

SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Procedure SGSI

RIDUTTORI ITALIA S.r.l.

Presentazione Aziendale Sintetica e Schematica

PROFILO AZIENDALE

Riduttori Italia S.r.l. è un'azienda d'eccellenza specializzata nella progettazione, ingegnerizzazione e fornitura di soluzioni avanzate per la trasmissione di potenza e il controllo del movimento meccanico.

Sede Operativa: Via Lago di Alleghe 16, 36015 Schio (VI)

Fondazione: 2009

Certificazioni: UNI EN ISO 9001:2015

Core Business: Riduttori di velocità di precisione ed organi di trasmissione speciali

I NOSTRI PUNTI DI FORZA

Ingegnerizzazione Custom (Co-progettazione): Capacità di sviluppare soluzioni su misura partendo dalle specifiche esigenze tecniche dell'ufficio tecnico del cliente, superando i vincoli dei prodotti standard a catalogo.

Qualità Certificata e Controllata: Rigorosa selezione dei materiali e trattamenti termici mirati, con certificazione ISO 9001:2015 che garantisce tolleranze minime e massima affidabilità nel tempo.

Radicamento nel Distretto di Schio: Posizionamento strategico nel cuore di una delle aree metalmeccaniche più avanzate d'Europa, con accesso a una filiera di subfornitura ad altissima precisione.

Alte Prestazioni Meccaniche: Ottimizzazione geometrica e rettifica dei denti degli ingranaggi per garantire massima silenziosità, rendimenti elevati e giochi angolari ridotti al minimo.

GAMMA PRODOTTI TRADIZIONALE

Riduttori Epicicloidali (Planetari): Massima densità di potenza in spazi ridotti, ideali per alte coppie.

Riduttori Ortogonali e a Coppia Conica: Layout compatti ad angolo retto con ingranaggi rettificati per minimizzare vibrazioni.

Componentistica Speciale: Ingranaggi e alberi scanalati a disegno cliente.

SETTORI STRATEGICI DI ESPANSIONE

Oltre ai mercati tradizionali come il Packaging e la Meccanica Generale, l'azienda sta focalizzando gli investimenti e lo sviluppo verso i seguenti settori ad alto tasso tecnologico:

Robotica Avanzata e Automazione Industriale: Sviluppo di riduttori epicicloidali a gioco ridottissimo per garantire la massima accuratezza cinetica e di posizionamento richiesta dai moderni bracci robotici e tavole rotanti.

Green Energy e Rinnovabili: Progettazione di azionamenti speciali ad alta efficienza per inseguitori solari e piccoli impianti eolici, studiati per resistere ad agenti atmosferici e cicli di lavoro continui.

Logistica Automatizzata: Soluzioni di azionamento compatte ed efficienti per veicoli a guida autonoma (AGV e AMR) e sistemi di sollevamento per la logistica interna 4.0.

Food and Beverage: Sviluppo di linee speciali con casse in acciaio inox o trattamenti superficiali anticorrosione specifici, lubrificati con oli alimentari per l'impiego in ambienti lavabili e sterili.

APPLICAZIONI SPECIALI E AD ALTO CARICO

L'affidabilità ingegneristica di Riduttori Italia S.r.l. si estende anche a mercati di nicchia e a contesti operativi estremi, dove la resistenza strutturale e la sicurezza sono requisiti mandatori:

Settore Militare e Difesa: Sviluppo di azionamenti ad altissima affidabilità e resistenza agli urti per veicoli tattici, sistemi di puntamento radar e movimentazioni speciali blindate.

Settore Ferroviario e Infrastrutture: Fornitura di riduttori e componenti di trasmissione conformi alle severe normative di sicurezza del settore ferroviario, impiegati in sistemi di trazione, scambi, officine di manutenzione e impianti di sollevamento del materiale rotabile.

Impianti Siderurgici e Fonderie: Progettazione di riduttori corazzati per resistere a temperature ambientali elevatissime, carichi d'urto continui, polveri abrasive e atmosfere aggressive tipiche delle linee di colata continua, laminatoi e movimentazione sivere.

Luna Park e Attrazioni: Soluzioni speciali incentrate sulla massima sicurezza intrinseca dei passeggeri e sulla ridondanza meccanica, impiegate per la movimentazione e il sollevamento di giostre e grandi attrazioni panoramiche.

Settore Tessile: Fornitura di riduttori coassiali e ortogonali ad alta precisione e fluidità di movimento, ottimizzati per ridurre le vibrazioni e garantire la tensione costante dei filati sui macchinari di filatura e tessitura moderni.

FOCUS STRATEGICO: DIFESA E SPAZIO

Il settore della Difesa e dello Spazio rappresenta la massima frontiera tecnologica verso cui Riduttori Italia S.r.l. sta indirizzando le proprie risorse di Ricerca e Sviluppo. In questo ambito, i requisiti superano gli standard industriali comuni, richiedendo soluzioni ingegneristiche estreme:

Applicazioni Aerospaziali e Spaziali: Sviluppo di cinematismi e microriduttori alleggeriti con materiali speciali come le leghe di titanio o alluminio aeronautico, progettati per operare in condizioni di vuoto, temperature estreme e forti sollecitazioni vibrazionali tipiche del lancio.

Sistemi di orientamento per antenne satellitari e pannelli solari.

Sistemi di Difesa Terrestre e Navale: Realizzazione di gruppi di trasmissione ad altissima precisione per torrette di puntamento, inseguimento optoelettronico e movimentazione di sistemi radar. Ogni componente è sviluppato per garantire la massima resistenza agli shock meccanici e la conformità alle specifiche militari.

Affidabilità a Guasto Zero: Implementazione di protocolli di controllo qualità totali, tracciabilità completa dei materiali con certificati e simulazioni strutturali avanzate per garantire l'assoluta continuità operativa in scenari critici dove la manutenzione non è possibile.

Codice	SGSI-PRC-001
Data documento	15/07/2026
Versione	00
Approvato da	Alta direzione

PRESENTAZIONE

Il presente documento è redatto per fornire una rappresentazione organica, elegante e professionale del Sistema di Gestione per la Sicurezza delle Informazioni dell'organizzazione, collegando business, asset, rischi, controlli, responsabilità e miglioramento continuo in un impianto coerente con la ISO/IEC 27001:2022.

