Copyright ® RGI Public

Requisiti di conformità alla Sicurezza e Riservatezza delle informazioni

Versione 6 del 31/01/2024

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

Copyright ® RGI Public

Contents

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

Copyright ® RGI Public

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

Copyright ® RGI Public

Requisiti di conformità della Sicurezza e Riservatezza delle informazioni

1. Premessa

1.1.Ambito del documento

Obiettivo del documento è la definizione delle linee guida e dei requisiti organizzativi-tecnici-amministrativi per garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici per RGI Spa, la rispondenza di adeguati livelli di sicurezza.

Si ritiene infatti che - durante i processi di acquisizione - i fornitori, in relazione alla natura dei servizi offerti, possano accedere al patrimonio informativo di RGI Spa, introducendo potenziali rischi delle informazioni, con impatto in particolare su riservatezza, integrità, disponibilità, autenticità e non ripudio dei dati.

Processi di acquisizione condotti senza attenzione agli aspetti di sicurezza delle informazioni possono vanificare, o comunque rendere meno efficaci, le misure prese da RGI Spa per tutelare il proprio patrimonio informativo.

Per quanto sopra, il presente documento - che riguarda certamente il tema generale della sicurezza delle informazioni - ha un ambito circoscritto, e si concentra sulla sicurezza nell'approvvigionamento di beni e servizi informativi.

È utile, in questa premessa, ricordare che i contratti stipulati da RGI Spa con i fornitori che riguardano l'ICT:

- possono derivare da una gara o rappresentano appalti specifici di accordi quadro;
- possono essere pluriennali (per cui un certo grado di avvicendamento del personale del fornitore è inevitabile);
- possono comprendere più di un'iniziativa progettuale, in genere numerosi progetti distinti, che vengono condotti in parte sequenzialmente, in parte in parallelo, non necessariamente dallo stesso gruppo di lavoro del fornitore;

Ai fini del presente documento, i contratti ICT si possono classificare come segue:

- contratti di sviluppo, realizzazione e manutenzione evolutiva di applicazioni informatiche;
- contratti di acquisizione di prodotti (hardware o software);
- contratti per attività di operation e conduzione;

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

Copyright ® RGI Public

- contratti per servizi diversi da a) e c) (es. supporto, consulenza, formazione, help desk, ecc.);
- contratti per forniture miste, combinazioni delle precedenti tipologie.

1.2.A chi è rivolto il documento

I contenuti del documento vanno intesi in termini linee guida e procedure cui il fornitore deve allinearsi, anche sulla base della rilevanza e dei profili di criticità delle varie acquisizioni ICT da condurre, come illustrato nel dettaglio, per le varie indicazioni, nel capitolo 2.

l documento è rivolto ai fornitori di RGI Spa che dovranno essere a conoscenza delle problematiche legate alla sicurezza delle informazioni, in modo che siano pronti a recepire le richieste del committente senza impatti rilevanti sulle negoziazioni, e anzi con spirito di collaborazione.
Si ritiene necessario stabilire un lessico comune e condividendo gli obiettivi di sicurezza per rappresentare un vantaggio per i RGI Spa ma anche per i fornitori, rendendo più efficienti le clausole dei contratti.

1.3.Finalità del documento

Le finalità del documento sono:

- illustrare in maniera semplice e immediatamente fruibile la problematica della sicurezza delle informazioni;
- mettere a sistema (tramite opportuni glossari e classificazioni), formalizzare definizioni e concetti legati alla sicurezza delle informazioni, rendendoli coerenti con la norma e con il contesto dell'attività operative di RGI Spa;
- presentare misure di sicurezza che il fornitore deve adottare (strumenti operativi, esempi pratici, riferimenti puntuali) per garantire che le attività erogate seguano il livello di sicurezza degli attuali processi in RGI Spa ed eventualmente proporre soluzioni per alzare tale livello senza per questo aumentare in modo eccessivo la complessità dei processi e l'impegno necessario a condurli

Copyright ® RGI Public

1.4.Definizioni

- **Accordo quadro** - Gli Accordi quadro definiscono le clausole generali (ad esempio corrispettivi unitari, SLA, ecc.) che, in un determinato periodo temporale, regolano i contratti da stipulare. Nell'ambito dell'Accordo quadro, RGI Spa provvede poi, attraverso la contrattazione di appalti specifici, a negoziare i singoli contratti, personalizzati sulla base delle proprie esigenze (ad esempio quantità, caratteristiche specifiche, ecc.).
- **Account management** - Gestione account/credenziali accesso**.**
- **Asset management** - Gestione degli asset oggetto del contratto di servizio/fornitura.
- **Audit** - Processo indipendente di valutazione e verifica.
- **Change management** - Gestione del cambiamento
- **Code review** - Processo di revisione del codice/istruzioni di programmazione.
- **Penetration test** - Processo di valutazione della sicurezza di un sistema o di una rete attraverso la simulazione di un attacco.
- **Risk management** - Gestione dei rischi
- **Vulnerability assessment** - Processo di individuazione e classificazione delle vulnerabilità di sicurezza di un sistema o di una rete.
- **Web server** - Applicazione software installata su un server che gestisce le richieste di pagine web provenienti dai browser dei client (Browser Web).
- **Wiping** - Processo di cancellazione definitiva di dati contenuti su un supporto di memorizzazione, ad esempio da un Hard Disk.

1.5.Dati personali

Dati identificativi - Sono i dati che possono identificare, direttamente o indirettamente una persona, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online.

Dati Particolari - Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (Ex Art. 9 del Regolamento).

Dati giudiziari - Dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (Ex. Art. 10 del Regolamento).

