CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 28 del REGOLAMENTO UE 2016/679 (infra "REGOLAMENTO")

tra

la Società **ISTITUTO CLINICO QUARENGHI s.r.l**., con sede legale in San Pellegrino Terme (BG), via San Carlo n. 70, C.F. e P.IVA 00404280166, in persona del Legale Rappresentante Dott.ssa Michèle Quarenghi (di seguito anche "**Titolare**"),

e

la Società **SERVIZI CONFINDUSTRIA BERGAMO S.r.l.**, con sede legale in Bergamo (BG), via C. Maffei n. 3, C.F. e P.IVA 00431200161, in persona del Legale Rappresentante Dott.ssa Monica Santini (di seguito anche "**Responsabile**");

Titolare e Responsabile, potranno essere definiti anche singolarmente la "Parte" e congiuntamente le Parti.

PREMESSO CHE

- in base all'art. 28 del Regolamento, il Titolare dei trattamenti di dati personali può proporre una persona fisica, una persona giuridica, una pubblica amministrazione e qualsiasi altro ente, associazione od organismo quale Responsabile del trattamento dei dati, che sia selezionato tra soggetti che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso i profili di sicurezza;

- il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

- il Responsabile deve procedere al trattamento secondo le istruzioni impartite per iscritto dal Titolare con contratto o altro atto giuridico che vincoli il Responsabile del trattamento e che specifichi durata, natura e finalità del trattamento, tipo di dati personali, categorie di interessati, obblighi e diritti del Titolare;

- il Titolare consente al Responsabile, ed agli Incaricati del trattamento, l'accesso ai soli dati personali la cui conoscenza sia necessaria per adempiere ai compiti loro attribuiti;

- Il Titolare e il Responsabile hanno sottoscritto un accordo di cui tale contratto è parte integrante;

- Con riferimento al Servizio reso disponibile dal Responsabile, la descrizione delle attività di trattamento è contenuta nell'Allegato I;

TUTTO CIÒ PREMESSO,

1) Il **TITOLARE DEL TRATTAMENTO DEI DATI**, soggetto cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, in persona del suo Legale Rappresentante, **designa** il **RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI effettuati nell'ambito degli accordi contrattuali in vigore.**

2) In ogni caso, il Titolare affida al Responsabile tutte – ed esclusivamente – le operazioni di trattamento dei dati personali necessarie per dare piena esecuzione al presente contratto. In caso di danni derivanti dal trattamento, il Responsabile manterrà manlevato e indenne il Titolare da qualsiasi danno diretto e indiretto (incluse eventuali sanzioni amministrative comminate da legittime autorità nei confronti del Titolare) qualora questi non abbia adempiuto agli obblighi del Regolamento specificatamente diretti ai Responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento (art. 83 e ss. Regolamento).

3) Il Titolare si impegna a comunicare ufficialmente al Responsabile qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati. Il Responsabile o i suoi incaricati non potranno effettuare alcuna operazione di trattamento dei dati al di fuori di quelle necessarie sopra ricordate.

4) Il Responsabile, per quanto di propria competenza, è tenuto in forza di legge e del presente contratto, per sé e per i propri dipendenti e per chiunque collabori con la sua attività, al rispetto delle disposizioni del sopraccitato Regolamento, della normativa nazionale di settore applicabile, nonché dei provvedimenti e/o delle autorizzazioni e/o linee guida del Garante per la Protezione dei Dati.

5) Il Responsabile dovrà eseguire i trattamenti funzionali alle mansioni ad esso attribuite in conformità al presente contratto e con le finalità per cui i dati sono raccolti. Qualora sorgesse la necessità di trattamenti sui dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il Responsabile si impegna ad informare preventivamente e in tempo utile il Titolare del trattamento che potrà opporsi.