SCOPO

Lo scopo del documento è supportare direzione, funzioni aziendali, auditor, consulenti e parti autorizzate nella comprensione del perimetro del SGSI, della logica di governo adottata, delle priorità di rischio e delle misure poste a presidio delle informazioni e dei servizi rilevanti.

DESCRIZIONE DELL'AZIENDA

RIDUTTORI ITALIA S.r.l.

Presentazione Aziendale Sintetica e Schematica

PROFILO AZIENDALE

Riduttori Italia S.r.l. è un'azienda d'eccellenza specializzata nella progettazione, ingegnerizzazione e fornitura di soluzioni avanzate per la trasmissione di potenza e il controllo del movimento meccanico.

Sede Operativa: Via Lago di Alleghe 16, 36015 Schio (VI)

Fondazione: 2009

Certificazioni: UNI EN ISO 9001:2015

Core Business: Riduttori di velocità di precisione ed organi di trasmissione speciali

I NOSTRI PUNTI DI FORZA

Ingegnerizzazione Custom (Co-progettazione): Capacità di sviluppare soluzioni su misura partendo dalle specifiche esigenze tecniche dell'ufficio tecnico del cliente, superando i vincoli dei prodotti standard a catalogo.

Qualità Certificata e Controllata: Rigorosa selezione dei materiali e trattamenti termici mirati, con certificazione ISO 9001:2015 che garantisce tolleranze minime e massima affidabilità nel tempo.

Radicamento nel Distretto di Schio: Posizionamento strategico nel cuore di una delle aree metalmeccaniche più avanzate d'Europa, con accesso a una filiera di subfornitura ad altissima precisione.

Alte Prestazioni Meccaniche: Ottimizzazione geometrica e rettifica dei denti degli ingranaggi per garantire massima silenziosità, rendimenti elevati e giochi angolari ridotti al minimo.

GAMMA PRODOTTI TRADIZIONALE

Riduttori Epicicloidali (Planetari): Massima densità di potenza in spazi ridotti, ideali per alte coppie.

Riduttori Ortogonali e a Coppia Conica: Layout compatti ad angolo retto con ingranaggi rettificati per minimizzare vibrazioni.

Componentistica Speciale: Ingranaggi e alberi scanalati a disegno cliente.

SETTORI STRATEGICI DI ESPANSIONE

Oltre ai mercati tradizionali come il Packaging e la Meccanica Generale, l'azienda sta focalizzando gli investimenti e lo sviluppo verso i seguenti settori ad alto tasso tecnologico:

Robotica Avanzata e Automazione Industriale: Sviluppo di riduttori epicicloidali a gioco ridottissimo per garantire la massima accuratezza cinetica e di posizionamento richiesta dai moderni bracci robotici e tavole rotanti.

Green Energy e Rinnovabili: Progettazione di azionamenti speciali ad alta efficienza per inseguitori solari e piccoli impianti eolici, studiati per resistere ad agenti atmosferici e cicli di lavoro continui.

Logistica Automatizzata: Soluzioni di azionamento compatte ed efficienti per veicoli a guida autonoma (AGV e AMR) e sistemi di sollevamento per la logistica interna 4.0.

Food and Beverage: Sviluppo di linee speciali con casse in acciaio inox o trattamenti superficiali anticorrosione specifici, lubrificati con oli alimentari per l'impiego in ambienti lavabili e sterili.

APPLICAZIONI SPECIALI E AD ALTO CARICO

L'affidabilità ingegneristica di Riduttori Italia S.r.l. si estende anche a mercati di nicchia e a contesti operativi estremi, dove la resistenza strutturale e la sicurezza sono requisiti mandatori:

Settore Militare e Difesa: Sviluppo di azionamenti ad altissima affidabilità e resistenza agli urti per veicoli tattici, sistemi di puntamento radar e movimentazioni speciali blindate.

Settore Ferroviario e Infrastrutture: Fornitura di riduttori e componenti di trasmissione conformi alle severe normative di sicurezza del settore ferroviario, impiegati in sistemi di trazione, scambi, officine di manutenzione e impianti di sollevamento del materiale rotabile.

Impianti Siderurgici e Fonderie: Progettazione di riduttori corazzati per resistere a temperature ambientali elevatissime, carichi d'urto continui, polveri abrasive e atmosfere aggressive tipiche delle linee di colata continua, laminatoi e movimentazione siviere.

Luna Park e Attrazioni: Soluzioni speciali incentrate sulla massima sicurezza intrinseca dei passeggeri e sulla ridondanza meccanica, impiegate per la movimentazione e il sollevamento di giostre e grandi attrazioni panoramiche.

Settore Tessile: Fornitura di riduttori coassiali e ortogonali ad alta precisione e fluidità di movimento, ottimizzati per ridurre le vibrazioni e garantire la tensione costante dei filati sui macchinari di filatura e tessitura moderni.

FOCUS STRATEGICO: DIFESA E SPAZIO

Il settore della Difesa e dello Spazio rappresenta la massima frontiera tecnologica verso cui Riduttori Italia S.r.l. sta indirizzando le proprie risorse di Ricerca e Sviluppo. In questo ambito, i requisiti superano gli standard industriali comuni, richiedendo soluzioni ingegneristiche estreme:

Applicazioni Aerospaziali e Spaziali: Sviluppo di cinematismi e microriduttori alleggeriti con materiali speciali come le leghe di titanio o alluminio aeronautico, progettati per operare in condizioni di vuoto, temperature estreme e forti sollecitazioni vibrazionali tipiche del lancio. Sistemi di orientamento per antenne satellitari e pannelli solari.

Sistemi di Difesa Terrestre e Navale: Realizzazione di gruppi di trasmissione ad altissima precisione per torrette di puntamento, inseguimento optoelettronico e movimentazione di sistemi radar. Ogni componente è sviluppato per garantire la massima resistenza agli shock meccanici e la conformità alle specifiche militari.

Affidabilità a Guasto Zero: Implementazione di protocolli di controllo qualità totali, tracciabilità completa dei materiali con certificati e simulazioni strutturali avanzate per garantire l'assoluta continuità operativa in scenari critici dove la manutenzione non è possibile.

DESCRIZIONE DEL SERVIZIO

RIDUTTORI ITALIA S.r.l.

