# ALLEGATO TECNICO
## AI SERVIZI DI INFRASTRUTTURA TECNOLOGICA

Sommario

SERVICE FARM® ..... 1
Infrastruttura tecnica ..... 1
Alimentazione energetica ..... 1
Sistema di raffrescamento ..... 1
Sistema antincendio ..... 1
Sistema di monitoraggio e gestione ..... 1
Sistema di gestione accessi fisici ..... 2
RIFERIMENTI NORMATIVI ..... 2
SICUREZZA DELLE INFORMAZIONI ..... 2
Certificazione ISO/IEC 27001:2013 ..... 2
PROTEZIONE ..... 3
Audit interno ..... 6
Riesame della direzione ..... 6

## SERVICE FARM®

I Servizi di Infrastruttura tecnologica sono erogati dalla Service Farm® Sistemi, che è proprietà e gestione diretta di Sistemi S.p.A.
Le sedi in cui sono ubicate le Service Farm® Sistemi si trovano in:
- Sito Primario: Via Magenta 31 - 10093 Collegno (TO) - ITALIA
- Sito Secondario: Campus Data Center Data4 Via Monzoro, 101-105 - 20010 Cornaredo (MI) - ITALIA

La connessione alla Service Farm® avviene in forma criptata e protetta tramite certificati SSL su porta TCP 443. Non richiede una dotazione hardware specifica e non fa uso di VPN dedicate.

Il Servizio SIR, nell'infrastruttura condivisa Sistemi S.p.A., utilizza la tecnologia Citrix® per virtualizzare le applicazioni Sistemi e renderle fruibili telematicamente.

### Infrastruttura tecnica

Sistemi ha realizzato una Service Farm® ad alta disponibilità di energia ed efficienza con le seguenti caratteristiche infrastrutturali.

### Alimentazione energetica

I locali sono adeguatamente alimentati da gruppi di continuità in grado di mitigare ogni rischio derivante dalla mancanza di alimentazione. A loro volta gli UPS sono alimentati da gruppi elettrogeni (con commutazione automatica da rete pubblica) per garantire la continuità anche in caso di importanti guasti alla rete pubblica:
- carico IT pari a 30KW espandibile fino a 96KW
- protezione elettrica con UPS ad alta efficienza con ridondanza N+1.

### Sistema di raffrescamento

- Raffrescamento In Row affiancato ai Rack per la gestione efficiente del calore, ridondato a livello di alimentazione e controllo.
- Ridondanza di raffrescamento N+1 mediante l'impiego di due chiller ad acqua refrigerata a free-cooling da 50KW in ridondanza, scalabile fino a 12 unità dotati di funzionalità free-cooling intelligente, compressori a inverter e management.
- Pannelli di distribuzione elettrica ad alta efficienza e scalabili a caldo integrati nelle file con ridondanza 2N a livello di Rack.

### Sistema antincendio

I locali sono protetti da un sistema per l'estinzione degli incendi costituito da:
- impianto di estinzione a gas inerte contenuto in bombole in pressione
- sistema di rivelazione incendi a norma UNI EN 12094 per mezzo di rilevatori di fumo collegati a una centrale di rilevazione
- sistema di rivelazione incendi a campionamento.

### Sistema di monitoraggio e gestione

Un sistema di monitoraggio scalabile e indipendente dai vendor che raccoglie, organizza e distribuisce allarmi critici, video di sorveglianza e informazioni di base.
Il sistema consente di monitorare in modo efficiente l'intera infrastruttura fisica critica: alimentazione, raffreddamento, sicurezza e condizioni ambientali.

### Sistema di gestione accessi fisici

Tutti i soggetti autorizzati all'accesso alle Service Farm® sono dotati di badge elettronico di identificazione che consente l'autorizzazione e la tracciatura dei varchi. I soggetti autorizzati sono debitamente formati e correttamente informati sulla necessità di adottare le necessarie cautele per assicurare la sicurezza dei locali.

## RIFERIMENTI NORMATIVI

La legislazione cogente e le norme internazionali di riferimento cui Sistemi S.p.A. ha volontariamente deciso di adeguare la propria azione, rilevanti in relazione al prodotto in esame sono:

- ISO/IEC 27001:2013 "Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti"; norma ISO riconosciuta a livello internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni. Include aspetti relativi alla sicurezza logica, fisica e organizzativa.
- Regolamento UE 2016/679 sulla protezione dei dati personali relativi alle persone fisiche.
- D.Lgs. 196/03 del 30/06/2003 Codice in materia di protezione dei dati personali.