Copyright ® RGI Public

2. Requisiti di Sicurezza – Regole di Condotta

2.1.Gestione delle informazioni - Generalità

Fatte salve le disposizioni dei Termini e Condizioni, in ogni Contratto e altri Allegati in materia di Privacy e Riservatezza, il fornitore, in esecuzione di ciascun servizio a beneficio di RGI Spa, dovrà attenersi alle seguenti regole di gestione:

- Il Fornitore riconosce formalmente la propria responsabilità per la protezione delle informazioni riservate sottoscrivendo un impegno di riservatezza e un accordo di non divulgazione (NDA);
- Tutte le informazioni inviate da RGI Spa al Fornitore o accessibili al Fornitore tramite accessi concordati rimangono di proprietà di RGI Spa e delle terze parti che le hanno affidate a RGI Spa. Pertanto, tali informazioni non devono essere:
  - utilizzate dal Fornitore eccetto nell'ambito del contratto;
  - divulgate, vendute, cedute
  - fornite a terzi solo nei casi previsti dal contratto;
  - sfruttate commercialmente da o in nome del Fornitore.
- al termine del lavoro, del contratto o dell'accordo, il Fornitore deve restituire tutti gli asset, compresi i dati di proprietà di RGI Spa e delle terze parti entro un termine definito e documentato; inoltre, il Fornitore deve dimostrare evidenza di aver cancellato tutte le informazioni, dati e asset ricevuti o prodotti per RGI Spa durante il periodo del contratto;
- Il fornitore deve garantire che la classificazione dei dati specificata da RGI Spa (in termini di riservatezza, integrità e disponibilità) sia rispettata durante tutte le fasi del trattamento delle informazioni;
- Il Fornitore (e qualsiasi persona occupata o incaricata da detta parte in merito al servizio offerto) deve garantire che utilizzerà le informazioni riservate di RGI Spa esclusivamente per gli scopi relativi ai servizi relativi al contratto di servizio;
- Il fornitore si impegna a rispettare le misure di sicurezza implementate da RGI Spa per la protezione e l'utilizzo dei dati; in caso di migrazione dei dati, il Fornitore si impegna a redigere un piano alternativo e un piano di recupero per prevenire la perdita o la corruzione delle informazioni di RGI Spa. Il piano alternativo dovrà essere proposto per approvazione a RGI Spa

Copyright ® RGI Public

2.2. Gestione delle informazioni - Confidenzialità, Integrità, disponibilità

Il Fornitore, in esecuzione di ciascun servizio o contratto dovrà attenersi alle seguenti regole di condotta:

- adottare misure protettive in grado di assicurare la riservatezza delle informazioni di proprietà di RGI Spa e delle informazioni di terzi affidate a RGI Spa, archiviate o in transito, che possono includere una adeguata politica / procedura di controllo accessi logici che preveda, tra le altre:
  - politiche di gestione delle registrazioni degli eventi sulle informazioni (almeno le registrazioni relative agli accessi amministrativi – accessi normali) ;
  - rispettare le prescrizioni relative alla crittografia delle informazioni riservate e delle informazioni segrete previste dalla politica di classificazione dei dati RGI Spa
  - rispettare le prescrizioni relative alla crittografia delle comunicazioni;
  - rispettare le prescrizioni relative alla gestione delle chiavi;
  - concedere l'accesso alle informazioni di RGI Spa al proprio personale utilizzando il principio del "need to know" e il privilegio minimo.
  - In caso il Fornitore debba utilizzare sub-fornitori o sub-appaltatori dovrà adottare tutte le precauzioni necessarie per mantenere la sicurezza delle informazioni e degli asset di RGI Spa. La nomina di sub-fornitori e sub-appaltatori dovrà essere comunicata a RGI Spa che si riserva di accettare o rigettare le nomine comunicando per iscritto la propria decisione.
- dimostrare di aver adottato una idonea politica di "Clear Desk e Clear Screen". Tale politica dovrà essere attuata obbligatoriamente per tutte la attività che interessano le informazioni di RGI Spa. e di terze parti.
- prevedere che tutti i documenti cartacei o altri mezzi contenenti le informazioni di RGI Spa e/o di terze parti, quando non utilizzati per attività relative ai servizi contrattualizzati, debbano essere archiviati in armadi a chiusura (chiave) o in idonei classificatori protetti da una chiusura a combinazione numerica;
- non effettuare copie di documenti classificati da RGI Spa, o da terze parti, con il livello "**Secret**" e "**Confidential**" senza la previa autorizzazione del proprietario delle informazioni;
- non effettuare copie di documenti classificati da RGI Spa, o da terze parti, con il livello "**Reserved**" utilizzando stampanti condivise al di fuori delle aree strettamente controllate;
- l'utilizzo di dispositivi per la stampa e / o l'esportazione su larga scala di informazioni riservate richiede un'autorizzazione specifica a RGI Spa e il processo di stampa o il processo di esportazione deve essere adeguatamente monitorato.

Copyright ® RGI Public

2.3.Gestione delle informazioni - Gestione dei rischi

2.3.1. Politiche di gestione dei rischi delle informazioni

Il Fornitore deve dimostrare di avere una politica di gestione del rischio che copre almeno le seguenti aree:

- valutazione e trattamento dei rischi legati ai controlli di accesso logico con particolare riferimento a:
  - processo di on-bording
  - processo di out-bording
  - processo di gestione change ruolo/mansione
  - verifica periodica dei diritti di accesso degli utenti;
- valutazione e trattamento dei rischi legati alla gestione dei ruoli e delle responsabilità assegnati a ciascuna parte
- valutazione e trattamento dei rischi delle informazioni riguardo:
  - i processi legati alla Confidenzialità
  - i processi legati all'integrità
  - i processi legati alla disponibilità
- valutazione e trattamento dei rischi legati alla sicurezza delle aree dove e informazioni sono trattate
- valutazione e trattamento dei rischi legati alla sicurezza dell'infrastruttura IT riguardo alla ridondanza degli apparati/Sistemi/dispositivi di rete
- valutazione e trattamento dei rischi legati ai processi relativi ai ruoli e alle responsabilità degli utenti che trattano e gestiscono in qualsiasi contesto le informazioni di RGI Spa
- valutazione e trattamento dei rischi legati al processo di formazione degli utenti sui temi della sicurezza delle informazioni, del dato in generale e della consapevolezza dei rischi connessi (Cyber compresi);
- valutazione e trattamento dei rischi legati alla sicurezza dello sviluppo di sistemi e manutenzione degli stessi;
- valutazione e trattamento dei rischi legati alla conformità alle normative applicabili;
- valutazione e trattamento dei rischi legati alla sicurezza della supply-chain IT
- valutazione e trattamento dei rischi legati alla sicurezza relativa ai fornitori
- valutazione e trattamento dei rischi legati al Data Leakage and Data Loss Prevention

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com

Copyright ® RGI Public

Il Fornitore dovrà nominare un Responsabile della gestione dei rischi sopracitati. La persona sarà responsabile della protezione delle informazioni di proprietà di RGI Spa e qualsiasi informazione che terze parti hanno affidato a RGI Spa
Il Fornitore valuterà periodicamente i rischi che incidono sulle attività incluse nel contratto con RGI Spa, approvando i risultati e i piani d'azione proposti; il Fornitore inoltre dovrà informare RGI Spa di eventuali ritardi nelle date concordate per lo svolgimento di specifici controlli in materia di gestione dei rischi e si conforma alle procedure concordate per il controllo di eventuali slittamenti

Il Fornitore deve dimostrare di avere attivato il processo relativo alla diffusione delle proprie responsabilità relativamente a:

- mantenere la conoscenza e il rispetto delle politiche di sicurezza pubblicate, delle procedure, degli standard e dei requisiti normativi applicabili;
- mantenimento di un ambiente di lavoro sicuro e protetto; proteggere i dispositivi non presidiati.
- informare RGI Spa di eventuali cambiamenti nell'ambiente aziendale che potrebbero avere un effetto significativo sul livello di sicurezza del servizio;

2.3.2. Monitoraggio dei Rischi

Il Fornitore deve stabilire procedure di monitoraggio dei rischi per la gestione del personale, garantendo in particolare che:

- tutto il personale del Fornitore e dei subappaltatori dovranno sottoscrivere un accordo di riservatezza per le informazioni di proprietà di RGI Spa e che terze parti hanno affidato a RGI SpaRGI Spa;
- il programma di Gestione dei rischi delle Informazioni proposto deve tenere conto anche dei rischi ambientali;
- il Fornitore dovrà predisporre un'adeguata procedura per la risoluzione delle controversie relative ad attività rientranti nell'ambito gestione dei rischi delle informazioni.
- effettuare il monitoraggio e la notifica della gestione dei rischi informatici attuando come minimo:
    - il monitoraggio e notifica dello stato di sicurezza;
    - la notifica di eventuali incidenti relativi alla gestione del rischio informatico;

Copyright ® RGI Public

2.4.Gestione dei vincoli di divulgazione ed awareness

Il Fornitore deve dimostrare di aver istituito un programma di sensibilizzazione del personale (dipendenti, terzi, ecc.) sui temi relativi ai vincoli di divulgazione delle informazioni seguendo le seguenti linee guida:

- • diffusione e adozione delle linee guida e delle politiche di gestione delle informazioni relative, con un divieto assoluto di:
  - rendere disponibili informazioni gestite dalla Società al di fuori della propria struttura organizzativa (ad esempio se un dipendente cambia azienda) senza l'espressa autorizzazione del Gestore delle informazioni;
  - uso eccessivo o indecoroso di Internet;
  - accedere o scambiare messaggi diffamatori, consultare siti Web che incitano all'odio o ai siti di giochi d'azzardo;
  - accesso a informazioni illegali, ad esempio la copia da Internet di informazioni protette da copyright come immagini, suoni o software;
  - invio automatico di e-mail interne via Internet su account privati o non autorizzati.
- I collaboratori devono essere consapevoli di:
  - rischi e le precauzioni per scaricare file o codice da Internet;
  - rischi e le precauzioni contro il download di malware da Internet;
  - uso corretto di dispositivi di archiviazione rimovibili.
  - rischi legati al phishing
  - rischi legati alle tecniche di social engineering
- la responsabilità individuale è un aspetto essenziale della sicurezza delle informazioni e deve essere raggiunta attraverso una combinazione di elevati standard di condotta, verifiche e controlli conformi allo spirito delle norme di sicurezza:
  - ogni dipendente (incluso lo staff temporaneo) deve proteggere le risorse per la sicurezza delle informazioni, in particolare i dispositivi di elaborazione durante il loro spostamento e l'uso in siti remoti o in Smart working;
  - ogni dipendente (compreso il personale temporaneo) deve notificare gli incidenti relativi alla sicurezza delle informazioni all'ufficio Sicurezza delle informazioni secondo le procedure;
  - gli utenti non devono interferire con le operazioni eseguite dalle piattaforme di sicurezza. Gli utenti non devono cercare di eludere i controlli di sicurezza;
  - gli utenti devono rispettare i requisiti di licenza del software e le restrizioni del copyright;
  - gli utenti devono essere informati dei pericoli causati dai virus informatici e delle migliori pratiche per ridurre le possibilità di infezione. Gli utenti devono utilizzare software antivirus e adottare misure adeguate in merito al rischio causato dai virus informatici;

