Sistema di Gestione per la Sicurezza delle Informazioni

Procedura

Requisiti di sicurezza

Redatto da:	ISMS Manager	Marco Saccani	27/11/2023 Data
Approvato da:	CEO	Federico Germi	27/11/2023 Data

Codice documento: SGI PROC Requisiti di Sicurezza

Revisione Rev. 1 del 27/11/2023

STORIA DELLE MODIFICHE APPORTATE

Revisione	Data	Modifica
Rev. 1	27-11-2023	Prima Emissione

SOMMARIO

1. GENERALITA'

1.1 Scopo

Scopo della presente disposizione è quello di definire i requisiti di sicurezza minimi da inserire negli accordi con i clienti, con i dipendenti e collaboratori e negli accordi di servizio con i fornitori.

In particolare, di fornire le linee guida sulla manutenzione dei principali strumenti HW/SW per i fornitori dei servizi IT, monitorare e controllare l'operato del fornitore.

1.2 Applicazione

Questo documento si applica a tutti i processi di Ilger.com S.r.l (di seguito "Ilger).

1.3 Validità e Decorrenza

Il presente documento è valido dalla data di approvazione.

1.4 Allegati

Nessuno.

1.5 Riferimenti

Nessuno.

2. TERMINI E DEFINIZIONI

Acronimo/ Termine	Testo esplicativo della definizione
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Informazione	Conoscenza o insieme di informazioni e dati che hanno valore per un individuo o un'organizzazione
Titolare	La persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che Tratti Dati Personali per conto del Titolare
Responsabile	La persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che, da solo o congiuntamente con altri soggetti, determini le finalità e le modalità del Trattamento dei Dati Personali

3. PARTE PRINCIPALE

Ilger considera la sicurezza delle informazioni un requisito importante delle proprie attività, da tutelare anche nei rapporti con l'esterno.

A questo scopo, tutti i soggetti che intrattengono rapporti contrattuali o attuano uno scambio di informazioni con la stessa devono sottoscrivere clausole di riservatezza e sono tenuti a rispettare i requisiti di sicurezza specificati di seguito per ciascun soggetto:

- Fornitori di servizi
- Cliente/altri fornitori
- Dipendente/Collaboratore

3.1 Requisiti di sicurezza richiesti ai fornitori di servizi

I contratti nei confronti degli "outsourcer" devono contenere, in allegato o incluso nello stesso, i parametri relativi ai livelli di servizio garantiti. In particolare, i contratti con gli outsourcer devono specificare:

- **Descrizione del servizio**: descrizione di ciascun servizio richiesto e del livello di sicurezza garantito, sulla base della classificazione delle informazioni gestite.

- **Modalità di erogazione**: modalità di interazione Cliente/Fornitore nel corso della ordinaria erogazione del servizio.

- **I requisiti di sicurezza richiesti**, in particolare riferimento a quelli:
  Logici: ad esempio i requisiti tecnologici di profilazione degli accessi, di sistemi antintrusivi e antivirus, di protezione della rete, del salvataggio periodico dei dati, della gestione delle configurazioni e degli aggiornamenti, della manutenzione periodica di HW e SW.
  Organizzativi: ad esempio la dotazione di politiche e procedure, delle attività di formazione e sensibilizzazione sulle tematiche relative alla sicurezza delle informazioni, dell'assegnazione delle responsabilità e dei ruoli, gli accordi relativi alle verifiche ispettive, alla reportistica da fornire, alle responsabilità contrattuali.
  Fisici: per la tutela fisica degli asset, la protezione fisica con misure adeguate come casseforti, armadi ignifughi o sistemi antintrusivi.

- **Key Performance Indicator (KPI)**: *elenco, descrizione, modalità di misurazione, SLA;*
  Gli indicatori possono riguardare tra l'altro:
  - Tempi di risposta.
  - Tempi di intervento.
  - Tempi di ripristino in caso di "failure".
  - Continuità di servizio, incluse le misurazioni della disponibilità e affidabilità, conformemente alle priorità di business.

- **Modalità di Gestione delle anomalie**: specificando le modalità di comunicazione e di gestione delle anomalie sui servizi.