6) Il Responsabile, per quanto di propria competenza, è tenuto in forza di legge e del presente contratto, per sé e per le persone autorizzate al trattamento che collaborano con la sua organizzazione, a dare attuazione alle misure di sicurezza previste dalla normativa pro tempore vigente in materia di trattamento di dati personali, fornendo assistenza al Titolare nel garantire il rispetto della medesima. Il Responsabile, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, deve assicurarsi che le misure di sicurezza predisposte ed adottate siano adeguate a garantire un livello di sicurezza adeguato al rischio, in particolare contro:

- distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;

- trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento.

7) Il Responsabile applicherà le misure di sicurezza, di cui al punto precedente, al fine di garantire:

- se del caso, la pseudonimizzazione e la cifratura dei dati personali;

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Il Responsabile implementerà una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, trasmettendo tempestivamente al Titolare la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito adottate.
Il Responsabile deve assicurarsi che il testo dell'informativa di cui all'art. 13 del Regolamento venga inoltrato ai soggetti interessati. A tal riguardo, il Titolare ed il Responsabile ne concordano in buona fede versione e modalità di consegna, in attuazione delle prescrizioni del Regolamento.
Il Responsabile deve, altresì, gestire tramite adeguate procedure, secondo criteri di efficienza e garantendone la custodia, la non alterazione e l'agevole reperimento della documentazione relativa agli adempimenti formali previsti dal Regolamento. Il Responsabile, su richiesta del Titolare, coadiuva quest'ultimo nelle procedure davanti al Garante o all'autorità giudiziaria in relazione alle attività rientranti nella sua competenza.

8) Il Responsabile metterà a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento; consentirà e contribuirà alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato. A tal fine, il Responsabile del trattamento informerà immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

9) Il Responsabile, nell'ambito della propria struttura aziendale, provvederà ad individuare le persone fisiche da nominare "Incaricati" del trattamento. Contestualmente alla designazione, il Responsabile si fa carico di fornire adeguate istruzioni scritte agli incaricati circa le modalità del trattamento, in ottemperanza a quanto disposto dall'art. 29 del Regolamento e dal presente mandato. A titolo esemplificativo e non esaustivo, il Responsabile, nel designare per iscritto gli incaricati, dovrà prescrivere che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Dovrà, inoltre, verificare che questi ultimi applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiave (trattamenti elettronici). Dovrà infine verificare che conservino in luogo sicuro i supporti non informatici contenenti atti o documenti con dati particolari o la loro riproduzione, adottando contenitori con serratura (trattamenti cartacei di dati sensibili). Sarà cura del Responsabile vincolare i propri incaricati al segreto, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da essi eseguite.
Inoltre, per quanto concerne i trattamenti effettuati per fornire il servizio oggetto del contratto dai propri incaricati con mansioni di "Amministratore di Sistema", il Responsabile è tenuto altresì al rispetto delle previsioni contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009, in quanto applicabili. Il

Responsabile, in particolare, si impegna a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema e a fornirli prontamente al Titolare su richiesta del medesimo.

10) Nel caso in cui il Responsabile riceva istanze dagli interessati per l'esercizio dei diritti di cui agli artt. 15 e 22 del Regolamento dovrà:

- darne tempestiva comunicazione scritta al Titolare, allegando copia della richiesta;

- tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

11) Col presente contratto, il Titolare conferisce autorizzazione scritta generale al Responsabile a poter ricorrere a eventuali ulteriori responsabili del trattamento ("sub-responsabile/i" – si veda eventuale Allegato III "Sub-responsabili"), nella prestazione del Servizio.
Nel caso in cui il Responsabile faccia effettivo ricorso a sub-responsabili, il Responsabile medesimo si impegna a selezionare sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate descritte nell'Allegato II "Misure di sicurezza", in modo tale che il trattamento soddisfi i requisiti di cui alla normativa pro tempore applicabile e garantisca la tutela dei diritti degli interessati. Il Responsabile si impegna altresì a stipulare specifici contratti, o altri atti giuridici, con i sub-responsabili a mezzo dei quali il Responsabile descriva analiticamente i loro compiti e imponga a tali soggetti di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei dati personali, imposti dal Titolare sul Responsabile ai sensi della normativa pro tempore vigente e degli applicabili provvedimenti speciali della competente Autorità di Controllo, prevedendo, in particolare, garanzie sufficienti per mettere in atto le sopraccitate misure tecniche e organizzative, di cui all'All. II.
Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile riconosce di conservare nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei sub-responsabili coinvolti, nonché si impegna a manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare al Titolare dalla mancata osservanza di tali obblighi e più in generale dalla violazione della normativa applicabile sulla tutela dei dati personali da parte del Responsabile e dei suoi sub-fornitori.
Il Responsabile si impegna altresì ad informare il Titolare di eventuali modifiche o sostituzioni previste riguardanti i sub-responsabili, dando così al Titolare la possibilità di opporsi a tali modifiche.
Il Titolare autorizza espressamente, altresì, il Responsabile, che a ciò si impegna, a stipulare per suo conto con eventuali sub-fornitori, quando stabiliti in un paese al di fuori dell'Unione Europea per il quale la Commissione Europea non abbia emesso un giudizio di adeguatezza del livello di protezione dei dati personali, un accordo per il trasferimento dei dati all'estero contenente le apposite clausole contrattuali (e successive modifiche) adottate dalla stessa Commissione Europea con Decisione 2010/87/EU del 5 febbraio 2010 (di seguito: "Clausole Contrattuali Tipo") e l'Allegato II "Misure di sicurezza" che dovrà essere inteso come Appendix 2 delle Clausole Contrattuali Tipo.

12) Il Responsabile tratterà i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo al di fuori dell'Unione Europea o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento informerà il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; e deve rispettare le disposizioni di cui agli artt. 44;45;46;49 del Regolamento;

13) Il Titolare dichiara, inoltre, che i dati, di cui al precedente punto 1), da lui trasmessi al Responsabile:

- sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;

- in ogni caso, i dati personali e/o le categorie particolari di dati personali, oggetto delle operazioni di trattamento affidate al Responsabile, sono raccolti e trasmessi rispettando ogni prescrizione della normativa applicabile. Resta inteso che rimane a carico del Titolare l'onere di individuare la base legale del trattamento dei dati personali degli interessati.

14) Il Titolare rimane responsabile del trattamento delle informazioni attuate tramite procedure applicative sviluppate secondo sue specifiche e/o attraverso propri strumenti informatici o di telecomunicazioni.

15) Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente contratto e della normativa applicabile, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato. A tale scopo il Responsabile riconosce al Titolare, e agli incaricati dal medesimo, il diritto di accedere ai locali di sua pertinenza ove hanno svolgimento le operazioni di trattamento o dove sono custoditi dati o

documentazione relativa al presente contratto. In ogni caso il Titolare si impegna per sé e per i terzi incaricati da quest'ultimo, a che le informazioni raccolte durante le operazioni di verifica siano utilizzate solo per tali finalità. Il Responsabile sarà, inoltre, tenuto a comunicare tempestivamente al Titolare istanze degli interessati, contestazioni, ispezioni o richieste dell'Autorità di Controllo e dalle Autorità Giudiziarie, ed ogni altra notizia rilevante in relazione al trattamento dei dati personali.

16) In caso di violazione dei dati personali, il Responsabile si impegna ad informare il Titolare senza ingiustificato ritardo e non al più tardi di 12 ore dal momento in cui ha conoscenza della violazione a mezzo PEC al seguente indirizzo: direzione@pec.clinicaquarenghi.it, nonché al Responsabile Protezione Dati designato dal Titolare alla casella rpd@clinicaquarenghi.it .