Copyright ® RGI Public

- se un utente rileva un virus, deve seguire immediatamente le procedure aziendali;
- i dipendenti del Fornitore (compreso il personale temporaneo) non devono intraprendere alcuna azione che possa impedire e /o limitare le funzioni di gestione per la revisione di messaggi e transazioni (ad esempio l'uso di software di crittografia personale);
- i dipendenti del Fornitore (incluso lo staff temporaneo) devono rispettare gli standard della Società e quelli che possono essere imposti da RGI Spa.
- i dipendenti del Fornitore (compreso lo staff temporaneo) non devono stabilire connessioni, installare dispositivi elettronici e / o utilizzare software personale;
- i dipendenti del Fornitore (compreso lo staff temporaneo) devono proteggere le proprie credenziali, password e il sistema di gestione e generazione dei token autorizzativi (MFA);
- i dipendenti del Fornitore (compreso lo staff temporaneo) devono rispettare le leggi e i regolamenti applicabili.
- Il programma per sensibilizzare i collaboratori deve riguardare la sicurezza delle informazioni, del dato e i rischi Cyber

- nel processo di selezione e orientamento del personale d'ufficio, dei consulenti e delle società terze, il Fornitore deve attenersi almeno ai seguenti criteri di valutazione relativi alla sicurezza:
  - i nuovi assunti, compresi i temporanei e i consulenti esterni, devono accettare e firmare un documento informativo sulla sicurezza. Nessun diritto di accesso può essere concesso prima della sua firma;
  - le informazioni fornite dai candidati (identità, certificati, ecc.) devono essere verificate dal personale dell'ufficio HR che ha accesso a risorse sensibili (software o dati).
- Il Responsabile dei rischi del Fornitore deve assicurarsi che il personale abbia compreso le minacce legate al dipartimento e alle politiche di gestione delle Informazioni;
- Il personale del Fornitore incaricato di svolgere un servizio deve ricevere regolare formazione e aggiornamento sulle politiche e procedure rilevanti per la gestione dei rischi informativi e deve essere informato sul sistema di RGI Spa per la classificazione dei rischi e le procedure appropriate comunicate da quest'ultimo;
- I subappaltatori del Fornitore, incaricati di prestare il servizio, devono essere informati del sistema di classificazione dei rischi di RGI Spa e delle procedure appropriate comunicate da quest'ultimo.

Copyright ® RGI Public

2.5.Attività di sviluppo sicuro

Il Fornitore deve disporre di politiche di sicurezza che indichino espressamente i requisiti e i processi di sicurezza da adottare durante lo sviluppo di software e applicazioni, progettati secondo gli standard di sicurezza commerciale accettati (ad esempio: OWASP per applicazioni Web) e conformi alle normative.

2.5.1. Requisiti di sicurezza funzionali

I requisiti di sicurezza funzionale riguardano le funzioni solitamente visibili dagli utilizzatori di un programma software. Il Fornitore dovrà poter dimostrare di averli documentati in documenti di specifiche funzionali. Si riporta un elenco di requisiti comuni a cui il Fornitore dovrà adottare:

- le modalità di autenticazione dell'utente negli ambienti di sviluppo, che potrebbero basarsi su password, token o caratteristiche biometriche o loro combinazioni; i requisiti funzionali devono anche specificare come assicurare la sicurezza del meccanismo di autenticazione (caratteristiche delle password, mascheramento della password nella pagina di login, controllo delle credenziali solo sul server, cifratura della comunicazione); si può anche prevedere l'uso di un meccanismo di autenticazione esterno o tecniche di MFA;
- prevedere i profili, ruoli e autorizzazioni previsti dal software, incluse eventuali separazioni dei compiti;
- prevedere limitazione delle funzionalità e delle query agli utenti sulla base del loro profilo;
- prevedere utenze di amministrazione e loro autorizzazioni;
- prevedere modalità di interfacciamento con altri software; dovrebbe avvenire su canali cifrati impostati con lo scambio di certificati in modo da garantire l'identificazione delle diverse istanze;
- prevedere modalità di trasmissione su rete Internet basate solo su canali cifrati;
- impedire la possibilità degli utenti ad accedere direttamente ai dati senza la mediazione dell'applicazione;
- prevedere scelte relative all'integrità referenziale nei db;
- prevedere scelte relative alle transazioni concorrenti nei db (per esempio, se una transazione è concorrente ad una già avviata, l'utente ne deve essere avvisato in modo che possa decidere se sottoporla nuovamente);
- modalità di controllo dell'integrità delle transazioni (per esempio attraverso caratteri di controllo, rilevazione duplicati non previsti, ACK all'utente);
- modalità di conferma delle azioni degli utenti dove opportuno (per esempio con messaggi di conferma quando si vogliono cancellare dei dati);
- modalità di logging delle attività i cui log siano protetti con strumenti di anti-tampering e per i quali sia stato deciso un adeguato tempo di conservazione;

Copyright ® RGI Public

- modalità di gestione delle capacità previste (per esempio, numero massimo di utenti previsti) e possibilità di aumentarle (scaling);
- misuse case, ossia potenziali azioni degli utenti che potrebbero danneggiare l'applicazione o presentare problemi di sicurezza;
- la normativa vigente applicabile, altri regolamenti e obblighi contrattuali e loro requisiti applicabili (p.e. normativa sul trattamento dei dati personali, normativa bancaria, requisiti dei clienti);
- opzioni di configurazione dei meccanismi di sicurezza disponibili agli amministratori e agli utenti del sistema.

2.5.2. Requisiti di sicurezza tecnici

I requisiti di sicurezza tecnici sono divisi in due famiglie:

- requisiti di raffinamento dei requisiti funzionali, e
- requisiti relativi all'architettura.