- **Reportistica:** quale evidenza delle attività svolte e del rispetto dei requisiti di contratto, dettagliata per tipologie, frequenza e modalità di comunicazione.

- **Audit**: Attività di verifica sul campo (audit).

- **Altri documenti utili** a specificare la tipologia, il livello, e i requisiti di servizio richiesti.

3.2 Service Level Agreement (SLA) richiesti ai fornitori dei servizi IT

Nell'erogazione dei servizi IT i datacenter a cui Ilger si appoggia ed altri fornitori iCT individuati sono tenuti a rispettare i requisiti di seguito descritti.

3.2.1 Requisiti logici

- Gestione dei profili di autorizzazione ai sistemi e agli applicativi nelle fasi di generazione, aggiornamento, e disattivazione.
- strumenti HW e SW idonei a garantire la protezione dei propri sistemi da intrusioni esterne o intrusioni di software maligni.
- periodiche attività di vulnerability assessment (almeno una volta l'anno), e fornire le evidenze di tali attività.
- attività di salvataggio periodico dei dati in linea con le policy aziendali e secondo i relativi criteri di classificazione dei dati.
- aggiornamento periodico delle configurazioni dei sistemi in linea con i requisiti e i parametri di sicurezza e di servizio concordati.
- dismissione sicura degli apparati di storage, provvedendo alla cancellazione sicura dei dati
- Disaster Recovery Plan
- Incident Management Plan

3.2.2 Requisiti organizzativi

- **Definizione della Politica Generale di sicurezza.**

  Il fornitore deve definire all'interno della propria organizzazione una formale Policy di Sicurezza e garantire il suo rispetto attraverso la divulgazione di tali disposizioni a tutti i propri dipendenti, collaboratori o sub-fornitori.
  Il fornitore deve adottare tutte le misure necessarie ad assicurare che tale politica sia compresa, applicata ed attuata.

- **Pianificazione della formazione per utenti e amministratori di sistema sul tema sicurezza**

  Il fornitore si deve impegnare affinchè il personale che svolge attività che influenzano la qualità dei prodotti sw/servizi e dei processi erogati possiede la competenza adeguata alle mansioni assegnate. La competenza si basa su istruzione, addestramento, abilità ed esperienza.

- **Definizione del livello di consapevolezza e delle responsabilità relative alle problematiche di sicurezza, ad es. accordi per assicurarsi che tutte le parti coinvolte (collaboratori, subcontractors) siano a conoscenza delle proprie responsabilità.**

  Il fornitore si deve impegnare a istruire e informare in modo opportuno i componenti delle parti coinvolte nei processi di erogazione dei servizi, quali collaboratori e sub-fornitori, comunicando le politiche e le procedure di sicurezza richieste e facendo rispettare i requisiti logici, organizzativi e fisici definiti.

- **Definizione del processo di gestione dei cambiamenti**

  Il fornitore si deve impegnare a gestire gli aspetti di cambiamento dei servizi attraverso l'adozione e l'attuazione di un modello operativo utile alla gestione delle configurazioni dei sistemi.

- **Responsabilità relative dei due contraenti e conseguenze del mancato rispetto**.

  Il fornitore deve impiegare la migliore tecnologia di cui è a conoscenza e le migliori risorse a sua disposizione per fornire i propri Servizi.

  In caso di interruzione del Servizio, il fornitore si deve impegnare a ripristinare il Servizio nei tempi definiti contrattualmente.

- **Responsabilità indotte dall'applicazione delle leggi (come mantenere e testare la riservatezza e l'integrità dei dati aziendali).**

  Il fornitore si impegna a gestire i servizi, gli strumenti e i dati secondo quanto richiesto dalle leggi in vigore in Italia in merito al trattamento dei dati (D.Lgs. 196/03 e Regolamento n. 2016/679 GDPR) e conformemente a quanto richiesto dall'applicazione delle leggi del settore; quando necessario si impegna a sottoscrivere un accordo sul trattamento dei dati personali con Ilger.

- **Gestione dei sub-fornitori, e delle contromisure da adottare.**

Il fornitore si deve impegnare a comunicare per tempo, vale a dire entro 90 gg, la possibilità di usufruire di sub-fornitori per l'erogazione dei servizi, garantendo il rispetto dei livelli di servizio concordati, delle prestazioni stabilite e dell'adozione da parte del sub-fornitore delle misure di sicurezza richieste dall'Agenzia.