Il Responsabile deve assistere il Titolare avviando un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della "Scheda Evento" utilizzando il modello Allegato IV al presente contratto, contenente tutte le seguenti informazioni:

- Società/Azienda coinvolta (indicare se Responsabile o Sub-Responsabile)
- Indicazione della data, anche presunta (in tal caso, da precisare) della violazione, nonché data e ora in cui se è avuto conoscenza della medesima;
- Fonte della segnalazione;
- Tipologia di violazione e di informazioni coinvolte;
- Descrizione evento anomalo;
- Numero interessati coinvolti;
- Numerosità di dati personali di cui si presume una violazione;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Una volta condotta l'analisi preliminare, il Responsabile deve condurre un esame di primo livello per verificare che la segnalazione non tratti un falso positivo; all'esito di tale accertamento, il Responsabile recupera le informazioni di dettaglio sull'evento necessarie alle analisi di II livello e le riporta nella Scheda Evento, che deve essere inviata a mezzo PEC tempestivamente e non oltre 24 ore dalla conoscenza della violazione, al proprio referente interno del Titolare, nonché al DPO del Titolare che, nelle more, devono essere costantemente allineati.

L'evento deve essere inserito in un apposito Registro delle violazioni.

Il Responsabile si impegna a garantire il rispetto della suddetta tempistica, nonché a manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa, risarcimento, e/o sanzione che possa derivare al Titolare dalla mancata osservanza di tali obblighi.

Il Responsabile si impegna a fornire la più ampia collaborazione al Titolare medesimo, nonché alle Autorità di Controllo competenti e coinvolte, al fine di soddisfare ogni obbligo imposto dalla normativa pro tempore applicabile (es. notifica della violazione dei dati personali all'Autorità Controllo compente; eventuale comunicazione di una violazione dei dati personali agli interessati).

17) Le comunicazioni tra le parti, ai fini del presente incarico, dovranno avvenire:

- per il Titolare, a mezzo PEC all'indirizzo direzione@pec.clinicaquarenghi.it , nonché alla casella di posta elettronica direzione@clinicaquarenghi.it;

- per il Responsabile, all'indirizzo INFO@PEC.SERVIZICONFINDUSTRIA.IT nonché alla casella di posta elettronica amministrazione@serviziconfindustria.it

18) Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione, per qualsiasi causa, del trattamento da parte del Responsabile o del rapporto sottostante, il Responsabile a discrezione del Titolare sarà tenuto a: (i) restituire al Titolare i dati personali oggetti del trattamento oppure (ii) a provvedere alla loro integrale distruzione, salvo solo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini (contabili, fiscali, ecc.). In entrambi i casi il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esista alcuna copia dei dati personali di titolarità del Titolare. Il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione.

19) La presente nomina avrà la medesima durata del contratto. Qualora questo venisse meno o perdesse efficacia e per qualsiasi motivo, anche la presente nomina verrà automaticamente meno senza bisogno di comunicazioni o revoche, ed il Responsabile non sarà più legittimato a trattare i dati del Titolare.

20) Il Responsabile, ove ricorrano le ipotesi di cui all'art. 30 del Regolamento, dovrà tenere un registro ex art. 30.2 di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del Rappresentante del Titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del Responsabile della Protezione dei Dati;
- le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del Regolamento, la documentazione delle garanzie adeguate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento.

21) Resta inteso che la presente nomina non comporta alcun diritto del Responsabile ad uno specifico compenso e/o indennità e/o rimborso derivante dalla nomina medesima.

Con la presente nomina si intende espressamente revocare e sostituire ogni altra eventuale nomina per qualsivoglia tipologia di dati.

Allegati:

- ALLEGATO I "DESCRIZIONE DELLE ATTIVITÀ DI TRATTAMENTO"
- ALLEGATO II "CODICE DELLE MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- ALLEGATO III " SUB-RESPONSABILI"
- ALLEGATO IV "SCHEDA EVENTO"

Letto, confermato e sottoscritto,

San Pellegrino Terme, lì .....

