Privacy Policy

Meranarena GmbH | Srl
Rechtssitz: Gampenstraße 74 · Verwaltungssitz und Direktion: Piavestraße 46 · I-39012 Meran (BZ)
Sede legale: Via Palade, 74 · Sede amministrativa e direzione: Via Piave, 46 · I-39012 Merano (BZ)
T +39 0473 236 982 · info@meranarena.it · www.meranarena.it · MwSt.-Nr. & St.-Nr. | Part. IVA e cod. fisc.: IT01692600214

Iter di emissione				
Versione	**Autore**	**Data**	**Revisione**	**Firma**

Approvazioni			
Nome		**Data approvazione**	**Firma**

Sommario

1. Adempimenti in materia di dati personali

1.1. Premessa

La Società è da sempre particolarmente sensibile alla riservatezza ed alla sicurezza dei dati personali, propri e di terze parti. Per tale motivo ha uniformato il proprio modo di trattare i dati personali ai dettati del GDPR – Regolamento UE 2016/679, prevedendo, altresì, misure di sicurezza adeguate a quanto richiesto dalla norma.

La riservatezza delle persone fisiche attraverso la corretta acquisizione, gestione e circolazione dei dati personali e mediante l'adozione di idonee misure di sicurezza per la loro protezione è tutelata dal citato Regolamento, nonché, in quanto non incompatibili, dalle singole normative nazionali e dai provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali.

Il Regolamento afferma importanti principi quali il diritto alla protezione dei dati personali e quello della necessità del trattamento (*need to know*) e, al contempo, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale, al diritto alla protezione dei dati personali, alla portabilità dei dati, sino al diritto all'oblio.

I principi fondamentali introdotti dal Regolamento e non presenti nel precedente "Codice Privacy" (dec. legisl. 196/03), possono essere riassunti come segue:

- Privacy by design e by default;
- Rafforzamento del principio del "need to know";
- Introduzione di adempimenti formali come l'adozione del Registro dei Trattamenti e redazione del PIA – Privacy Impact Assessment;
- Nuovi diritti degli interessati;
- Obbligo di gestione dei Data Breaches;
- Determinazione delle misure di sicurezza secondo un approccio "risk based";
- Introduzione della figura del DPO – Data Protection Officer (Responsabile della Protezione dei Dati Personali);
- Ridefinizione della figura del Responsabile del Trattamento dei Dati Personali e del Contitolare del trattamento;

- Forte inasprimento delle sanzioni che, in caso di inadempimento, possono arrivare sino a € 20 milioni o al 4% del fatturato annuo worldwide.

Il Regolamento specifica, altresì, che il trattamento dei dati è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il suo esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Il Regolamento si compone di 173 "consideranda" e di 99 articoli.

Il presente documento contiene la Politica definita dalla Società (nel seguito la "Società") per adempiere alle prescrizioni del Regolamento. Esso contiene le indicazioni per l'effettuazione degli adempimenti necessari verso l'Autorità Garante (quali la notificazione dei trattamenti e dei Data Breaches), verso i soggetti interessati (quali l'informativa, la raccolta del consenso al trattamento, laddove necessario, il riscontro delle richieste di esercizio del diritto d'accesso) e verso le strutture operative (quali le nomine e le istruzioni agli Incaricati ed agli eventuali Responsabili del trattamento ed al Responsabile per la Protezione dei Dati Personali).

1.2. Definizioni

Preliminarmente, al fine di una corretta interpretazione degli adempimenti che saranno menzionati nel seguito, si fornisce un'esplicitazione dei termini utilizzati nel Regolamento.

In particolare si intende per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento a un dato come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) Privacy by Design e Privacy by Default: l'art. 25 del GDPR prevede in capo al Titolare del Trattamento due modalità di gestione del Modello Privacy interno della propria azienda. La prima, prevista al comma 1 dell'art. 25 è definita privacy by Design poiché il compito del Titolare sarà quello di adottare e attuare misure tecniche organizzative che tutelano i principi di protezione dei dati sin dal momento della progettazione. Differente è invece la Privacy by Default (art. 25 com. 2) il cui principio è quello di garantire che vengano trattati per impostazione predefinita solo i dati necessari per ogni specifica finalità del trattamento, garantendo in questo modo automaticamente il principio di minimizzazione dei dati;

5) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

6) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che tali dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

7) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

8) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri,

il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

9) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

10) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri (4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT) non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

11) "Responsabile della Protezione dei Dati Personali": noto con l'acronimo inglese DPO (Data Protection Officer), è la figura prevista e normata dagli artt. 37, 38 e 39 del Regolamento il cui compito precipuo è quello di monitorare il rispetto della normativa; fungere da *trait d'union* tra l'azienda ed il Garante; informare e fornire consulenza al titolare, al responsabile e/o ai dipendenti in ordine agli obblighi previsti dal Regolamento; fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

12) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

13) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

14) «violazione dei dati personali» (Data Breach): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

15) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

16) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; 4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT;

20) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione.