La presente scheda descrive le modalità con cui Sistemi S.p.A. attua, mantiene e migliora in modo continuo il proprio sistema di gestione per la sicurezza delle informazioni (SGSI) in conformità ai requisiti della norma richiamata sopra.

## SICUREZZA DELLE INFORMAZIONI

I dati degli Utenti risiedono in ITALIA o in paesi EU (West Europe); Sistemi assicura che il servizio non comporta alcun trasferimento di dati fuori dall'Unione Europea.
In questo ambito ha stabilito un sistema di gestione per la sicurezza delle informazioni (**SGSI**), la cui finalità è garantire all'Utente, in fase di utilizzo dei suoi dati, un livello di sicurezza superiore a quello che si potrebbe assicurare con l'approccio tradizionale di un'installazione "on-premise".

Sistemi S.p.A. intende salvaguardare, come principio fondamentale e inderogabile, **l'INTEGRITÀ** del dato, garantendo nel contempo una adeguata accessibilità al dato stesso. Ciò si traduce nella definizione di rigide politiche di conservazione dei dati stabilite contrattualmente, personalizzabili con l'Utw, sulla base delle sue specifiche esigenze, attraverso l'adozione di servizi integrativi.

Il sistema di gestione della sicurezza dei dati è organizzato in modo da consentire il raggiungimento dei due seguenti obiettivi:

1. salvaguardare la **RISERVATEZZA** del dato; non deve cioè essere possibile che Utenti accedano a dati che non sono autorizzati a consultare;
2. salvaguardare la **DISPONIBILITÀ** del dato, cioè la continuità di accesso alle informazioni.

Tali obiettivi sono misurati tramite opportuni indicatori e i dati risultanti sono oggetto di periodica analisi al fine di migliorare in modo continuo le performance aziendali riguardo la sicurezza delle informazioni, tramite gli strumenti messi a disposizione dal SGSI.
Sistemi S.p.A. effettua altresì periodicamente, per il tramite di società esterne specializzate nel campo della CyberSecurity, attività di **Vulnerability Assesment e Penetration Test**: questi "stress tests" portano all'elaborazione di specifici report, nei quali sono evidenziate potenziali aree di rischio, minacce riscontrate e miglioramenti da attuare.
Il sistema implementato consente un'adeguata conoscenza del livello di protezione e dello stato di sicurezza dei nostri sistemi informatici. Sempre nel rispetto del principio di accountability, Sistemi ha inoltre adottato specifici criteri di classificazione del rischio e relativi tempi di remediation, nel prosieguo specificati.

Sulla base dei dati raccolti vengono proposti e diffusi ai pertinenti livelli aziendali, con frequenza almeno annuale, obiettivi misurabili e target per ciascuno degli indicatori individuati.

Il raggiungimento degli obiettivi è garantito tramite:

- attenta analisi e aggiornamento delle prescrizioni legali e regolamentari che si applicano all'infrastruttura tecnologica
- attenta analisi delle aspettative dell'Utente che richiede il servizio e definizione di conseguenti requisiti contrattuali congrui
- rivalutazione periodica del sistema rispetto al business aziendale e individuazione di nuovi eventuali requisiti di sicurezza
- definizione e attuazione di criteri e procedure per la valutazione dei rischi
- disponibilità di risorse umane qualificate e di tecnologia adeguatamente aggiornata.

### Certificazione ISO/IEC 27001:2013

In merito alla Politica appena descritta, i servizi erogati in modalità SaaS di Sistemi sono Certificati **ISO/IEC 27001:2013** ("Erogazione in modalità SaaS di servizi applicativi di natura fiscale, amministrativa e aziendale") da parte di **BureauVeritas**©.
Su questo specifico servizio, Sistemi S.p.A. ha valutato quali siano i fattori interni e esterni all'organizzazione che possono influenzare la capacità di raggiungere gli obiettivi del sistema di gestione per la sicurezza delle informazioni.

I fattori interni fondamentali sono:

- l'organizzazione aziendale dei processi
- la competenza e la consapevolezza delle persone coinvolte
- il processo di sviluppo tecnologico dell'infrastruttura aziendale
- la qualità del processo di comunicazione interna e con gli Utenti
- la capacità di fornire supporto agli Utenti del servizio
- la capacità finanziaria dell'azienda, che deve poter garantire i punti di cui sopra.