- **Diritti di verifica di requisiti contrattuali o di affidarli a terze.**
  Ilger si riserva il diritto di effettuare, o far effettuare a terzi per conto proprio, delle attività di verifica ispettiva relativa al rispetto dei requisiti richiesti, ivi incluse il rispetto di policy e procedure e dei rischi comunicati.

3.2.3 Requisiti fisici

- Ilger definisce e nomina preventivamente il personale autorizzato ad accedere fisicamente nei propri locali per effettuare attività di manutenzione, intervento ordinario o straordinario sui sistemi e/o sugli impianti.
- Il fornitore si deve impegnare a seguire le disposizioni di accesso ai locali previste dal sistema di gestione.

3.2.4 Key Performance Indicator (KPI)

elenco, descrizione, modalità di misurazione, SLA

- Ilger fissa dei target di servizio, concordando con il fornitore i relativi indicatori e livelli. Gli indicatori possono riguardare tra l'altro:
  - tempi di risposta
  - tempi di intervento
  - tempi di ripristino in caso di "failure"
  - Continuità di servizio, incluse le misurazioni della disponibilità e affidabilità, conformemente alle priorità di business

- **Problem Management**: modalità di comunicazione e di gestione delle anomalie sui servizi;
  - Il fornitore si deve impegnare a definire un processo di escalation per la risoluzione di problemi tenendo in considerazione i requisiti di sicurezza e di business espressi dalla Società.
  - Il fornitore deve definire con Ilger le modalità per riportare, notificare e investigare incidenti relativi alla sicurezza delle informazioni, e alla sicurezza delle informazioni in generale, ad es. a seguito di violazioni del presente accordo.

- **Reportistica**: report standard forniti al Cliente (tipologia, frequenza, modalità di comunicazione,..);

- Il fornitore garantisce di fornire evidenze sullo stato di gestione del sistema informativo in particolare si impegna a fornire un report contenente:
  - Gestione delle credenziali di autenticazione: generazione, aggiornamenti, disattivazioni.
  - Elenco Incaricati abilitati/disabilitati e relativi profili
  - Elenco strumenti contro il rischio di intrusione e malware e relativi aggiornamenti Firewall, IDS, Antivirus.
  - Elenco attività di vulnerability assessment e correttivi implementati (patch management).
  - Salvataggi dei dati effettuati.
  - Elenco strumenti contro accessi abusivi e relativi aggiornamenti (Firewall, IDS, Antivirus)
  - Attività di custodia, uso, riuso e distruzione dei supporti di memorizzazione rimovibili
  - Segnalazioni di anomalie/emergenze (tentativi di accesso non autorizzato, continuità operativa).

- **Verifiche:** il fornitore concorda con Ilger delle verifiche periodiche. Tali verifiche potranno vertere su:
  - Verifica ispettiva dei locali del fornitore per la sicurezza ambientale ed il controllo degli accessi (se dovuto)
  - Verifica delle Politiche e delle Procedure di Gestione e Controllo delle Misure di Sicurezza: credenziali di autenticazione, sistema di autorizzazione, protezione da SW malevolo, protezione dalle intrusioni, supporti di memorizzazione rimovibili, back-up, continuità operativa, attestati di conformità degli installatori
  - Elenco Incaricati interni ed esterni: verifica dell'aggiornamento
  - Erogazione del Piano di formazione e sensibilizzazione
  - Segnalazioni di anomalie/emergenze: verifica della procedura e del registro di gestione delle anomalie.

3.2.5 LIVELLI DI SERVIZIO

Vengono individuati i livelli di servizio che il fornitore deve garantire ad Ilger in merito alla gestione dei servizi IT di base.

Definizioni

Incidente: qualsiasi evento che non fa parte del normale funzionamento di un servizio e che provoca o può provocare un'interruzione o una riduzione della qualità del servizio.