Il Fornitore deve documentare i propri requisiti all'interno di specifiche o, quando si seguono metodi di tipo Agile, nelle "definition of done" o in task collegati alle user story.

Per i requisiti tecnici di raffinamento di quelli funzionali, il Fornitore deve dimostrare di utilizzare uno o più dei seguenti requisiti:

- modalità di caching delle credenziali;
- controllo e sanificazione dei dati in input da utenti e da altri processi;
- controllo delle query degli utenti;
- scelta dei protocolli crittografici e delle loro impostazioni (per esempio per la lunghezza delle chiavi).

Per i requisiti architetturali il Fornitore deve dimostrare di utilizzare uno o più dei seguenti requisiti:

- suddivisione in più livelli o tier (per esempio, in db, applicazione, presentazione);
- coesione dei moduli (ciascun modulo deve realizzare un'unica funzione);
- separazione del controllo accessi e delle autorizzazioni dagli altri moduli;
- separazione dell'interfaccia di amministrazione dagli altri moduli;
- disaccoppiamento dei moduli (loose coupling), che include il divieto di codificare dati, configurazioni e password negli oggetti software;

Copyright ® RGI Public

- verifica delle autorizzazioni per ogni operazione su un oggetto o sui dati (mediazione completa);
- utenze e relative autorizzazioni per l'interfacciamento con gli altri sistemi;
- gestione sicura delle sessioni e dei loro parametri;
- scelta di software e delle librerie di origine esterna (per cui deve essere assicurata l'affidabilità delle fonti e la disponibilità di manutenzione);
- gestione delle configurazioni in modo da permettere il patching e fixing tempestivo;
- gestione delle operazioni quando una dà errore; in particolare dovrebbero essere bloccate tutte le successive e l'utente dovrebbe essere avvertito (fail safe);
- intercettazione di tutti i possibili errori, in modo che siano gestiti.

2.5.3. Requisiti di codifica

Il Fornitore deve dimostrare di utilizzare questi requisiti anche attraverso l'evidenza della loro pubblicazione in documenti specifici (anche in wiki ad uso interno o in Regole di sviluppo sicuro) o, quando si seguono metodi di tipo Agile, nelle "definition of done".

Le regole di codifica da seguire dipendono dal linguaggio utilizzato; pertanto, il Fornitore sarà chiamato a dimostrare solo quanto ha valenza nel proprio campo di sviluppo comprendendo uno o più dei seguenti requisiti:

- definire uno standard per denominare classi, metodi, variabili e costanti in modo che ne sia comprensibile la finalità e la natura;
- la gestione dei commenti (quantità, collocazione, attenzione affinché non riportino informazioni utili per comprendere l'architettura del sistema o altre informazioni critiche);
- la gestione delle variabili per prevenire gli attacchi più diffusi;
- la lista delle funzioni da evitare.

2.5.4. Verifica test e rilascio

Il Fornitore deve effettuare una verifica finale dello stato di sicurezza del software sviluppato (compresi i Penetration test) come parte del processo di rilascio per garantire che non vi siano vulnerabilità note. Inoltre, deve garantire almeno quanto segue:

- deve supportare l'esecuzione dei test di valutazione delle vulnerabilità e di penetrazione eseguiti da RGI Spa (o da personale delegato / soggetti terzi) ai fini della verifica della sicurezza di software e sistemi;

Copyright ® RGI Public

- impegnarsi a implementare piani d'azione per correggere eventuali vulnerabilità, concordando tempi e metodi con RGI Spa, in base agli standard di Gruppo che in genere prevedono 30 giorni per risolvere le vulnerabilità di tipo "Critico", 45 giorni per le vulnerabilità di tipo elevato (high), 90 giorni per le vulnerabilità di tipo medio (medium) e 180 giorni per le vulnerabilità di tipo basso (low)";
- eseguire o consentire la revisione automatica o manuale del codice (revisione del codice sorgente) per garantire che il codice sia esente da eventuali vulnerabilità della sicurezza.

2.6.Gestione del diritto di autore

Il Fornitore deve dimostrare un atteggiamento responsabile nei confronti del copyright che possa riguardare l'uso e la licenza del software, che include:

- procedure per la gestione delle licenze software;
- controllo e divieto esplicito di utilizzo di software non autorizzato / non licenziato;

2.7.Intelligenza Artificiale

Il Fornitore deve dichiarare i propri processi interni di utilizzo dell'Intelligenza artificiale con particolare riferimento alle aree che possono essere compresi servizi contrattualizzati con RGI Spa.
Nell'ambito del perimetro del contratto con RGI Spa, il Fornitore deve fare divieto assoluto di utilizzo di piattaforme esterne per l'intelligenza artificiale per evitare compromissione e divulgazione non autorizzata di codice, dati e informazioni di RGI Spa.

Copyright ® RGI Public

3. Gestione degli incidenti

Il Fornitore deve dimostrare di avere attivato un processo di Incident Management che preveda operazioni in sequenza per la sua risoluzione. Inoltre, il Fornitore deve dimostrare la metodologia applicata per la registrazione degli incidenti. Le registrazioni devono contenere tutte le informazioni sufficienti per poter effettuare un'analisi dettagliata; i ticket relativi agli incidenti e alle vulnerabilità devono essere classificati e prioritizzati in modo appropriato in base alla gravità, e devono essere seguite le procedure di escalation e comunicazione definite per garantire la minimizzazione dell'impatto e l'informazione adeguata alla direzione. Il Fornitore deve anche dimostrare la strategia di risoluzione degli incidenti. Tale strategia dovrebbe prevedere la nomina di responsabili della raccolta delle informazioni sugli incidenti per ogni area relativa ai servizi contrattualizzati. I responsabili dovrebbero avere il compito di raccolta ma anche il compito di identificare e guidare le attività e gli sforzi relativi alla risoluzione degli incidenti.