I Nostri Servizi Ingegneristici e di Supporto

CO-PROGETTAZIONE E INGEGNERIZZAZIONE CUSTOM (R&D)

Affiancamento Tecnico: Collaborazione diretta con l'ufficio tecnico del cliente fin dalle prime fasi di ideazione del macchinario per definire la soluzione di trasmissione ottimale.

Dimensionamento Personalizzato: Calcolo e progettazione assistita di riduttori speciali su misura, superando i limiti dimensionali o prestazionali dei prodotti standard a catalogo.

Analisi e Simulazione Avanzata: Utilizzo di software di simulazione FEM (Metodo degli Elementi Finiti) e modellazione cinematica per prevedere il comportamento strutturale, la resistenza a fatica e l'usura dei componenti in condizioni di carico reali.

SVILUPPO DI CINEMATISMI PER SETTORI AD ALTA TECNOLOGIA

Ottimizzazione per lo Spazio e l'Aerospazio: Progettazione di microriduttori e meccanismi alleggeriti in leghe speciali (come titanio e alluminio aeronautico) adatti a lavorare nel vuoto e a resistere a forti shock vibrazionali.

Sistemi di Precisione per la Difesa: Sviluppo di gruppi di trasmissione ad alta accuratezza cinetica e gioco ridottissimo per sistemi di puntamento radar, torrette e inseguimento optoelettronico.

Soluzioni per l'Automazione e Robotica: Calcolo e fornitura di riduttori epicicloidali con giochi angolari minimi per bracci robotici e tavole rotanti che richiedono ripetibilità millimetrica.

ADATTAMENTO E PERSONALIZZAZIONE DI PRODOTTI TRADIZIONALI

Configurazione su Misura: Modifica di alberi d'uscita, flange di collegamento, predisposizioni motore e layout di montaggio su riduttori epicicloidali, ortogonali e ad assi paralleli.

Trattamenti Superficiali Specifici: Applicazione di verniciature speciali, trattamenti anticorrosione o casse completamente in acciaio inox per i settori alimentare, farmaceutico o marino.

Lubrificazione Dedicata: Fornitura di riduttori dotati di oli sintetici per alte/basse temperature o lubrificanti certificati per uso alimentare (Food-grade).

CONTROLLO QUALITÀ E TRACCIABILITÀ TOTALE

Verifica e Metrologia: Controlli dimensionali stringenti sui profili dei denti degli ingranaggi e sulle tolleranze di accoppiamento per garantire la massima silenziosità e rendimento.

Tracciabilità dei Materiali: Gestione e fornitura di certificazioni complete sulle materie prime (certificati 3.1) e sui trattamenti termici effettuati, fondamentale per i settori Ferroviario, Militare e Spaziale.

Test e Collaudi: Possibilità di eseguire test di tenuta, prove di rumorosità e simulazioni di carico prima della consegna del gruppo di trasmissione.

ASSISTENZA POST-VENDITA E CONSULENZA APPLICATIVA

Problem Solving: Supporto tecnico rapido per la risoluzione di anomalie di funzionamento o per l'ottimizzazione di impianti esistenti (attività di revamping di vecchie trasmissioni).

Ricambistica Specialistica: Fornitura di ingranaggi, alberi scanalati e componenti di ricambio realizzati a disegno o a campione, anche per macchinari obsoleti.

INDICE DEL DOCUMENTO

Pack procedure SGSI

TERMINI IN USO

Termine	Definizione
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni.
Informazione	Dato o insieme di dati rilevanti per l'organizzazione, indipendentemente dal formato o supporto.
Asset	Qualsiasi risorsa informativa, organizzativa, tecnologica, fisica o di supporto rilevante per il SGSI.
Rischio	Effetto dell'incertezza sugli obiettivi, valutato in termini di probabilità e impatto.
Controllo	Misura organizzativa, fisica o tecnica adottata per modificare o presidiare il rischio.
Trattamento del rischio	Decisione e insieme di azioni per mitigare, trasferire, evitare o accettare un rischio.
SoA	Statement of Applicability: documento che riporta i controlli applicabili, il relativo stato e la giustificazione.
Parte interessata	Soggetto interno o esterno che può influenzare, essere influenzato o percepirsi influenzato dal SGSI.

PACK PROCEDURE SGSI

Le procedure riportate di seguito definiscono i controlli operativi minimi per la gestione del SGSI.

PROC-BCK-001 - Backup e ripristino

Procedura Backup e ripristino

Scopo

Stabilire regole operative coerenti con il SGSI di RIDUTTORI ITALIA S.R.L..

Campo di applicazione

Riferimenti al contesto

Struttura Organizzativa e Governance

Modello Organizzativo: Struttura snella e fortemente centralizzata attorno alla Direzione Generale, che garantisce rapidità decisionale ma presenta un'alta dipendenza da figure chiave (Key Man Risk).

Flussi Informativi: La comunicazione interna è prevalentemente diretta. È in corso di formalizzazione un comitato/funzione per la Sicurezza delle Informazioni (SGSI) per coordinare le decisioni OT con la Direzione.

Ruoli e Responsabilità (Matrice RASCI in ambito Sicurezza)

Direzione Generale: Promuove e approva le politiche del SGSI, definisce i livelli di rischio accettabili.

Ufficio Tecnico / R&D: Custode della proprietà intellettuale (disegni 2D/3D, modelli FEM, calcoli cinematici). Ha la responsabilità di garantire la riservatezza dei progetti dei clienti.

Produzione e Controllo Qualità: Responsabili dell'integrità dei dati di produzione (report di collaudo, dati del banco prova).

Sistemi Informativi (OT in Outsourcing): Gestione operativa della rete aziendale, dei backup, dei log e della business continuity.

Processi Aziendali Chiave

Progettazione e Calcolo Meccanico: Processo ad alto valore aggiunto basato su software specialistici . Genera il patrimonio informativo critico dell'azienda.

Pianificazione e Produzione (Officina): I dati critici includono i cicli di lavoro e le varie fasi.

Montaggio e Collaudo (Banco Prova): fase in cui vengono raccolti dati prestazionali, termografici e vibrazionali dei riduttori. La manipolazione o la perdita di questi dati inficia la certificazione del prodotto.

Gestione Commerciale e Procurement: Gestione di contratti, accordi di riservatezza (NDA) con i clienti e specifiche tecniche fornite ai subfornitori (trattamenti termici, fusioni).