Il Titolare

Istituto Clinico Quarenghi S.r.l.

_____

Per accettazione dell'incarico a Responsabile

SERVIZI CONFINDUSTRIA BERGAMO SRL

Dott.ssa Monica Santini

Per specifica accettazione del mandato conferito ai sensi dell'art.1704 Codice Civile alla nomina da parte del Responsabile di altri responsabili ai sensi dell'art. 28, c.2, del Regolamento.

Per accettazione

SERVIZI CONFINDUSTRIA BERGAMO SRL

Dott.ssa Monica Santini

ALLEGATO I

DESCRIZIONE DELLE ATTIVITÀ DI TRATTAMENTO

Categorie di interessati

Personale

Tipologia di Dati Personali oggetto di trattamento

Dati personali dei partecipanti ai corsi (nome, cognome, codice fiscale, data e luogo di nascita, cittadinanza, inquadramento, cnel, anno assunzione, tipologia contrattuale, titolo di studio, area aziendale)

Natura e finalità del trattamento

Richiesta finanziamento di attività formative a Fondimpresa.

ALLEGATO II

CODICE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE DEL FORNITORE

ALLEGATO AL CONTRATTO DI TRATTAMENTO DEI DATI PERSONALI CON "SUB-RESPONSABILI"

1.	Procedure sulla sicurezza delle informazioni	Risposta del compilatore	
	È in grado di affermare che sono stati definiti una serie di criteri e procedure per chiarire la direzione e il supporto dell'azienda in merito alla sicurezza delle informazioni ed ai controlli per i dispositivi mobili (come laptop, tablet, dispositivi ICT indossabili, smartphone, gadget USB e altri "dispositivi connessi") e per il telelavoro (come per il lavoro da casa, i road warriors e i luoghi di lavoro da remoto/virtuali).	SI	
	È in grado di affermare che sono stati definiti ruoli e responsabilità separati per la sicurezza delle informazioni e che essi sono stati assegnati a singole persone, se del caso, per evitare conflitti di interesse e prevenire attività inappropriate.	SI	
	È in grado di affermare che sono stati stipulati idonei contratti con i sub-responsabili che confermino l'adozione da parte dei medesimi di idonee misure di sicurezza tecniche e organizzative per la protezione dei dati personali.	SI	
2.	Sicurezza delle risorse umane		
	È in grado di affermare che le responsabilità sulla sicurezza delle informazioni vengano prese in considerazione, prima dell'assunzione, al momento in cui vengono selezionati dipendenti a tempo indeterminato, collaboratori e personale temporaneo (ad es. attraverso adeguate descrizioni del tipo di occupazione, screening pre-assunzione) e previste nei contratti (ad esempio nei termini e condizioni del rapporto di lavoro e in altri accordi sottoscritti che definiscano ruoli e responsabilità in materia di sicurezza, obblighi di conformità, ecc.).	SI	
	È in grado di confermare che nel corso del rapporto di lavoro, le figure direttive si assicurino che i dipendenti e i collaboratori siano consapevoli e determinati a rispettare i loro obblighi in materia di sicurezza delle informazioni e della possibilità di essere sottoposti ad un formale procedimento disciplinare in caso di incidenti in materia di sicurezza delle informazioni presumibilmente causati dai lavoratori.	SI	
	È in grado di affermare che esiste un formale procedimento disciplinare in caso di incidenti in materia di sicurezza delle informazioni presumibilmente causati dai lavoratori.	SI	
	È in grado di affermare che al momento in cui una persona lascia l'azienda, o vi siano significativi cambiamenti di ruolo all'interno della stessa, gli aspetti relativi alla sicurezza siano adeguatamente gestiti, come la restituzione delle informazioni e delle apparecchiature aziendali, l'aggiornamento dei loro diritti di accesso, e ricordando a tali soggetti i loro perduranti obblighi nel rispetto della normativa in materia di privacy e proprietà intellettuale, termini contrattuali ecc. nonché le aspettative di carattere etico.	SI	
3.	Gestione patrimoniale		
	È in grado di affermare che tutte le risorse di natura informativa siano inventariate e che i detentori siano identificati per garantire la responsabilità della loro sicurezza? Sono definite procedure di "utilizzo idoneo" e le risorse vengono restituite al momento in cui una persona lascia l'azienda.	SI	
	È in grado di confermare che le informazioni siano classificate e contrassegnate dai detentori nel rispetto delle esigenze di sicurezza e soggette ad un'adeguata gestione.	SI	
	È in grado di affermare che i supporti di memorizzazione delle informazioni siano gestiti, controllati, spostati e smaltiti in modo tale da non compromettere il contenuto delle informazioni.	SI	