1.3. Qualità e conservazione dei dati personali, principio di necessità del trattamento

I dati personali devono essere:

- esatti ed aggiornati;
- trattati unicamente per gli scopi determinati, espliciti e legittimi definiti dalla Società;
- pertinenti, completi e non eccedenti rispetto alle finalità della raccolta.

I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. All'uopo sono utilizzate opportune clausole contrattuali quando lo sviluppo del software è commissionato all'esterno della Società. I dati personali da

questa trattati sono conservati per il tempo necessario al raggiungimento delle finalità specificate nelle informative per le diverse categorie di soggetti, dopodiché vengono cancellati seguendo le procedure interne e le prescrizioni di legge.

1.4. Adempimenti

NOMINA DEL DPO: il Responsabile della Protezione dei dati deve essere nominato obbligatoriamente nei casi in cui, ex art. 37, le attività principali del titolare consistano in trattamenti che, per la loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala; e tali attività consistano nel trattamento, su larga scala, di categorie particolari di dati.

Tale adempimento spetta al CdA o ad un Consigliere espressamente delegato delle incombenze.

NOTIFICAZIONE DEI DATA BREACHES: ogni qual volta si verifichi un attacco informatico, una perdita, una manomissione o un accesso abusivo dei dati personali trattati il Titolare o quando necessario il Responsabile della Protezione dei dati deve avvertire il Garante della Privacy entro 72 ore dalla scoperta (art. 33). La notifica deve contenere le caratteristiche della violazione; il numero degli interessati coinvolti; i contatti interni dell'operatore (in particolare quello del DPO) ed una stima delle conseguenze. Nel caso in cui tale violazione metta a rischio i diritti e le libertà degli interessati il Titolare dovrà – con un linguaggio semplice – informarli di quanto accaduto e delle misure adottare per affrontare la violazione.

INFORMARE I SOGGETTI INTERESSATI: Per questo gruppo di adempimenti sono considerate le categorie di soggetti interessati rappresentate dalle terze parti i cui dati sono trattati dalla Società. Sono altresì prese in considerazione le specifiche situazioni relative alla videosorveglianza con registrazione immagini, al trattamento dei dati dei SIC e ai trattamenti effettuati attraverso il sito internet.

NOMINARE E FORNIRE ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO: l'Incaricato del Trattamento è la persona fisica autorizzata dal Titolare o dal Responsabile a compiere le operazioni di trattamento dei dati. Avendo il compito di effettuare materialmente le operazioni di trattamento sui dati personali egli deve agire sotto la diretta autorità del titolare del trattamento. Gli incaricati sono nominati dal Responsabile delle Risorse Umane.

NOMINARE E ISTRUIRE I RESPONSABILI DEL TRATTAMENTO: i Responsabili, interni o esterni, elaborano i dati personali per conto del Titolare del trattamento nel pieno rispetto delle disposizioni in materia di protezione dei dati e delle linee guida del Titolare. Dato l'importante ruolo che questi svolgono all'interno dell'organigramma Privacy, questi devono essere nominati direttamente dal CdA.

NOMINARE E ISTRUIRE GLI AMMINISTRATORI DI SISTEMA: l'amministratore di sistema o, tecnico sistemista di rete, è una figura professionale che approfondisce le competenze di un tecnico hardware e software soprattutto per quanto riguarda le caratteristiche delle architetture informatiche, i livelli di sistemistica e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione.

1.5. Responsabilità interna dei trattamenti, la struttura della funzione Privacy

Il referente privacy è affiancato nello svolgimento dei compiti dalla figura del Privacy Officer Dott.ssa Barbara Caggegi e dall'IT Officer Ivan Tessari.

Inoltre, per ogni legal entity è nominato un Amministratore "responsabile" per la privacy.

1.6. Trattamenti affidati all'esterno della Società

Ricadono in questa fattispecie le esternalizzazioni di attività aziendali che comportano il trattamento di dati personali di cui la Società risulti essere Titolare del trattamento. È importante considerare che in tali situazioni deve essere prestata particolare attenzione al rapporto che si instaura con il destinatario dei dati. Nel caso in cui il destinatario sia un outsourcer di servizi, la normativa sulla privacy evidenzia obblighi specifici di controllo da parte del Titolare su tali trattamenti. Nel caso di designazione della società esterna quale responsabile del trattamento è richiesta, ad esempio, una fase propedeutica di valutazione dell'affidabilità del soggetto[1], la resa di specifiche istruzioni[2] ed il controllo dell'operato dell'outsourcer[3].