Il Fornitore deve assicurare che i suoi processi di Incident Management siano gestiti correttamente senza costi aggiuntivi per RGI Spa, secondo le scadenze definite nel contratto sul livello dei servizi; inoltre, il Fornitore deve:

- consentire a RGI Spa di rilevare e intraprendere azioni a seguito di incidenti di sicurezza delle informazioni che le coinvolgano;
- assicurare che i log delle attività sui servizi erogati siano disponibili per la gestione corretta degli incidenti sulla sicurezza delle informazioni;
- informare immediatamente il Gestore del Contratto di RGI Spa di qualsiasi compromissione accertata o sospetta; in caso di compromissione di dati privacy il Fornitore dovrà rispettare i vincoli imposti dalla normativa in vigore sulla tutela della privacy fornendo a RGI Spa comunicazione entro 24 ore dall'accertamento della possibile/probabile compromissione

3.1.Processo di gestione e risoluzione

In caso di incidente o vulnerabilità confermata o sospettata, i responsabili della sicurezza pertinenti agli eventi in analisi hanno il compito di garantire che gli sforzi richiesti nella propria area di responsabilità siano adeguatamente compresi, assegnati e prioritizzati.
Il responsabile della sicurezza pertinente sarà coinvolto in tutte e 4 le fasi dell'incidente, ovvero:

- **Rilevamento** - Questa fase si deve identificare la modalità di scoperta prevedendo automatismi per la fase successiva di registrazione dove si registra l'incidente avviando il processo. Il Fornitore dovrà considerare l'avanzamento del processo di gestione facendo attenzione al "time-Tracking".

Copyright ® RGI Public

- **Analisi e classificazione** - Il Fornitore dovrà classificare l'incidente secondo parametri quale tipologia, valutazione iniziale dell'impatto e urgenza di gestione. La valutazione fornirà le basi per la corretta prioritizzazione dell'incidente. Questa classificazione dovrà essere propedeutica alla corretta scelta di chi dovrà occuparsi dell'incidente, della metodologia di gestione e dell'utilizzo di eventuali work-around se fossero presenti nella Knowledge Base.
- **Contenimento, eradicazione e ripristino** - Il Fornitore deve seguire attentamente questa fase che può essere assegnata a una persona singola se l'incidente è già stato trattato in passato e sono state utilizzate tecniche o soluzioni di contenimento che hanno avuto successo. In caso di nuova tipologia di incidente, o in caso si sia di fronte a una situazione complessa, il fornitore dovrà avere una procedura di gestione che preveda un team cross-function per meglio gestire l'incidente. La diagnosi potrà dare come risultato una nuova classificazione dell'incidente. **Un incidente sarà risolto** quando la soluzione di mitigazione sarà attuata in maniera automatica o sarà fornita all'utente/i la procedura di ripristino o, infine, sarà gestita da un team dedicato che metterà in campo tutte le attività necessarie. **Se i tempi di risoluzione supereranno eventuali SLA contrattuali**, il Fornitore dovrà attuare strategia di ripristino attraverso i piani di Disaster Recovery concordati con RGI Spa. Inoltre, il Fornitore deve provare di avere attivato il processo per la chiusura degli incidenti che preveda:
  - la procedura per la comunicazione agli stakeholders interessati della chiusura dell'incidente e ripristino delle normali attività di lavoro;
  - la consuntivazione di tutte le attività di gestione dell'Incidente;
  - la procedura di revisione, se necessario, della documentazione relativa alle configurazioni degli asset aziendali che sono stati oggetto di mitigazione dell'Incidente;
- **Attività post incidente** - Il Fornitore deve dimostrare di avere un processo di post analisi che preveda:
  - analisi delle attività per individuare quelle che hanno portato effetti positivi e quelle che non hanno portato effetti positivi per la risoluzione dell'incidente
  - creazione di un playbook di gestione relativo all'incidente da inserire nella Knowledge-base
  - processo di test periodico di incidenti per migliorare la prontezza operativa

3.2.Incident Response Team (IRT)

Il Fornitore è inoltre chiamato a dare evidenza dell'organizzazione del proprio Incident Response Team (IRT) o, in alternativa, predisporne uno per la gestione degli incidenti su informazioni di RGI Spa. Inoltre, l'IRT del Fornitore dovrà essere in grado di collaborare con il team di risposta alle emergenze identificato da RGI Spa, in caso di violazione della gestione di un rischio grave.

Copyright ® RGI Public

4. Controlli logici e misure di Sicurezza

4.1.Misure di sicurezza generali

Il Fornitore deve garantire l'implementazione di adeguati controlli logici di sicurezza da applicare su dati e ambienti oggetto del contratto in base ai seguenti requisiti di RGI Spa:

- Il Fornitore dovrà garantire che la necessaria documentazione di ambiente (Infrastruttura IT), per esempio le guide operative per l'utente e per l'amministratore, i diagrammi dell'architettura di Sistema oggetto del contratto, eventuali PlayBook per la gestione di aree particolari, ecc., sia messa a disposizione del personale autorizzato al fine di garantire:
  - la progettazione, l'installazione e il funzionamento del sistema di informazione relativo al contratto;
  - l'uso efficace delle funzioni di sicurezza del sistema.
- il Fornitore deve garantire la separazione logica dei DATI di RGI Spa dai dati degli altri Clienti, che nel proprio data center e in tutte le apparecchiature IT, compresi gli ambienti in Cloud, sono utilizzate per fornire servizi per RGI Spa;
- l'ambiente RGI Spa, oggetto del servizio contrattualizzato, presso la sede del Fornitore o da esso gestito (Cloud) deve essere separato almeno logicamente dalle altre infrastrutture per garantire che non sia possibile la penetrazione da ambienti o reti di altri clienti della Società;
- sia garantita la separazione degli ambienti di sviluppo relativi alle componenti delle applicazioni oggetto dei servizi contrattualizzati (presentazione, elaborazione dati, database, processo di identificazione e autenticazione, ecc.) e, se possibile, ospitati su server fisici o virtuali diversi in modo che i vari componenti si trovino in zone diverse sull'architettura di rete.

