazione delle procedure di backup e ripristino e qualsiasi altra misura tecnica od organizzativa proporzionata alla situazione.

d) Indagine e analisi delle cause. Per gli incidenti significativi e gravi, il RSI conduce un'indagine per individuare le cause dell'incidente, le vulnerabilità sfruttate, l'estensione effettiva del danno e le eventuali responsabilità. L'indagine è documentata nel Registro degli incidenti.

e) Ripristino. Il RSI coordina le attività di ripristino delle condizioni operative normali, verificando che le cause dell'incidente siano state eliminate e che i controlli siano stati adeguati a prevenire il ripetersi dell'evento.

f) Comunicazione e notifica. Per gli incidenti che comportano una violazione di dati personali ai sensi del GDPR, il PdI, in qualità di Titolare del trattamento, valuta la necessità di notifica all'Autorità Garante (entro 72 ore dalla conoscenza della violazione) e di comunicazione agli interessati, avvalendosi del supporto del RSI e, se del caso, del consulente legale. Per gli incidenti che possono avere impatto sui servizi erogati ai clienti, il RSI coordina la comunicazione verso i clienti interessati. Viene valutata anche la necessità di conformarsi agli obblighi di comunicazione previsti dall'attuale normativa in materia di cybersicurezza nazionale (es. Legge 90/2024).

g) Analisi post-incidente e Azioni Correttive. A chiusura dell'incidente, il RSI predispone un rapporto di analisi post-incidente compilando i dati significativi su SQuadra ed in particolare i dati relativi: alla rilevazione dell'evento (date di rilevazione, natura dell'evento, fonte della segnalazione, conseguenze, ecc.), alla valutazione (Numero di persone/registrazioni interessate e categorie relative, informazioni sulle comunicazioni obbligatorie, minaccia all'origine dell'evento, ecc.), alle misure adottate (misure e date di effettuazione e chiusura, le Azioni Correttive proposte e le lezioni apprese).

Il rapporto è sottoposto alla Direzione e, ove opportuno, genera un'azione correttiva per rafforzare le difese sistemiche e prevenire il ripetersi di situazioni analoghe. L'analisi degli incidenti significativi costituisce elemento in ingresso per il Riesame della Direzione.

Responsabilità

Il RSI è responsabile del coordinamento della gestione degli incidenti, della tenuta del Registro degli incidenti di sicurezza e della predisposizione dei rapporti di analisi. Il PdI è responsabile delle decisioni relative alla notifica delle violazioni di dati personali. La Direzione Aziendale è responsabile dell'approvazione delle Azioni Correttive derivanti dagli incidenti gravi e della valutazione complessiva dell'efficacia del processo di gestione degli incidenti in sede di Riesame della Direzione. Tutto il personale è responsabile della tempestiva segnalazione degli eventi sospetti.

10.2 Miglioramento continuo

L'analisi del raggiungimento degli obiettivi, gli indici di monitoraggio ed i dati ottenuti anche per mezzo di tecniche statistiche sui servizi e sui processi ed i verbali degli Audit, sono la base per la formulazione della necessità di azioni volte all'eliminazione delle cause di Non Conformità potenziali con l'obiettivo di evitare che queste si verifichino.

Durante il Riesame della Direzione vengono analizzati gli indicatori al fine di individuare interventi possibili atti a prevenire potenziali cause di Non Conformità e/o l'avvio di processi di miglioramento in termini aziendali.