I principali fattori esterni, invece, sono:
- il contesto normativo e legislativo
- le relazioni con i fornitori e la qualità del servizio erogato dagli stessi
- il contesto macro-economico italiano ed europeo che influenza la capacità finanziaria di Sistemi S.p.A., degli Utenti e dei Fornitori.

## PROTEZIONE

Sistemi S.p.A., per gestire la protezione delle informazioni secondo le norme vigenti, ha implementato e gestirà specifiche procedure che vengono descritte nella tabella sottostante:

| AREA | PROCEDURE |
|---|---|
| **Organizzazione della Sicurezza delle Informazioni** | **Valutazione del rischio relativo alla sicurezza delle informazioni**<br>Sistemi S.p.A. ha predisposto una procedura di **Valutazione dei rischi**, che definisce specifici criteri per individuare, analizzare e ponderare i rischi.<br>La procedura è coerente con i requisiti di sicurezza individuati da Sistemi nella politica del SGSI ed impone l'adozione di criteri specifici che permettono di stabilire i livelli di accettabilità del rischio. Attraverso l'utilizzo dei necessari strumenti informatici e di parametri predefiniti è inoltre garantita la riproducibilità e la ripetibilità dei risultati, che possono, quindi, essere comparati nel tempo.<br>Il sistema di valutazione dei rischi di Sistemi si articola nelle seguenti fasi:<br>1. Identificazione dei rischi<br>2. Analisi dei rischi<br>3. Valutazione del rischio nella sua sussistenza (frequenza/gravità)<br>4. Determinazione delle misure (tecniche, organizzative e procedurali) necessarie per la gestione del rischio<br>5. Determinazione del costo economico da sostenere per far fronte al rischio.<br>Sistemi S.p.A., nella volontà di assicurare ai propri Utenti la continua evoluzione delle misure di protezione dei dati (personali e non), anche in conformità con quanto stabilito dal Regolamento generale sulla protezione dei dati personali (EU) 2016/679 - che richiede il controllo periodico delle misure di sicurezza adottate - ha stabilito la seguente periodicità di verifica dei propri sistemi:<br>• **Vulnerability Assesment: ogni 6 mesi**<br>• **Penetration Test: una volta all'anno sui servizi esterni**<br><br>**Trattamento del rischio relativo alla sicurezza delle informazioni**<br>Sistemi S.p.A. ha determinato e applica un processo di valutazione del rischio definito; la procedura prevede le seguenti fasi:<br>1. Applicare i controlli appropriati (misure preventive tecniche, organizzative e procedurali).<br>2. Accettare i rischi in modo consapevole e obiettivo, quando il livello di rischio soddisfi chiaramente i criteri per l'accettazione.<br>3. Evitare i rischi, modificando, per esempio, l'organizzazione, l'infrastruttura o i processi, in modo che il rischio non sia più presente.<br>4. Trasferire i rischi associati al business ad altre parti, per esempio richiedendo a fornitori qualificati la gestione dell'infrastruttura, del processo o del servizio cui il rischio si riferisce.<br><br>A seguito di ciò, l'azienda provvede a:<br>1. Predisporre la Dichiarazione di Applicabilità<br>2. Formulare un piano di trattamento del rischio<br>3. Ottenere l'approvazione della direzione circa il piano di trattamento e i rischi residui proposti, tramite la sottoscrizione del documento di sintesi previsto dalla procedura.<br><br>**Pianificazione e controlli operativi**<br>Sistemi S.p.A., a seguito di detta valutazione, per tutti i rischi non considerati accettabili formula un piano di trattamento del rischio, che identifica le azioni gestionali appropriate, le necessarie risorse, le responsabilità e le priorità per gestire i rischi riguardanti la sicurezza del sistema. Sistemi S.p.A. ha inoltre attivato, un piano di trattamento del rischio per conseguire gli obiettivi di controllo identificati (decidendo quindi se attuare una nuova misura di controllo, evitare il rischio o trasferirlo), includendo considerazioni sulla relativa copertura economica, nonché sull'attribuzione di ruoli e responsabilità.<br>Sistemi S.p.A. gestisce le modifiche pianificate tramite la procedura di Gestione del cambiamento. Le procedure di Gestione incidenti, Monitoraggio e riesame del sistema permettono di tenere traccia degli eventi degni di nota, avviando azioni correttive al fine di mitigare gli effetti negativi riscontrati.<br>Nell'ambito delle attività di Vulnerability Assesment e Penetration Test, Sistemi ha adottato criteri standard di classificazione del rischio e stabilito precisi tempi di adozione delle misure di miglioramento consigliate, che variano a seconda del livello di rischio/criticità riscontrato:<br>• Critical: entro 30 giorni<br>• High: entro 60 giorni<br>• Medium: entro 90 giorni<br>• Low: entro 120 giorni. |