Classificazione dei disservizi
La priorità di un incidente è determinata da:

Impatto: il fattore chiave nella misurazione dell'impatto è l'impatto che l'evento/incidente ha sul business e sull'operatività dei servizi IT, secondo la seguente scala di valori:

Alto = completa o parziale interruzione di un servizio critico
Medio = completa o parziale interruzione di un servizio non critico
Basso = diminuzione delle prestazioni dei servizi

Urgenza: indica quanto il processo produttivo viene influenzato dall'evento/incidente; questo influenza il tempo che può essere tollerato per la risoluzione del problema.

Alto = il sistema/processo colpito è bloccato e gli utenti non possono lavorare
Medio = il sistema/processo è influenzato dall'evento/incidente e gli utenti non possono utilizzare alcune funzionalità
Basso = il sistema/processo non è influenzato dall' evento/incidente, ma necessità di un intervento per ripristinarne la piena efficienza

La matrice riportata qui di seguito mette in relazione Impatto ed Urgenza e definisce quindi le priorità di intervento.

Priorità		***Impatto***		
		Alto	***Medio***	***Basso***
Urgenza	***Alta***	***1***	***2***	***3***
	Media	***2***	***3***	***4***
	Bassa	***3***	***4***	***5***

L'intervento inizia quando il cliente effettua la richiesta; Il riferimento per l'inizio è la data e l'ora del ticket aperto per ogni evento.

Il tempo per completare ogni intervento è definito dai livelli di servizio concordato con il fornitore.

3.3 Requisiti di sicurezza richiesti ai dipendenti/lavoratori

- Tutto il personale sottoscrive l'impegno di riservatezza, contemporaneamente alla ricezione dell'incarico, e sicuramente prima dell'inizio del rapporto di lavoro con Ilger.
- Tutto il personale interno deve essere informato relativamente agli aspetti di sicurezza delle informazioni e deve aderire alle policy e procedure che proteggono tali informazioni.
- Tutto il personale deve rispettare politiche e procedure adottate da Ilger.
- Tutto il personale deve rispettare le istruzioni impartite da Ilger in merito alla gestione degli strumenti aziendali ed in merito al trattamento delle informazioni ed in particolare dei dati personali.
- Tutte le informazioni acquisite nello svolgimento delle mansioni/funzioni cui ciascuno è destinato sono e rimangono riservate, indipendentemente dal mezzo attraverso cui si fruiscono.

3.4 Requisiti di sicurezza dei documenti

La documentazione di sistema viene classificata in base a tre fattori:

- Ad uso interno: distribuzione liberamente all'interno dell'Azienda
- Ad uso riservate: distribuzione ad un numero ristretto di persone, tipicamente la Direzione
- Controllata: messa a disposizione dalla Direzione

3.5 REQUISITI RISPETTATI NELL'EROGAZIONE DEL SERVIZIO ZIMBRA IN CLOUD

Ilger garantisce un elevato livello di sicurezza delle informazioni nell'ambito dell'erogazione dei servizi Zimbra in cloud ai propri clienti. Tale livello di sicurezza, è raggiunto anche attraverso l'efficace implementazione di quanto previsto dai controlli degli standard internazionali in tema di sicurezza delle informazioni e dei dati, quali lo standard ISO 27001:2022.

3.5.1 RUOLI E RESPONSABILITA'

Il Cliente del servizio cloud si configura come "Titolare" del trattamento dei dati personali e delle informazioni che sono elaborate nell'ambito dell'erogazione del servizio. In quanto Titolare, il Cliente determina le finalità e i mezzi attraverso cui dati personali e informazioni sono trattati, mentre Ilger, in qualità di fornitore del servizio, si configura come "Responsabile" del trattamento dei dati.

Ilger al fine di normare, ai sensi del Regolamento UE 2016/679, le condizioni relative al trattamento dei dati personali in capo alla società, ha inviato ai propri clienti un'informativa per il trattamento dei dati personali attestante la dichiarazione di conformità al Regolamento UE 2016/679, con l'indicazione delle misure di sicurezza garantire nell'erogazione dei servizi. Inoltre, viene sottoscritto con il cliente una "Nomina del Responsabile Esterno del trattamento informatico dei dati personali" in cui sono delineati gli obblighi e i diritti in capo al Titolare e al Responsabile del trattamento e i limiti delle finalità e modalità del trattamento in capo ad Ilger.