1.6.1. Esclusioni dalle operazioni di trattamento

Gli addetti alle pulizie appartenenti ad altre società, che, per necessità operative, accedono ai locali della Società, non sono autorizzati a svolgere alcuna operazione di trattamento. Gli incaricati adottano comportamenti atti ad evitare che ai trattamenti da loro svolti accedano, pur se accidentalmente, le persone non autorizzate.

[1] Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

[2] I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

[3] Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

1.7. Dettaglio degli adempimenti

1.7.1. Richiesta di verifica preliminare

Il trattamento dei dati diversi da quelli particolari (art. 9) e quelli relativi a condanne penali e reati (art. 10) che presenta rischi specifici per i diritti e le libertà fondamentali è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato che sono prescritti dal Garante nell'ambito di una verifica preliminare anche a seguito di una richiesta del Titolare.

La verifica preliminare è da richiedere ad esempio per l'uso di sistemi di videosorveglianza c.d. "intelligenti", che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli.

1.7.2. Informativa e consenso – Artt. 12, 13 e 14

Prima della raccolta dei dati del soggetto vi è l'obbligo di rendere l'informativa ai soggetti interessati e di raccogliere il consenso che, presso la Società, viene raccolto in forma scritta, al trattamento, laddove necessario, tramite gli appositi moduli di informativa/consenso.
In conseguenza di quanto sopra, il trattamento dei dati personali può essere effettuato esclusivamente per le finalità riportate nelle informative suddette e, nel caso di necessità di consenso, solo per quelle finalità per le quali è stato rilasciato il consenso dagli interessati: è vietato qualsiasi altro utilizzo non esplicitamente previsto in tale consenso.

I consensi al trattamento riguardano le seguenti finalità:

1. trasferimento dei dati personali al di fuori dell'Unione Europea;
2. gestione delle comunicazioni e correlati trattamenti funzionali ai servizi ed operazioni richiesti dal cliente (anche referenti e garanti), da parte sia della Società sia degli altri soggetti indicati nella informativa stessa;
3. trattamento di dati particolari (nei limiti in cui ciò sia strumentale a specifiche finalità perseguite in operazioni contrattuali);

4. informazioni commerciali, ricerche di mercato, ovvero iniziative promozionali relative a prodotti o servizi della società o di terzi.

1.8. Riscontro delle richieste avanzate dagli interessati ai sensi dell'art. 15 del Regolamento (Diritto d'accesso)

Il Regolamento tutela l'Interessato riservandogli, tra l'altro, specifici diritti (artt. da 15 a 21) in merito al trattamento ed al diritto di accesso ai propri dati personali ed in particolare consentendogli di ottenere dal Titolare, dal Responsabile, se designato, e/o dal DPO:

A. la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, la loro comunicazione in forma intelligibile nonché l'indicazione della loro origine, delle finalità e delle modalità del trattamento, della logica applicata in caso di trattamenti effettuati con l'ausilio di mezzi elettronici, degli estremi identificativi del Titolare, del Responsabile dei Trattamenti, del Responsabile della Protezione dei Dati Personali e del Rappresentante del Titolare, se designato, dei soggetti o delle categorie di soggetti che possono venirne a conoscenza dei propri dati personali;
B. l'aggiornamento, la rettifica, l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati e l'attestazione che queste ultime operazioni (dall'aggiornamento al blocco) sono state portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi; di opporsi in tutto o in parte per legittimi motivi al trattamento di dati personali che lo riguardano anche quando questo è previsto a fini di informazioni commerciali o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale.

Il riscontro alla richiesta dell'Interessato, ai sensi dell'art. 15 del Regolamento ("Diritto di accesso dell'Interessato"), deve essere effettuato dal Titolare o dal Responsabile.

1.9. Nomina degli Autorizzati e ambito di trattamento consentito (art. 29)

La nomina degli autorizzati è un adempimento fondamentale per il trattamento dei dati personali sia in caso di utilizzo di strumenti elettronici[4] sia nel caso di trattamenti effettuati senza l'ausilio di essi[5].

Gli Autorizzati sono nominati dal Responsabile delle Risorse Umane tramite una lettera di nomina (in caso di nuovo dipendente all'atto dell'assunzione). Tale documento dovrà essere firmato dall'Incaricato in calce al documento.

Nel caso in cui il dipendente sia un lavoratore interinale, la nomina dovrà essere predisposta dalle Risorse Umane coadiuvata dalla struttura organizzativa destinataria della risorsa. Anche in questo caso la nomina dovrà essere debitamente firmata in calce dall'Interessato.

La nomina di Autorizzato per i collaboratori esterni spetterà alle Risorse Umane coadiuvata dalla struttura organizzativa destinataria della collaborazione. La nomina, personalizzata a seconda del tipo di collaborazione, deve essere consegnata all'atto dell'inizio del rapporto di collaborazione con le specifiche istruzioni e ritiro della relativa dichiarazione.