*(segue)*

*(segue)*

| AREA | PROCEDURE |
|---|---|
| | **Responsabile della protezione dei dati**<br>Sistemi S.p.A. ha nominato un Responsabile per la Protezione dei Dati personali, per assolvere a funzioni di supporto e controllo, consultive, formative e informative nei confronti del Titolare del Trattamento relativamente all'applicazione del Regolamento UE 2016/679. Il Responsabile per la Protezione dei Dati, inoltre, coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).<br>Il RPD di Sistemi S.p.A. è contattabile all'indirizzo: rpd@sistemi.com o al numero +39.011.40.19.111 |
| **Gestione dei dispositivi** | **Inventario dei dispositivi**<br>Sistemi S.p.A. redige un inventario di tutti i beni, costantemente aggiornato, sui quali sono archiviati i dati delle società. L'accesso agli inventari di tali supporti di memorizzazione è limitato al personale Sistemi S.p.A. in possesso di debita autorizzazione.<br>**Sicurezza delle apparecchiature**<br>Sistemi S.p.A. applica regole specifiche per la messa in sicurezza delle apparecchiature in modo da:<br>• limitare l'accesso in modo appropriato<br>• gestire la continuità di servizio<br>• gestire la dismissione del bene in maniera sicura e la cancellazione del dato tramite software standard.<br>Nel caso sia necessario il trasporto del bene tra una sede ed un'altra, verranno seguite le specifiche istruzioni in materia. |
| **Gestione delle Risorse Umane** | **Competenza**<br>Sistemi S.p.A si assicura che tutto il personale a cui sono state attribuite responsabilità relative alla gestione della sicurezza delle informazioni, sia competente e debitamente istruito al fine di svolgere i compiti richiesti (cioè abbia un adeguato grado di istruzione, addestramento, abilità ed esperienza e siano vincolati alla riservatezza).<br>La procedura appena citata definisce nel dettaglio le modalità per:<br>1. Stabilire le competenze necessarie per occupare ruoli che comportano lo svolgimento di operazioni che hanno effetto sul SGSI.<br>2. Assicurare che le persone che occupano i ruoli di cui al punto 1 abbiano le competenze necessarie per istruzione, formazione, addestramento e/ o esperienza.<br>3. Ove applicabile, attuare azioni per soddisfare le necessità di cui al punto 2 (tramite per esempio: affiancamento, addestramento, formazione continua, utilizzo di personale già formato) e valutare l'efficacia delle suddette azioni.<br>4. Conservare registrazioni riguardo istruzione, formazione e addestramento, abilità, esperienza e qualifiche del personale, in generale, sulle sue competenze.<br>**Formazione relativa alla sicurezza**<br>Sistemi S.p.A. forma il proprio personale sulle procedure di sicurezza pertinenti, sui differenti livelli di accesso alle informazioni e sui ruoli dei membri del personale stesso.<br>Sistemi S.p.A forma inoltre il proprio personale sulle possibili conseguenze del mancato rispetto di regole e procedure di sicurezza. |
| **Sicurezza Fisica e Ambientale** | **Accesso fisico alle strutture**<br>Sistemi S.p.A. limita l'accesso alle strutture in cui sono situati i sistemi informativi a individui identificati e debitamente autorizzati.<br>L'eventuale accesso di terze parti è consentito, dopo registrazione e sottoscrizione di un impegno di riservatezza, solo se il terzo è accompagnato dal personale autorizzato che deve sorvegliare tutte le attività svolte dal visitatore.<br>**Protezione dalle interruzioni di alimentazione e comunicazione**<br>I locali sono adeguatamente alimentati da gruppi di continuità in grado di mitigare ogni rischio derivante dalla mancanza di alimentazione. A loro volta gli UPS sono alimentati da gruppi elettrogeni (con commutazione automatica da rete pubblica) per garantire la continuità anche in caso di importanti guasti alla rete pubblica:<br>• carico IT pari a 30KW espandibile fino a 96KW<br>• protezione elettrica con UPS ad alta efficienza con ridondanza N+1.<br>**Servizio SIR: eliminazione dei dati**<br>Come evidenziato anche nelle Condizioni generali di contratto, Sistemi S.p.A. ha stabilito precisi processi per eliminare i dati non più necessari. In particolare, l'eliminazione della componente applicativa, compresi i dati, viene effettuata trascorsi 60 giorni dalla cessazione del servizio. Nei backup i dati restano altri 30 giorni. Tale previsione, che ha natura contrattuale ed è funzionale alla gestione della Server Farm Sistemi, non lede i diritti dell'interessato riconosciuti dal Regolamento UE 2016/679. Tali impostazioni possono essere personalizzate dall'Utente, attraverso la sottoscrizione di specifici accordi integrativi. |