Strumenti, Tecnologie e Asset Informativi

Software di Progettazione e Ingegneria: Licenze e file sorgente CAD/CAE e software di calcolo per ingranaggeria.

Infrastruttura IT Core: Sistema ERP per la gestione aziendale, server di file sharing interno, posta elettronica aziendale, sistemi di backup (locali e cloud).

Competenze e Consapevolezza (Awareness)

Competenze Tecniche: Elevato know-how ingegneristico e meccanico del personale, che rappresenta il core

business aziendale.

Competenze IT/Cybersecurity: Divario storico tra la forte competenza meccanica e la sensibilità alla sicurezza informatica. È identificata la necessità di formazione continua sul phishing, la gestione delle password e l'uso sicuro dei dispositivi

Dipendenze Interne

Interconnessione IOT: Un blocco della rete IT ferma l'officina.
gli uffici.

Dipendenza Ufficio Tecnico - Produzione: La supply chain interna si basa sulla disponibilità immediata e sicura delle distinte base (BOM) e dei disegni aggiornati.

Criticità Interne (Punti di Debolezza da Mitigare)

Protezione del Know-How (IP): Rischio di esfiltrazione di disegni tecnici proprietari o personalizzati per clienti strategici (settori critici come difesa, spazio o ferroviario).

Cultura della Sicurezza: Resistenza culturale nell'adozione di misure di sicurezza rigide (es. autenticazione a due fattori, blocco schermo automatico in officina) percepite come un rallentamento della produzione.

Documentazione dei Processi: Molte procedure operative sono storicamente basate sulla prassi e non formalizzate; questo aumenta il rischio di errore umano in caso di sostituzione del personale.

Asset rilevanti

- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- Database clienti (Database)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)
- PC e laptop dipendenti (Endpoint)
- Server / infrastruttura virtuale (Infrastruttura)
- Sito web aziendale (Sito web)

Rischi rilevanti

- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]
- Database clienti: Accesso non autorizzato ai dati [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- PC e laptop dipendenti: Smarrimento o furto del dispositivo [Alto]
- Asset: Accesso non autorizzato [Medio]

Controlli / SoA correlati

- A.5.1 Politiche per la sicurezza delle informazioni (implemented)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato

- Mitigare: Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità

La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative

1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-CLS-001 - Classificazione delle informazioni

Procedura Classificazione delle informazioni

Scopo

Stabilire regole operative coerenti con il SGSI di RIDUTTORI ITALIA S.R.L..

Campo di applicazione

Riferimenti al contesto

Struttura Organizzativa e Governance

Modello Organizzativo: Struttura snella e fortemente centralizzata attorno alla Direzione Generale, che garantisce rapidità decisionale ma presenta un'alta dipendenza da figure chiave (Key Man Risk).

Flussi Informativi: La comunicazione interna è prevalentemente diretta. È in corso di formalizzazione un comitato/funzione per la Sicurezza delle Informazioni (SGSI) per coordinare le decisioni OT con la Direzione.

Ruoli e Responsabilità (Matrice RASCI in ambito Sicurezza)

Direzione Generale: Promuove e approva le politiche del SGSI, definisce i livelli di rischio accettabili.

Ufficio Tecnico / R&D: Custode della proprietà intellettuale (disegni 2D/3D, modelli FEM, calcoli cinematici). Ha la responsabilità di garantire la riservatezza dei progetti dei clienti.

Produzione e Controllo Qualità: Responsabili dell'integrità dei dati di produzione (report di collaudo, dati del banco prova).

Sistemi Informativi (OT in Outsourcing): Gestione operativa della rete aziendale, dei backup, dei log e della business continuity.

Processi Aziendali Chiave

Progettazione e Calcolo Meccanico: Processo ad alto valore aggiunto basato su software specialistici . Genera il patrimonio informativo critico dell'azienda.

Pianificazione e Produzione (Officina): I dati critici includono i cicli di lavoro e le varie fasi.

Montaggio e Collaudo (Banco Prova): fase in cui vengono raccolti dati prestazionali, termografici e vibrazionali dei riduttori. La manipolazione o la perdita di questi dati inficia la certificazione del prodotto.

Gestione Commerciale e Procurement: Gestione di contratti, accordi di riservatezza (NDA) con i clienti e specifiche tecniche fornite ai subfornitori (trattamenti termici, fusioni).

Strumenti, Tecnologie e Asset Informativi

Software di Progettazione e Ingegneria: Licenze e file sorgente CAD/CAE e software di calcolo per ingranaggeria.

Infrastruttura IT Core: Sistema ERP per la gestione aziendale, server di file sharing interno, posta elettronica aziendale, sistemi di backup (locali e cloud).

Competenze e Consapevolezza (Awareness)

Competenze Tecniche: Elevato know-how ingegneristico e meccanico del personale, che rappresenta il core

business aziendale.

Competenze IT/Cybersecurity: Divario storico tra la forte competenza meccanica e la sensibilità alla sicurezza informatica. È identificata la necessità di formazione continua sul phishing, la gestione delle password e l'uso sicuro dei dispositivi

Dipendenze Interne

Interconnessione IOT: Un blocco della rete IT ferma l'officina.
gli uffici.

Dipendenza Ufficio Tecnico - Produzione: La supply chain interna si basa sulla disponibilità immediata e sicura delle distinte base (BOM) e dei disegni aggiornati.

Criticità Interne (Punti di Debolezza da Mitigare)

Protezione del Know-How (IP): Rischio di esfiltrazione di disegni tecnici proprietari o personalizzati per clienti strategici (settori critici come difesa, spazio o ferroviario).

Cultura della Sicurezza: Resistenza culturale nell'adozione di misure di sicurezza rigide (es. autenticazione a due fattori, blocco schermo automatico in officina) percepite come un rallentamento della produzione.

Documentazione dei Processi: Molte procedure operative sono storicamente basate sulla prassi e non formalizzate; questo aumenta il rischio di errore umano in caso di sostituzione del personale.