Copyright ® RGI Public

4.2.Controllo Accessi logico e crittografia dei flussi informativi

Il Fornitore deve accettare le restrizioni e le misure di sicurezza di RGI Spa riportate di seguito:

- RGI Spa concede l'accesso minimo per la corretta gestione dei servizi relativi al contratto. Se il Fornitore richiede l'accesso a determinate applicazioni, l'accesso deve, ove possibile, essere fornito attraverso un sistema di servizi terminal. Se ciò non sarà possibile, i sistemi comuni dovranno essere configurati su una DMZ specifica.
- Il Fornitore deve assicurare che gestirà i diritti di accesso ai sistemi operativi e alle applicazioni secondo il principio del "Least Privilege".
- Il trasferimento di dati tra RGI Spa e il Fornitore dovrà avvenire tramite una connessione privata, sicura end-to-end che utilizzi un livello di crittografia che garantisca l'integrità della connessione e che sia allineato con gli standard di crittografia più "robusti" disponibili in commercio.
- Ove possibile, la connessione tra Fornitore e RGI Spa dovrà utilizzare meccanismi che permettano di profilare l'accesso e le connessioni esclusivamente a quanto richiesto per il servizio.
- In caso sia necessaria una connessione VPN classica, l'incapsulamento dell'applicazione (ad esempio, tramite i servizi terminal) dovrà avvenire utilizzando rigorosi controlli che permettano la segmentazione dell'accesso come sopra specificato;
- le postazioni di lavoro devono avere i supporti di archiviazione locale crittografati
- Viene concesso l'utilizzo di supporti di archiviazione rimuovibili solo se debitamente protetti da un sistema di crittografia del supporto

4.3.Sicurezza degli end-point

Le postazioni di lavoro utilizzate dal personale del Fornitore devono garantire le seguenti misure di sicurezza degli end-point

- Anti-malware installato con aggiornamenti giornalieri gestiti da remoto. Il SW Anti-malware deve prevedere una soluzione di Advanced threat prevention non disattivabile dall'utente
- Personal Firewall installato ed attivo e non disattivabile dall'utente
- Gestione del processo di WEB Filtering per prevenire la navigazione per siti non pertinenti le attività
- adozione sistemi di Data leakage prevention
- il Fornitore deve applicare i necessari sistemi di filtraggio per impedire l'accesso illimitato da Internet alle interfacce amministrative dei Siti Web;
- blocco delle condivisioni di dati su piattaforme Cloud non approvate da RGI Spa
- Non è previsto l'utilizzo di dispositivi personali (BYOD) per le attività oggetto di fornitura di servizi contrattualizzati

Copyright ® RGI Public

- il Fornitore non deve stabilire connessioni o installare sistemi che consentano il controllo dell'end-point (esclusi i fornitori responsabili della gestione della rete), che possano interferire con il controllo della rete di una compagnia assicurativa e / o che permettano l'installazione di backdoor;
- la manutenzione remota degli end-point (compresi i Server) deve essere descritta in una procedura. La procedura deve prevedere adeguate misure di sicurezza, attività di controllo e registrazione di tutte le operazioni di manutenzione effettuate da remoto. L'accesso ai sistemi per le manutenzioni remote deve avvenire su un canale sicuro utilizzando strumenti crittografici adeguati.
- Il Fornitore deve assicurare e dimostrare l'inibizione degli end-point nel consentire la connessione contemporanea della rete oggetto di contratto di servizio ed una rete non sicura (per esempio connessioni Wi-Fi-free o casalinghe) o non pertinente al servizio (es. altri clienti) e di adottare i corretti controlli per evitare l'effetto "testa di ponte".
- politiche e procedure devono essere stabilite e implementate per limitare l'accesso ai dati sensibili da dispositivi mobili e portatili, come computer portatili, telefoni cellulari e smartphone, che sono generalmente più a rischio rispetto ai dispositivi non portatili.

4.4.Secure Wiping. - Secure Disposal

SECURE WIPING – Il Fornitore deve dimostrare di aver implementato una politica per la cancellazione sicura dei dati sui supporti dismessi o riassegnati. La politica deve prevedere metodologie sempre più stringenti intese a fornire una maggiore attenzione alle tecniche di Wiping per le informazioni classificate. Il processo di Wiping deve prevedere anche la raccolta sicura delle evidenze dell'avvenuta cancellazione dei dati in modo da poter ottemperare a eventuali richieste da parte di RGI Spa. La procedura deve prevedere la registrazione completa di tutte le operazioni di Wiping

SECURE DISPOSAL – Il Fornitore deve dimostrare di aver attuato una politica di secure disposal per tutti i supporti, dispositivi e sistemi che devono essere dismessi. Le procedure operative devono dimostrare di attuare adeguate misure di distruzione, sempre più stringenti in base al livello di confidenzialità dell'apparato, dispositivo o sistema da dismettere. La procedura deve prevedere la registrazione completa delle operazioni di dismissione.