*(segue)*

*(segue)*

| AREA | PROCEDURE |
|---|---|
| **Gestione delle Comunicazioni e delle Operazioni** | **Comunicazione**<br>Il sistema di gestione per la sicurezza adottato da Sistemi prevede specifici obblighi di comunicazione; nel modello adottato sono riportate informazioni riguardo:<br>• cosa comunicare<br>• quando comunicare<br>• con chi comunicare<br>• chi deve comunicare<br>• quali strumenti di comunicazione utilizzare.<br>**Procedure di backup e ripristino dei dati**<br>• Sistemi S.p.A. gestisce direttamente le operazioni di backup dei dati con cadenza giornaliera. Sistemi S.p.A. effettua mensilmente dei test di ripristino volti a validare il corretto funzionamento dei backup.<br>• Un ripristino deve essere richiesto espressamente dall'Utente titolare del servizio mediante una richiesta di assistenza, sottoposta in AOL, e apposita liberatoria controfirmata, che deve essere archiviata nel sistema.<br>**Registrazione di eventi**<br>Sistemi S.p.A. registra l'accesso o l'utilizzo dei sistemi informativi che contengono i dati delle società. |
| **Controllo dell'accesso** | **Autorizzazione all'accesso**<br>• Sistemi S.p.A. gestisce e conserva la registrazione degli accessi del personale autorizzato ad accedere ai sistemi che contengono i dati degli Utenti.<br>• Sistemi S.p.A. gestisce scrupolosamente, attraverso specifiche autorizzazioni, il personale incaricato, al fine di monitorare costantemente le risorse che potranno accedere, concedere, modificare o annullare l'accesso autorizzato ai dati.<br>• Sistemi S.p.A. garantisce che l'accesso ai dati dell'Utente, nei casi in cui più risorse siano autorizzate, avvenga sempre con identificatori/accessi specifici.<br>**Privilegi minimi**<br>• Il personale del supporto tecnico viene autorizzato ad accedere ai dati dell'Utente esclusivamente in caso di necessità tramite apposita liberatoria controfirmata dal Titolare dei dati.<br>• Sistemi S.p.A. limita l'accesso ai dati dell'Utente ai soli individui che ne hanno necessità per svolgere le proprie mansioni lavorative.<br>**Integrità e riservatezza**<br>• Sistemi S.p.A. forma il proprio personale affinché disattivi le sessioni amministrative prima di uscire dalle sedi e in ogni caso quando i computer vengono lasciati incustoditi.<br>• Sistemi S.p.A. gestisce le password in modo tale da renderle incomprensibili mentre sono valide. Le password sono salvate nell'Identity Provider di autenticazione con algoritmo SHA256-salted.<br>• Per innalzare il livello di sicurezza, Sistemi assicura la cifratura in transito dei dati, garantita da un certificato pubblico rilasciato da una Certification Authority internazionalmente riconosciuta.<br>• La cifratura "a riposo" è disponibile, ma richiede che l'Utente acquisti il Servizio Integrativo.<br>**Autenticazione**<br>• Sistemi S.p.A. utilizza procedure standard del settore per identificare e autenticare gli utenti che tentano di accedere ai sistemi informativi.<br>• L'autenticazione degli addetti Sistemi è basata su una specifica policy che prevede l'adozione di password di adeguata complessità, che devono essere rinnovate con cadenza periodica programmata.<br>• Sistemi S.p.A. garantisce che le utenze amministrative disattivate o scadute non vengono concesse e/o utilizzate da altri individui. |