Asset rilevanti

- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- Database clienti (Database)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)
- PC e laptop dipendenti (Endpoint)
- Server / infrastruttura virtuale (Infrastruttura)
- Sito web aziendale (Sito web)

Rischi rilevanti

- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]
- Database clienti: Accesso non autorizzato ai dati [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- PC e laptop dipendenti: Smarrimento o furto del dispositivo [Alto]
- Asset: Accesso non autorizzato [Medio]

Controlli / SoA correlati

- A.5.1 Politiche per la sicurezza delle informazioni (implemented)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato

- Mitigare: Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità

La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative

1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-BCP-001 - Continuità operativa e continuità ICT

Procedura Continuità operativa e continuità ICT

Scopo

Stabilire regole operative coerenti con il SGSI di RIDUTTORI ITALIA S.R.L..

Campo di applicazione

Riferimenti al contesto

Struttura Organizzativa e Governance

Modello Organizzativo: Struttura snella e fortemente centralizzata attorno alla Direzione Generale, che garantisce rapidità decisionale ma presenta un'alta dipendenza da figure chiave (Key Man Risk).

Flussi Informativi: La comunicazione interna è prevalentemente diretta. È in corso di formalizzazione un comitato/funzione per la Sicurezza delle Informazioni (SGSI) per coordinare le decisioni OT con la Direzione.

Ruoli e Responsabilità (Matrice RASCI in ambito Sicurezza)

Direzione Generale: Promuove e approva le politiche del SGSI, definisce i livelli di rischio accettabili.

Ufficio Tecnico / R&D: Custode della proprietà intellettuale (disegni 2D/3D, modelli FEM, calcoli cinematici). Ha la responsabilità di garantire la riservatezza dei progetti dei clienti.

Produzione e Controllo Qualità: Responsabili dell'integrità dei dati di produzione (report di collaudo, dati del banco prova).

Sistemi Informativi (OT in Outsourcing): Gestione operativa della rete aziendale, dei backup, dei log e della business continuity.

Processi Aziendali Chiave

Progettazione e Calcolo Meccanico: Processo ad alto valore aggiunto basato su software specialistici . Genera il patrimonio informativo critico dell'azienda.

Pianificazione e Produzione (Officina): I dati critici includono i cicli di lavoro e le varie fasi.

Montaggio e Collaudo (Banco Prova): fase in cui vengono raccolti dati prestazionali, termografici e vibrazionali dei riduttori. La manipolazione o la perdita di questi dati inficia la certificazione del prodotto.

Gestione Commerciale e Procurement: Gestione di contratti, accordi di riservatezza (NDA) con i clienti e specifiche tecniche fornite ai subfornitori (trattamenti termici, fusioni).

Strumenti, Tecnologie e Asset Informativi

Software di Progettazione e Ingegneria: Licenze e file sorgente CAD/CAE e software di calcolo per ingranaggeria.

Infrastruttura IT Core: Sistema ERP per la gestione aziendale, server di file sharing interno, posta elettronica aziendale, sistemi di backup (locali e cloud).

Competenze e Consapevolezza (Awareness)

Competenze Tecniche: Elevato know-how ingegneristico e meccanico del personale, che rappresenta il core

business aziendale.

Competenze IT/Cybersecurity: Divario storico tra la forte competenza meccanica e la sensibilità alla sicurezza informatica. È identificata la necessità di formazione continua sul phishing, la gestione delle password e l'uso sicuro dei dispositivi

Dipendenze Interne

Interconnessione IOT: Un blocco della rete IT ferma l'officina.
gli uffici.

Dipendenza Ufficio Tecnico - Produzione: La supply chain interna si basa sulla disponibilità immediata e sicura delle distinte base (BOM) e dei disegni aggiornati.

Criticità Interne (Punti di Debolezza da Mitigare)

Protezione del Know-How (IP): Rischio di esfiltrazione di disegni tecnici proprietari o personalizzati per clienti strategici (settori critici come difesa, spazio o ferroviario).

Cultura della Sicurezza: Resistenza culturale nell'adozione di misure di sicurezza rigide (es. autenticazione a due fattori, blocco schermo automatico in officina) percepite come un rallentamento della produzione.

Documentazione dei Processi: Molte procedure operative sono storicamente basate sulla prassi e non formalizzate; questo aumenta il rischio di errore umano in caso di sostituzione del personale.

Asset rilevanti

- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- Database clienti (Database)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)
- PC e laptop dipendenti (Endpoint)
- Server / infrastruttura virtuale (Infrastruttura)
- Sito web aziendale (Sito web)

Rischi rilevanti

- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]
- Database clienti: Accesso non autorizzato ai dati [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- PC e laptop dipendenti: Smarrimento o furto del dispositivo [Alto]
- Asset: Accesso non autorizzato [Medio]

Controlli / SoA correlati

- A.5.1 Politiche per la sicurezza delle informazioni (implemented)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato

- Mitigare: Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità

La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative

1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-ACC-001 - Gestione accessi

Procedura Gestione accessi

Scopo

Stabilire regole operative coerenti con il SGSI di RIDUTTORI ITALIA S.R.L..

Campo di applicazione

Riferimenti al contesto

Struttura Organizzativa e Governance

Modello Organizzativo: Struttura snella e fortemente centralizzata attorno alla Direzione Generale, che garantisce rapidità decisionale ma presenta un'alta dipendenza da figure chiave (Key Man Risk).

Flussi Informativi: La comunicazione interna è prevalentemente diretta. È in corso di formalizzazione un comitato/funzione per la Sicurezza delle Informazioni (SGSI) per coordinare le decisioni OT con la Direzione.

Ruoli e Responsabilità (Matrice RASCI in ambito Sicurezza)

Direzione Generale: Promuove e approva le politiche del SGSI, definisce i livelli di rischio accettabili.

Ufficio Tecnico / R&D: Custode della proprietà intellettuale (disegni 2D/3D, modelli FEM, calcoli cinematici). Ha la responsabilità di garantire la riservatezza dei progetti dei clienti.

Produzione e Controllo Qualità: Responsabili dell'integrità dei dati di produzione (report di collaudo, dati del banco prova).

Sistemi Informativi (OT in Outsourcing): Gestione operativa della rete aziendale, dei backup, dei log e della business continuity.

Processi Aziendali Chiave

Progettazione e Calcolo Meccanico: Processo ad alto valore aggiunto basato su software specialistici . Genera il patrimonio informativo critico dell'azienda.

Pianificazione e Produzione (Officina): I dati critici includono i cicli di lavoro e le varie fasi.