Qualora venga incaricato uno stagiaire, la nomina è predisposta dalle Risorse Umane che consegnerà all'atto dell'inizio dello stage. La dichiarazione deve essere firmata dallo stagiaire e consegnata alle Risorse Umane.

1.9.1. Nomina degli Autorizzati del trattamento interni all'azienda (dipendenti e professionisti)

Il personale dipendente in servizio presso la Società è autorizzato a trattare i dati personali, di cui la Società è Titolare, strettamente necessari e/o comunque connessi alle funzioni proprie dell'unità organizzativa di appartenenza alla quale il singolo incaricato è addetto. Tale trattamento può essere effettuato attraverso l'accesso agli archivi cartacei a disposizione della predetta unità organizzativa e l'utilizzo delle procedure informatiche previsto dal profilo di abilitazione assegnato.

[4] "Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti." Regola 1 del Disciplinare Tecnico allegato al Codice.

[5] Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali" Regola 27 del Disciplinare Tecnico allegato al Codice.

I dati personali particolari e relativi a condanne penali, potranno essere trattati, nel rispetto delle Autorizzazioni generali emanate dall'Autorità Garante (in particolare le Autorizzazioni n. 1, 5 e 7) e reperibili sul sito della stessa Autorità, dalle seguenti categorie di autorizzati della Società:

- per quanto riguarda i dati inerenti il rapporto di lavoro dei dipendenti e assimilati e dei loro familiari: dagli addetti delle Risorse Umane, nonché dai diretti superiori.

Taluni autorizzati di trattamenti di dati particolari e relativi a condanne penali potranno ricevere ulteriori specifiche indicazioni che integrano quelle generali di cui alla presente Policy. I responsabili delle Unità Organizzative verificano periodicamente la pertinenza, non eccedenza e indispensabilità dei dati particolari e relativi a condanne penali trattati presso le funzioni di competenza.

Inoltre per quanto riguarda:

- gli utenti della funzione HR, del Servizio Internal Audit, e di IT in funzione del ruolo ricoperto, è consentito l'accesso ai dati di diversa natura (particolari, relativi a condanne penali, di rischio specifico), necessari allo svolgimento di detto ruolo;
- i dati connessi alla gestione della segnalazione delle operazioni sospette, nel rispetto della Normativa

Antiriciclaggio: sono trattati dal Responsabile per la segnalazione delle operazioni sospette e dai soggetti coinvolti nel relativo processo.

2. Change Management/Gestione dei Cambiamenti

La Gestione dei Cambiamenti delle applicazioni e risorse IT ha per obiettivo di garantire il controllo su modifiche, sostituzioni e adeguamenti ai sistemi.

Il processo presuppone:

- la predisposizione e il costante aggiornamento nel tempo di un inventario o mappa del patrimonio IT (hardware, software, dati, procedure);
- la valutazione dell'impatto dei cambiamenti sul sistema e dei rischi correlati con le proposte di modifica;
- procedure per l'autorizzazione formale di ogni cambiamento in ambiente di produzione (con valutazione del nuovo rischio residuo nei casi in cui sia prevista la valutazione del rischio);
- la pianificazione, il coordinamento e la documentazione di tutti gli interventi di modifica;

- attività di collaudo e test, compresi i test di sicurezza, in un ambiente deputato e distinto da quello di produzione;
- il ricorso a un idoneo sistema di gestione della configurazione di sistema (hardware, software, procedure di gestione e utilizzo, modalità di interconnessione), per il controllo dell'implementazione dei cambiamenti, inclusa la possibilità di ripristino della situazione ex ante.

Devono inoltre essere previste apposite procedure per le modifiche in caso di emergenza. Tali modifiche possono essere gestite con presidi non pienamente conformi alle policy ordinarie ma comunque adeguati alla particolare situazione ed essere sottoposte a tracciamento e notificate ex post alle funzioni preposte.

3. Sicurezza dei Dati

L'informazione è un bene estremamente prezioso e in quanto tale deve essere protetto dai rischi che potrebbero minacciare la sua autenticità, riservatezza, integrità e disponibilità. La Sicurezza Informatica costituisce infatti l'insieme delle misure, di natura tecnologica, organizzativa e legale, volte ad impedire o in qualche modo ridurre i danni causati da eventi intenzionali (crimini, frodi) o non intenzionali (errori umani, fenomeni naturali), che violano il patrimonio informativo aziendale. Gli aspetti di sicurezza coinvolgono nello specifico i seguenti settori informativi:

- Sicurezza logica: volta a proteggere i dati relativi le risorse informatiche;
- Sicurezza fisica: volta a salvaguardare le infrastrutture (edifici, locali, strumentazioni, ecc.), attraverso la definizione di policy e procedure dettagliate;
- Sicurezza organizzativa: volta a proteggere risorse informatiche e dati attraverso la definizione di modelli di governance.

ALLEGATI