4.	Controllo degli accessi		
	È in grado di affermare che i requisiti organizzativi aziendali per il controllo degli accessi alle risorse informative sia chiaramente documentato in una policy e in una procedura di controllo degli accessi e che l'accesso alla rete ed alle connessioni sia limitato.	SI	
	È in grado di confermare che l'allocazione dei diritti di accesso agli utenti sia controllata dalla registrazione iniziale dell'utente fino alla rimozione dei diritti di accesso quando non più necessari, comprese speciali restrizioni per i diritti di accesso privilegiato e la gestione delle password (ora chiamate "informazioni segrete di autenticazione"), ed è soggetta a revisioni periodiche e aggiornamento dei diritti di accesso.	SI	
	È in grado di affermare che gli utenti siano consapevoli delle loro responsabilità attraverso il mantenimento di un effettivo controllo degli accessi, ad esempio scegliendo una password complessa e tenendola riservata.	SI	
	È in grado di assicurare che l'accesso alle informazioni sia soggetto a restrizioni nel rispetto della policy sul controllo degli accessi, ad esempio attraverso un sistema di accessi sicuri, la gestione delle password, il controllo sulle utilità privilegiate e l'accesso limitato ai codici sorgente.	SI	
5.	Crittografia		
	È in grado di assicurare che le politiche sulla sicurezza delle informazioni prevedano l'uso della crittografia, oltre all'autenticazione crittografica ed ai controlli di integrità come le firme digitali e i codici di autenticazione dei messaggi e la gestione delle chiavi di crittografia.	SI	
6.	Sicurezza fisica e ambientale		
	È in grado di affermare che sia stato chiaramente definito un perimetro fisico e delle barriere, con controlli fisici all'entrata e procedure di lavoro che proteggano i locali, gli uffici, le stanze, le aree di carico/scarico ecc. da accessi non autorizzati. (Si dovrebbe chiedere una consulenza specialistica in merito alla protezione contro incendi, inondazioni, terremoti, bombe, ecc.).	SI	
	È in grado di affermare che vengono protette e manutenute tutte le "apparecchiature" (ovvero, principalmente, le apparecchiature ICT) oltre che le utility di supporto (come l'alimentazione e l'aria condizionata) e il cablaggio. Le apparecchiature e le informazioni non sono portate fuori dall'area aziendale se non previa autorizzazione, e sono adeguatamente protette sia all'interno che all'esterno dell'area aziendale. Le informazioni vengono distrutte prima che i supporti di memorizzazione vengano smaltiti o riutilizzati. Le apparecchiature incustodite sono protette ed esiste un apposito spazio per le stesse ed una chiara politica di controllo.	SI	
7.	Sicurezza delle operazioni		
	È in grado di confermare che le responsabilità operative e le procedure IT siano documentate e che le modifiche alle strutture ed ai sistemi IT siano controllate. La capacità e le prestazioni sono gestite con sviluppo, test e sistemi operativi separati.	SI	
	È in grado di affermare che il controllo dei malware sia attivo e che l'utente ne sia consapevole.	SI	
	È in grado di affermare che, nel rispetto della politica aziendale per i backup, siano eseguiti e conservati idonei backup.	SI	
8.	Autenticazione e monitoraggio		
	È in grado di affermare che l'utente del sistema e le attività dell'amministratore/operatore, le eccezioni, i guasti e gli eventi sulla sicurezza delle informazioni siano registrati e protetti e che gli orologi siano sincronizzati.	SI	
	È in grado di affermare che l'installazione dei software sui sistemi operativi sia controllata.	SI	
9.	Gestione delle vulnerabilità tecniche		
	È in grado di affermare che tutte le vulnerabilità tecniche siano corrette, e che siano in vigore regole che disciplinano l'installazione del software da parte degli utenti per evitare la creazione di nuove vulnerabilità.	SI	