Montaggio e Collaudo (Banco Prova): fase in cui vengono raccolti dati prestazionali, termografici e vibrazionali dei riduttori. La manipolazione o la perdita di questi dati inficia la certificazione del prodotto.

Gestione Commerciale e Procurement: Gestione di contratti, accordi di riservatezza (NDA) con i clienti e specifiche tecniche fornite ai subfornitori (trattamenti termici, fusioni).

Strumenti, Tecnologie e Asset Informativi

Software di Progettazione e Ingegneria: Licenze e file sorgente CAD/CAE e software di calcolo per ingranaggeria.

Infrastruttura IT Core: Sistema ERP per la gestione aziendale, server di file sharing interno, posta elettronica aziendale, sistemi di backup (locali e cloud).

Competenze e Consapevolezza (Awareness)

Competenze Tecniche: Elevato know-how ingegneristico e meccanico del personale, che rappresenta il core

business aziendale.

Competenze IT/Cybersecurity: Divario storico tra la forte competenza meccanica e la sensibilità alla sicurezza informatica. È identificata la necessità di formazione continua sul phishing, la gestione delle password e l'uso sicuro dei dispositivi

Dipendenze Interne

Interconnessione IOT: Un blocco della rete IT ferma l'officina.
gli uffici.

Dipendenza Ufficio Tecnico - Produzione: La supply chain interna si basa sulla disponibilità immediata e sicura delle distinte base (BOM) e dei disegni aggiornati.

Criticità Interne (Punti di Debolezza da Mitigare)

Protezione del Know-How (IP): Rischio di esfiltrazione di disegni tecnici proprietari o personalizzati per clienti strategici (settori critici come difesa, spazio o ferroviario).

Cultura della Sicurezza: Resistenza culturale nell'adozione di misure di sicurezza rigide (es. autenticazione a due fattori, blocco schermo automatico in officina) percepite come un rallentamento della produzione.

Documentazione dei Processi: Molte procedure operative sono storicamente basate sulla prassi e non formalizzate; questo aumenta il rischio di errore umano in caso di sostituzione del personale.

Asset rilevanti

- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- Database clienti (Database)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)
- PC e laptop dipendenti (Endpoint)
- Server / infrastruttura virtuale (Infrastruttura)
- Sito web aziendale (Sito web)

Rischi rilevanti

- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]
- Database clienti: Accesso non autorizzato ai dati [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- PC e laptop dipendenti: Smarrimento o furto del dispositivo [Alto]
- Asset: Accesso non autorizzato [Medio]

Controlli / SoA correlati

- A.5.1 Politiche per la sicurezza delle informazioni (implemented)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato

- Mitigare: Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità

La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative

1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-AST-001 - Gestione asset informativi

Procedura Gestione asset informativi

Scopo

Stabilire regole operative coerenti con il SGSI di RIDUTTORI ITALIA S.R.L..

Campo di applicazione

Riferimenti al contesto

Struttura Organizzativa e Governance

Modello Organizzativo: Struttura snella e fortemente centralizzata attorno alla Direzione Generale, che garantisce rapidità decisionale ma presenta un'alta dipendenza da figure chiave (Key Man Risk).

Flussi Informativi: La comunicazione interna è prevalentemente diretta. È in corso di formalizzazione un comitato/funzione per la Sicurezza delle Informazioni (SGSI) per coordinare le decisioni OT con la Direzione.

Ruoli e Responsabilità (Matrice RASCI in ambito Sicurezza)

Direzione Generale: Promuove e approva le politiche del SGSI, definisce i livelli di rischio accettabili.

Ufficio Tecnico / R&D: Custode della proprietà intellettuale (disegni 2D/3D, modelli FEM, calcoli cinematici). Ha la responsabilità di garantire la riservatezza dei progetti dei clienti.

Produzione e Controllo Qualità: Responsabili dell'integrità dei dati di produzione (report di collaudo, dati del banco prova).

Sistemi Informativi (OT in Outsourcing): Gestione operativa della rete aziendale, dei backup, dei log e della business continuity.

Processi Aziendali Chiave

Progettazione e Calcolo Meccanico: Processo ad alto valore aggiunto basato su software specialistici . Genera il patrimonio informativo critico dell'azienda.

Pianificazione e Produzione (Officina): I dati critici includono i cicli di lavoro e le varie fasi.

Montaggio e Collaudo (Banco Prova): fase in cui vengono raccolti dati prestazionali, termografici e vibrazionali dei riduttori. La manipolazione o la perdita di questi dati inficia la certificazione del prodotto.

Gestione Commerciale e Procurement: Gestione di contratti, accordi di riservatezza (NDA) con i clienti e specifiche tecniche fornite ai subfornitori (trattamenti termici, fusioni).

Strumenti, Tecnologie e Asset Informativi

Software di Progettazione e Ingegneria: Licenze e file sorgente CAD/CAE e software di calcolo per ingranaggeria.

Infrastruttura IT Core: Sistema ERP per la gestione aziendale, server di file sharing interno, posta elettronica aziendale, sistemi di backup (locali e cloud).

Competenze e Consapevolezza (Awareness)

Competenze Tecniche: Elevato know-how ingegneristico e meccanico del personale, che rappresenta il core

business aziendale.

Competenze IT/Cybersecurity: Divario storico tra la forte competenza meccanica e la sensibilità alla sicurezza informatica. È identificata la necessità di formazione continua sul phishing, la gestione delle password e l'uso sicuro dei dispositivi

Dipendenze Interne

Interconnessione IOT: Un blocco della rete IT ferma l'officina.
gli uffici.

Dipendenza Ufficio Tecnico - Produzione: La supply chain interna si basa sulla disponibilità immediata e sicura delle distinte base (BOM) e dei disegni aggiornati.

Criticità Interne (Punti di Debolezza da Mitigare)

Protezione del Know-How (IP): Rischio di esfiltrazione di disegni tecnici proprietari o personalizzati per clienti strategici (settori critici come difesa, spazio o ferroviario).

Cultura della Sicurezza: Resistenza culturale nell'adozione di misure di sicurezza rigide (es. autenticazione a due fattori, blocco schermo automatico in officina) percepite come un rallentamento della produzione.

Documentazione dei Processi: Molte procedure operative sono storicamente basate sulla prassi e non formalizzate; questo aumenta il rischio di errore umano in caso di sostituzione del personale.