4.5.Secure Baseline

Il Fornitore deve implementare adeguate configurazioni di sicurezza dei dispositivi, delle applicazioni, degli apparati e dei sistemi, che almeno tengano conto dei seguenti requisiti:

- le configurazioni di sicurezza di base devono essere stabilite e applicate per la progettazione e lo sviluppo di applicazioni, database, sistemi, infrastrutture di rete (sviluppate o acquisite) e l'elaborazione delle informazioni deve essere conforme alle politiche, agli standard e ai requisiti normativi applicabili.
- periodicamente, almeno una volta all'anno, il Fornitore deve provvedere ad attivare un processo di revisione delle configurazioni di sicurezza applicate nella propria infrastruttura. Le varianti inserite alle varie configurazioni devono essere debitamente registrate.
- Il Fornitore deve dimostrare di aver attivato un processo di Patch Management efficace che vada a costituire uno strumento di contrasto alle vulnerabilità note ai produttori degli asset che per tale scopo emettono patch di sicurezza.
- Il Fornitore deve dimostrare di aver attivato all'interno del processo di patch Management anche le procedure di sicurezza relative all'inserimento delle patch nella propria infrastruttura. Tali operazioni di sicurezza devono prevedere ambienti di test dove si dovranno effettuare test applicativi per l'inserimento sicuro delle patch nella propria infrastruttura.
- La gestione delle patch deve prevedere una valutazione preventiva del rischio della vulnerabilità che viene mitigata con la patch. Il Fornitore deve dimostrare di aver e una procedura di valutazione e prioritizzazione dell'inserimento delle patch che tenga conto del rischio che deve essere mitigato.

4.6.Sicurezza fisica

Il Fornitore deve disporre di adeguate procedure di sicurezza fisica nei propri locali e / o uffici, per coprire le seguenti aree:

- tutti i visitatori dei Data center del Fornitore o ai quali il Fornitore ha accesso devono essere accompagnati e indossare un badge identificativo specifico. La data e l'ora di entrata e uscita devono essere registrate;
- l'identità dei visitatori deve essere verificata prima di entrare in un data center;
- nessun visitatore può essere ammesso a un data center della Società o al quale la Società ha accesso, senza un appuntamento confermato;
- il Fornitore deve stabilire procedure appropriate per garantire che le responsabilità per la manutenzione di un ambiente operativo sicuro siano correttamente assegnate e soddisfatte;
- il Fornitore deve applicare controlli fisici e ambientali per proteggere il servizio in modo proporzionato al livello di rischio e indicare le minacce fisiche e ambientali rilevate durante la valutazione del rischio;
- la protezione fisica delle attrezzature di servizio e l'area di lavoro del servizio devono includere almeno:

Copyright ® RGI Public

- sistemi per la scoperta e la notifica degli accessi illegale;
- Sicurezza degli utenti dal rischio di incendio e altre minacce come calamità naturali (tempeste, tornado, ecc.) e disastri non naturali (minacce di esplosione, attacchi cyber e altre attività accidentali o intenzionali);

- i siti in cui vengono gestiti i dati o i processi di RGI Spa devono essere conformi agli standard di sicurezza generalmente accettati (ad esempio ANSI / TIA942) per la gestione e la sicurezza dei data center.

5. Diritto di Audit

Il Fornitore deve accettare le restrizioni e le misure di sicurezza di RGI Spa riportate di seguito:

- RGI Spa o il suo personale delegato che ha firmato un accordo di non divulgazione ("NDA"), può accedere ai siti del Fornitore previo consenso di quest'ultimo (in caso di rifiuto, devono essere forniti i motivi appropriati) in base alle normative applicabili in materia di sicurezza, all'accordo sul relativo avviso preliminare da fornire in merito al personale, tempi, durata e portata dei servizi forniti e qualsiasi rifiuto di accesso alle persone delegate da RGI Spa in caso di conflitto di ruoli o impatto sul Livelli di prestazione dell'azienda;
- RGI Spa si riserva il diritto di condurre verifiche periodiche dei requisiti di sicurezza fisica dell'ambiente;
- RGI Spa (o il suo personale delegato) deve avere il diritto di ispezionare / verificare regolarmente (almeno una volta all'anno o ad intervalli pianificati) le procedure e i processi di sicurezza stabiliti all'interno dei servizi forniti, che includeranno almeno:
  - processo di gestione dei rischi;
  - processo di Incident and Change Management;
  - test di sicurezza (VA e PT, SAST, DAST, etc);
  - Linee guida per l'Hardening dei sistemi;
  - Linee guida e processi di sviluppo del software sicuro (S-SDLC)
  - Business Continuity Plan e DR e altri processi e servizi di contingenza.
- RGI Spa deve avere il diritto di ispezionare, senza costi aggiuntivi, i processi operativi implementati dal servizio, sulla base di ambiente, estensione e accordi con terze parti;
- RGI Spa si riserva il diritto di richiedere modifiche ai processi di sicurezza della Società, se questi sono considerati inadeguati. Questi cambiamenti devono essere concordati reciprocamente, commercialmente ragionevoli e soggetti a scadenze accettabili;
- RGI Spa si riserva il diritto di richiedere agli auditor di produrre rapporti di audit per verificare le misure di gestione dei rischi adottate dalla Società che fornisce il servizio, ad esempio, report sulla sicurezza IT e Penetration Test, valutazione delle vulnerabilità, piano di BCP / DR, rapporti di test sul software, ecc. .

Copyright ® RGI Public

- RGI Spa si riserva il diritto di richiedere il completamento annuale di un questionario di Autovalutazione allo scopo di valutare il livello di conformità della Società alle misure di sicurezza interne.

Sede legale:
Via San Gregorio 34
20124 Milano
t +39 02 22190111
f +39 02 22190100

Capitale Sociale € 2.522.319 i.v.
P.IVA 13251500156
C.F. 06602910017

Sede amministrativa:
Via Cesare Pavese 6
10015 Ivrea, TO
t +39 0125 935111
f +39 0125 935100

info@rgigroup.com
www.rgigroup.com