Ilger conserva anche la responsabilità di identificare e definire chiaramente, anche attraverso apposite nomine, le figure degli amministratori di sistema che interverranno nella fornitura del servizio. In caso di richiesta da parte del cliente, ne viene fornito l'elenco.

Eventuali ulteriori fornitori coinvolti nell'erogazione del servizio, previa autorizzazione del cliente, sono vincolati al rispetto della riservatezza e dei livelli e requisiti sulla sicurezza, perseguiti e definiti da Ilger, attraverso la stipula di opportuni accordi contrattuali e accordi sulla protezione dei dati personali.

3.5.2 Principi di Sicurezza

Di seguito vengono elencati i requisiti di sicurezza che Ilger si impegna ad adottare nell' erogazione dei servizi offerti; da parte sua il cliente si impegna a rispettare gli accordi definiti tra le parti in merito all' utilizzo dell'infrastruttura e dei sistemi messi a sua disposizione da Ilger e di mettere in atto tutti gli adempimenti previsto dalla normativa vigenti in materia di protezione dei dati personali, secondo il ruolo ricoperto.

3.5.2.1 Gestione accessi logici

Ilger garantisce di gestire gli accessi logici al sistema informativo e/o all'infrastruttura fornita, ovvero di fornire le specifiche al cliente affinché lo stesso sia in grado di gestirle, e di garantire la configurazione di corretti e idonei profili di autorizzazione e dei meccanismi di accesso limitando l'accesso agli autorizzati e impedendo accessi non autorizzati ai sistemi informativi.

3.5.2.2 Caratteristiche delle password

Ilger garantisce la riservatezza e le caratteristiche fondamentali, atte a garantire i requisiti di sicurezza, sulla componente riservata delle credenziali di autorizzazione o password.

3.5.2.3 Asset Management

Ilger S.r.l. identifica e mantiene aggiornato un inventario degli asset che permette di mappare adeguatamente e avere maggior controllo su tutti gli asset utilizzati per l'erogazione dei servizi.

3.5.2.4 Misure di Sicurezza

Ilger S.r.l. ha scelto di applicare di default per tutti i clienti un livello elevato di sicurezza a protezione delle informazioni e dei dati personali, indipendentemente dalla classificazione delle informazioni o dalla categoria di dati personali trattati. Ulteriori misure di sicurezza possono essere, inoltre, configurati ad integrazione.

3.5.2.5 Sicurezza fisica

Ilger S.r.l. garantisce la sicurezza del perimetro fisico in cui sono trattati i dati personali o elaborate le informazioni.

3.5.2.6 Gestione della rete aziendale e delle comunicazioni

Le reti e le comunicazioni sono gestite e controllate al fine di proteggere i dati e le informazioni presenti nei sistemi informativi e negli applicativi utilizzati internamente o trasferite all'esterno dell'organizzazione.
I meccanismi di sicurezza, i livelli di servizio (SLA) e i requisiti di gestione di tutti i servizi di rete sono identificati e inclusi negli accordi relativi a tali servizi.
Infine, è garantita la segregazione della rete sulla base dei ruoli, delle mansioni e delle responsabilità.

3.5.2.7 Gestione degli incidenti

Ilger S.r.l. ha redatto e si impegna a rispettare quanto previsto nella procedura di incident management, in modo da gestire gli incidenti in modo coerente ed efficace. Gli eventi relativi alla sicurezza delle informazioni e dei dati possono essere segnalati al fornitore e monitorati tramite gli opportuni strumenti messi a disposizione.

3.5.2.8 Log management e attività di monitoraggio

Ilger S.r.l. assicura un'adeguata gestione strutturata dei log e il loro monitoraggio.
I log sono protetti da accessi e da modifiche non autorizzate e sono esaminati e monitorati regolarmente.