Asset rilevanti

- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- Database clienti (Database)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)
- PC e laptop dipendenti (Endpoint)
- Server / infrastruttura virtuale (Infrastruttura)
- Sito web aziendale (Sito web)

Rischi rilevanti

- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]
- Database clienti: Accesso non autorizzato ai dati [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- PC e laptop dipendenti: Smarrimento o furto del dispositivo [Alto]
- Asset: Accesso non autorizzato [Medio]

Controlli / SoA correlati

- A.5.1 Politiche per la sicurezza delle informazioni (implemented)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato

- Mitigare: Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità

La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative

1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-SUP-001 - Gestione fornitori e terze parti

Procedura Gestione fornitori e terze parti

Scopo

Stabilire regole operative coerenti con il SGSI di RIDUTTORI ITALIA S.R.L..

Campo di applicazione

Riferimenti al contesto

Struttura Organizzativa e Governance

Modello Organizzativo: Struttura snella e fortemente centralizzata attorno alla Direzione Generale, che garantisce rapidità decisionale ma presenta un'alta dipendenza da figure chiave (Key Man Risk).

Flussi Informativi: La comunicazione interna è prevalentemente diretta. È in corso di formalizzazione un comitato/funzione per la Sicurezza delle Informazioni (SGSI) per coordinare le decisioni OT con la Direzione.

Ruoli e Responsabilità (Matrice RASCI in ambito Sicurezza)

Direzione Generale: Promuove e approva le politiche del SGSI, definisce i livelli di rischio accettabili.

Ufficio Tecnico / R&D: Custode della proprietà intellettuale (disegni 2D/3D, modelli FEM, calcoli cinematici). Ha la responsabilità di garantire la riservatezza dei progetti dei clienti.

Produzione e Controllo Qualità: Responsabili dell'integrità dei dati di produzione (report di collaudo, dati del banco prova).

Sistemi Informativi (OT in Outsourcing): Gestione operativa della rete aziendale, dei backup, dei log e della business continuity.

Processi Aziendali Chiave

Progettazione e Calcolo Meccanico: Processo ad alto valore aggiunto basato su software specialistici . Genera il patrimonio informativo critico dell'azienda.

Pianificazione e Produzione (Officina): I dati critici includono i cicli di lavoro e le varie fasi.

Montaggio e Collaudo (Banco Prova): fase in cui vengono raccolti dati prestazionali, termografici e vibrazionali dei riduttori. La manipolazione o la perdita di questi dati inficia la certificazione del prodotto.

Gestione Commerciale e Procurement: Gestione di contratti, accordi di riservatezza (NDA) con i clienti e specifiche tecniche fornite ai subfornitori (trattamenti termici, fusioni).

Strumenti, Tecnologie e Asset Informativi

Software di Progettazione e Ingegneria: Licenze e file sorgente CAD/CAE e software di calcolo per ingranaggeria.

Infrastruttura IT Core: Sistema ERP per la gestione aziendale, server di file sharing interno, posta elettronica aziendale, sistemi di backup (locali e cloud).

Competenze e Consapevolezza (Awareness)

Competenze Tecniche: Elevato know-how ingegneristico e meccanico del personale, che rappresenta il core

business aziendale.

Competenze IT/Cybersecurity: Divario storico tra la forte competenza meccanica e la sensibilità alla sicurezza informatica. È identificata la necessità di formazione continua sul phishing, la gestione delle password e l'uso sicuro dei dispositivi

Dipendenze Interne

Interconnessione IOT: Un blocco della rete IT ferma l'officina.
gli uffici.

Dipendenza Ufficio Tecnico - Produzione: La supply chain interna si basa sulla disponibilità immediata e sicura delle distinte base (BOM) e dei disegni aggiornati.

Criticità Interne (Punti di Debolezza da Mitigare)

Protezione del Know-How (IP): Rischio di esfiltrazione di disegni tecnici proprietari o personalizzati per clienti strategici (settori critici come difesa, spazio o ferroviario).

Cultura della Sicurezza: Resistenza culturale nell'adozione di misure di sicurezza rigide (es. autenticazione a due fattori, blocco schermo automatico in officina) percepite come un rallentamento della produzione.

Documentazione dei Processi: Molte procedure operative sono storicamente basate sulla prassi e non formalizzate; questo aumenta il rischio di errore umano in caso di sostituzione del personale.

Asset rilevanti

- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- Database clienti (Database)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)
- PC e laptop dipendenti (Endpoint)
- Server / infrastruttura virtuale (Infrastruttura)
- Sito web aziendale (Sito web)

Rischi rilevanti

- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]
- Database clienti: Accesso non autorizzato ai dati [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- PC e laptop dipendenti: Smarrimento o furto del dispositivo [Alto]
- Asset: Accesso non autorizzato [Medio]

Controlli / SoA correlati

- A.5.1 Politiche per la sicurezza delle informazioni (implemented)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato

- Mitigare: Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità

La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative

1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-INC-001 - Gestione incidenti di sicurezza

Procedura Gestione incidenti di sicurezza

Scopo

Stabilire regole operative coerenti con il SGSI di RIDUTTORI ITALIA S.R.L..

Campo di applicazione

Riferimenti al contesto

Struttura Organizzativa e Governance

Modello Organizzativo: Struttura snella e fortemente centralizzata attorno alla Direzione Generale, che garantisce rapidità decisionale ma presenta un'alta dipendenza da figure chiave (Key Man Risk).

Flussi Informativi: La comunicazione interna è prevalentemente diretta. È in corso di formalizzazione un comitato/funzione per la Sicurezza delle Informazioni (SGSI) per coordinare le decisioni OT con la Direzione.

Ruoli e Responsabilità (Matrice RASCI in ambito Sicurezza)

Direzione Generale: Promuove e approva le politiche del SGSI, definisce i livelli di rischio accettabili.

Ufficio Tecnico / R&D: Custode della proprietà intellettuale (disegni 2D/3D, modelli FEM, calcoli cinematici). Ha la responsabilità di garantire la riservatezza dei progetti dei clienti.

Produzione e Controllo Qualità: Responsabili dell'integrità dei dati di produzione (report di collaudo, dati del banco prova).