	È in grado di affermare che attraverso verifiche IT pianificate e controllate siano ridotti al minimo gli effetti negativi sui sistemi di produzione o accessi inappropriati ai dati.	SI	
10.	Sicurezza delle comunicazioni		
	È in grado di assicurare che le reti e i servizi di rete siano resi sicuri, ad esempio mediante la segregazione.	SI	
	È in grado di affermare che siano in vigore politiche, procedure e accordi (ad esempio accordi di riservatezza, contratti per il trattamento dei dati) relativi al trasferimento delle informazioni da/verso terze parti, compresi i messaggi elettronici.	SI	
11.	Acquisizione, sviluppo e manutenzione del sistema		
	È in grado di affermare che i requisiti relativi ai controlli di sicurezza siano analizzati e specificati, comprese le applicazioni web e le transazioni.	SI	
	È in grado di confermare che le regole che disciplinano la sicurezza dei software/lo sviluppo dei sistemi siano definite nel rispetto della policy aziendale con modifiche al controllo dei sistemi (sia applicazioni che sistemi operativi). I pacchetti software non vengono modificati e vengono osservati i principi ingegneristici di sicurezza dei sistemi. Oltre ciò, l'ambiente di sviluppo è protetto e lo sviluppo esternalizzato è controllato. La sicurezza dei sistemi è testata e i criteri di accettazione definiti al fine di includere gli aspetti sulla sicurezza.	SI	
	È in grado di affermare che i dati dei test siano accuratamente selezionati/generati e controllati.	SI	
12.	Rapporti con i fornitori		
	È in grado di confermare che sono in essere politiche, procedure, attività di sensibilizzazione e consapevolezza, ecc. per proteggere le informazioni aziendali che siano accessibili agli outsourcer IT e ad altri fornitori esterni lungo tutta la catena di fornitura, concordate all'interno dei contratti o degli accordi.	SI	
	È in grado di confermare che il monitoraggio e le revisioni/verifiche sono poste in essere per garantire che l'erogazione dei servizi da parte dei fornitori esterni soddisfi i criteri stabiliti nei contratti/accordi e che le modifiche al servizio siano controllate.	SI	
13.	Gestione degli incidenti sulla sicurezza delle informazioni		
	È in grado di affermare che le responsabilità e le procedure per gestire (segnalare, valutare, rispondere e imparare da) eventi sulla sicurezza delle informazioni, incidenti e debolezze siano poste in essere in modo coerente ed efficace in atto al fine di raccogliere idonee prove valide in giudizio ove richiesto.	SI	
14.	Aspetti della sicurezza delle informazioni relativi alla continuità aziendale		
	È in grado di affermare che la continuità della sicurezza delle informazioni sia pianificata, implementata e rivista come parte integrale dei sistemi di gestione della continuità di business aziendale.	SI	
	È in grado di confermare che le strutture IT siano sufficientemente ridondate per soddisfare le richieste di disponibilità.	SI	
15.	Conformità		
	È in grado di confermare che l'azienda identifica e documenta i suoi obblighi verso le autorità esterne ed altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, i registri [aziendali], la privacy/le informazioni personali e la crittografia.	SI	