*(segue)*

*(segue)*

| AREA | PROCEDURE |
|---|---|
| **Gestione degli Eventi Imprevisti relativi alla Protezione delle Informazioni** | **Processo di risposta agli eventi imprevisti**<br>Sistemi S.p.A conserva una registrazione delle violazioni alla sicurezza, contenente una descrizione dell'inadempimento, del periodo in cui si sono verificate e delle relative conseguenze; vengono inoltre registrati: il nome di chi ha effettuato la segnalazione, a chi è stato segnalato, nonché la procedura adottata per il ripristino dei dati.<br>Per ogni evento, classificabile ai sensi dell'art. 4 del Regolamento 2016/679, che genera una violazione di sicurezza e della protezione del dato, tale da comportare rischi per i diritti e le libertà degli Interessati, Sistemi S.p.A., invierà una comunicazione entro 3 giorni dal momento in cui ne ha avuto conoscenza conformemente a quanto stabilito dall'art.33 del Regolamento sopra citato.<br>**Non conformità e azioni correttive**<br>Sistemi S.p.A. ha definito una procedura per la gestione delle NC (Non Conformità). La NC è il mancato soddisfacimento di un requisito che può essere riscontrato in sede di monitoraggio, di audit, tramite la segnalazione dell'Utente o un incidente della sicurezza. Quando si riscontra una non conformità la procedura prevede, in linea generale, quanto segue:<br>1. registrazione della NC, definizione e attuazione di azioni per contenerla, correggerla e fronteggiare le conseguenze;<br>2. individuazione e registrazione delle cause delle non conformità;<br>3. valutazione delle esigenze di adottare azioni onde evitare che le non conformità abbiano a ripetersi;<br>4. individuazione ed attuazione delle azioni correttive necessarie (adeguate agli effetti delle NC riscontrate);<br>5. registrazione dei risultati delle azioni adottate;<br>6. verifica dell'attuazione e, in un secondo momento, dell'efficacia dell'azione correttiva proposta, oltre che verifica e valutazione dell'impatto dell'azione correttiva sul resto del sistema.<br>7. effettuazione, se necessario, di modifiche al SGSI per consolidare e rendere sistematiche le azioni intraprese. |
| **Gestione della Continuità Aziendale** | Sistemi S.p.A. ha definito una procedura di Business Continuity volta a mitigare il rischio di indisponibilità attraverso l'adozione di specifiche procedure tecniche ed organizzative. |

## Audit interno

Sistemi S.p.A. effettua audit interni ad intervalli pianificati per stabilire se il sistema di gestione per la sicurezza e i relativi obiettivi di controllo, controlli, processi e procedure siano:

- conformi alla certificazione di riferimento e a tutte i requisiti cogenti (norme, leggi, regolamenti, ecc.)
- conformi a quanto pianificato e ai requisiti stabiliti dal SGSI e dalla politica del SGSI
- efficacemente attuati, mantenuti attivi ed aggiornati
- funzionanti secondo le attese.

Le verifiche ispettive sono sempre eseguite da personale qualificato in base a requisiti specificati e indipendente da quello che ha effettuato o è responsabile delle stesse attività. I loro risultati, lo stato di conformità rilevato ed eventuali problemi riscontrati, sono registrati in un rapporto e segnalati ai responsabili delle attività affinché intraprendano con tempestività i provvedimenti (trattamento della NC o azione correttiva) in merito alle carenze emerse dalle verifiche.

Gli esiti della verifica ispettiva sono comunicati a tutto il personale interessato e alla Direzione. Il Responsabile della Sicurezza della Gestione delle Informazioni (RSGI) ha la responsabilità di pianificare, effettuare o far effettuare le verifiche ispettive, di far gestire le NC emerse, introdurre gli eventuali provvedimenti correttivi o preventivi, di seguire l'andamento della sicurezza delle informazioni dopo l'applicazione di dette azioni correttive, e infine valutarne l'efficacia.

## Riesame della direzione

La Direzione, annualmente, riesamina la gestione della sicurezza delle informazioni per assicurarsi della sua continua idoneità, adeguatezza ed efficacia.

Il riesame valuta le opportunità per il miglioramento e le esigenze di cambiamenti al SGSI, politica ed obiettivi del sistema inclusi.