3.5.2.9 Strumenti, dispositivi e apparecchiature utilizzate

Ilger S.r.l. assicura la protezione delle infrastrutture, nonché degli strumenti, dei dispositivi e delle apparecchiature utilizzate per l'erogazione del servizio (server, macchine, componenti di rete, computer, ecc.), anche preventiva tramite opportuni accorgimenti, configurazioni e opportune policy condivise con il personale, da danni, minacce e pericoli ambientali esterni, accessi non autorizzati, disservizi causati da malfunzionamenti dei servizi accessori e altri guasti accidentali. Inoltre, ne è sempre garantita la manutenzione per assicurare la disponibilità e l'integrità di tali strumenti.
Nel caso di dismissione dei dispositivi, tutte le informazioni sensibili contenute al loro interno sono rimosse in sicurezza o sovrascritte.
Inoltre, Ilger S.r.l. segue una politica di "Scrivania pulita", che è stata resa nota a tutto il personale affinché possa essere adeguatamente rispettata.

3.5.2.10 Ambienti di test e di produzione

Ilger S.r.l. garantisce sia assicurata la sicurezza delle informazioni e dei dati in tutto il ciclo di sviluppo dei sistemi informativi e che, quindi, gli ambienti di test sono mantenuti separati da quelli di produzione.

3.5.2.11 Crittografia

Ilger S.r.l. si impegna a garantire adeguati ed efficaci controlli crittografici che possano proteggere la confidenzialità, la riservatezza e l'autenticità dei dati personali e delle informazioni dei clienti.

3.5.2.12 Attività di backup

Ilger S.r.l. si impegna a garantire il backup e un agile recupero dei dati e delle informazioni in caso di incidente di sicurezza.

3.5.2.13 Continuità operativa

Ilger S.r.l. ha adottato un piano di Business Continuity per garantire la continuità operativa a fronte di emergenze ed eventi disastrosi (tra i quali l'indisponibilità della sede, l'indisponibilità dei sistemi informativi, l'indisponibilità del personale, ecc.).

3.5.2.14 Gestione delle attività manutentive

Ilger S.r.l. effettua e garantisce regolari attività di manutenzione al servizio di Zimbra e-mail & collaboration e all'infrastruttura utilizzata per l'erogazione dei servizi cloud annessi e connessi, informandoli preventivamente delle modifiche al servizio che potrebbero influire sul servizio di Zimbra stesso.

3.5.2.15 Screening del personale

Ilger S.r.l. si impegna ad eseguire una selezione del personale che sia conforme a leggi, regolamenti e principi etici, e che sia proporzionata ai requisiti specifici richiesti, alla classificazione delle informazioni e dei dati personali a cui il candidato avrà accesso e che dovrà trattare e al rischio percepito relativo alla specifica mansione assegnata.

3.5.2.16 Accordi con personale e collaboratori

Il personale e i collaboratori di Ilger S.r.l sono tutti vincolati al rispetto delle policies, delle procedure e dei regolamenti aziendali in materia di protezione e sicurezza delle informazioni e dei dati personali, nonché a specifici obblighi di riservatezza e segretezza. I profili di accesso sono mantenuti aggiornati sulla base della variazione delle responsabilità o della cessazione del rapporto di lavoro o collaborazione.

3.5.2.17 Attività formative e di sensibilizzazione

Al fine di garantire la consapevolezza, l'educazione e la formazione tra il personale in materia di sicurezza delle informazioni e protezione dei dati, Ilger S.r.l. predispone periodicamente dei corsi di formazione volti alla sensibilizzazione del proprio personale in materia di gestione della sicurezza delle informazioni, gestione della qualità e protezione dei dati personali.

3.5.2.18 Verifica e gestione delle vulnerabilità

Per garantire il massimo controllo sulla sicurezza delle informazioni viene realizzata, commissionata dal cliente o direttamente dal fornitore, un'attività di Vulnerability Assessment o di Penetration Test sul sistema informativo o sulle applicazioni installate su ambiente cloud. Le informazioni risultanti vengono messe a disposizione del cliente, su richiesta.

3.5.2.19 Audit interni

Ilger S.r.l. effettua audit interni periodici per verificare che il livello di sicurezza dichiarato sia effettivamente garantito al cliente.

3.5.2.20 Compliance e requisiti cogenti

La Società, infine, garantisce la completa conformità alla normativa relativa alla protezione dei dati personali (Regolamento Generale sulla Protezione dei Dati Personali UE 2016/679), dimostrando così la propria attenzione verso i dati personali trattati, anche nell'ambito dell'erogazione di servizi di cloud computing.