Sistemi Informativi (OT in Outsourcing): Gestione operativa della rete aziendale, dei backup, dei log e della business continuity.

Processi Aziendali Chiave

Progettazione e Calcolo Meccanico: Processo ad alto valore aggiunto basato su software specialistici . Genera il patrimonio informativo critico dell'azienda.

Pianificazione e Produzione (Officina): I dati critici includono i cicli di lavoro e le varie fasi.

Montaggio e Collaudo (Banco Prova): fase in cui vengono raccolti dati prestazionali, termografici e vibrazionali dei riduttori. La manipolazione o la perdita di questi dati inficia la certificazione del prodotto.

Gestione Commerciale e Procurement: Gestione di contratti, accordi di riservatezza (NDA) con i clienti e specifiche tecniche fornite ai subfornitori (trattamenti termici, fusioni).

Strumenti, Tecnologie e Asset Informativi

Software di Progettazione e Ingegneria: Licenze e file sorgente CAD/CAE e software di calcolo per ingranaggeria.

Infrastruttura IT Core: Sistema ERP per la gestione aziendale, server di file sharing interno, posta elettronica aziendale, sistemi di backup (locali e cloud).

Competenze e Consapevolezza (Awareness)

Competenze Tecniche: Elevato know-how ingegneristico e meccanico del personale, che rappresenta il core

business aziendale.

Competenze IT/Cybersecurity: Divario storico tra la forte competenza meccanica e la sensibilità alla sicurezza informatica. È identificata la necessità di formazione continua sul phishing, la gestione delle password e l'uso sicuro dei dispositivi

Dipendenze Interne

Interconnessione IOT: Un blocco della rete IT ferma l'officina.
gli uffici.

Dipendenza Ufficio Tecnico - Produzione: La supply chain interna si basa sulla disponibilità immediata e sicura delle distinte base (BOM) e dei disegni aggiornati.

Criticità Interne (Punti di Debolezza da Mitigare)

Protezione del Know-How (IP): Rischio di esfiltrazione di disegni tecnici proprietari o personalizzati per clienti strategici (settori critici come difesa, spazio o ferroviario).

Cultura della Sicurezza: Resistenza culturale nell'adozione di misure di sicurezza rigide (es. autenticazione a due fattori, blocco schermo automatico in officina) percepite come un rallentamento della produzione.

Documentazione dei Processi: Molte procedure operative sono storicamente basate sulla prassi e non formalizzate; questo aumenta il rischio di errore umano in caso di sostituzione del personale.

Asset rilevanti

- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- Database clienti (Database)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)
- PC e laptop dipendenti (Endpoint)
- Server / infrastruttura virtuale (Infrastruttura)
- Sito web aziendale (Sito web)

Rischi rilevanti

- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]
- Database clienti: Accesso non autorizzato ai dati [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- PC e laptop dipendenti: Smarrimento o furto del dispositivo [Alto]
- Asset: Accesso non autorizzato [Medio]

Controlli / SoA correlati

- A.5.1 Politiche per la sicurezza delle informazioni (implemented)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato

- Mitigare: Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità

La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative

1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-VUL-001 - Gestione vulnerabilità

Procedura Gestione vulnerabilità

Scopo

Stabilire regole operative coerenti con il SGSI di RIDUTTORI ITALIA S.R.L..

Campo di applicazione

Riferimenti al contesto

Struttura Organizzativa e Governance

Modello Organizzativo: Struttura snella e fortemente centralizzata attorno alla Direzione Generale, che garantisce rapidità decisionale ma presenta un'alta dipendenza da figure chiave (Key Man Risk).

Flussi Informativi: La comunicazione interna è prevalentemente diretta. È in corso di formalizzazione un comitato/funzione per la Sicurezza delle Informazioni (SGSI) per coordinare le decisioni OT con la Direzione.

Ruoli e Responsabilità (Matrice RASCI in ambito Sicurezza)

Direzione Generale: Promuove e approva le politiche del SGSI, definisce i livelli di rischio accettabili.

Ufficio Tecnico / R&D: Custode della proprietà intellettuale (disegni 2D/3D, modelli FEM, calcoli cinematici). Ha la responsabilità di garantire la riservatezza dei progetti dei clienti.

Produzione e Controllo Qualità: Responsabili dell'integrità dei dati di produzione (report di collaudo, dati del banco prova).

Sistemi Informativi (OT in Outsourcing): Gestione operativa della rete aziendale, dei backup, dei log e della business continuity.

Processi Aziendali Chiave

Progettazione e Calcolo Meccanico: Processo ad alto valore aggiunto basato su software specialistici . Genera il patrimonio informativo critico dell'azienda.

Pianificazione e Produzione (Officina): I dati critici includono i cicli di lavoro e le varie fasi.

Montaggio e Collaudo (Banco Prova): fase in cui vengono raccolti dati prestazionali, termografici e vibrazionali dei riduttori. La manipolazione o la perdita di questi dati inficia la certificazione del prodotto.

Gestione Commerciale e Procurement: Gestione di contratti, accordi di riservatezza (NDA) con i clienti e specifiche tecniche fornite ai subfornitori (trattamenti termici, fusioni).

Strumenti, Tecnologie e Asset Informativi

Software di Progettazione e Ingegneria: Licenze e file sorgente CAD/CAE e software di calcolo per ingranaggia.

Infrastruttura IT Core: Sistema ERP per la gestione aziendale, server di file sharing interno, posta elettronica aziendale, sistemi di backup (locali e cloud).

Competenze e Consapevolezza (Awareness)

Competenze Tecniche: Elevato know-how ingegneristico e meccanico del personale, che rappresenta il core

business aziendale.

Competenze IT/Cybersecurity: Divario storico tra la forte competenza meccanica e la sensibilità alla sicurezza informatica. È identificata la necessità di formazione continua sul phishing, la gestione delle password e l'uso sicuro dei dispositivi

Dipendenze Interne

Interconnessione IOT: Un blocco della rete IT ferma l'officina.
gli uffici.

Dipendenza Ufficio Tecnico - Produzione: La supply chain interna si basa sulla disponibilità immediata e sicura delle distinte base (BOM) e dei disegni aggiornati.

Criticità Interne (Punti di Debolezza da Mitigare)

Protezione del Know-How (IP): Rischio di esfiltrazione di disegni tecnici proprietari o personalizzati per clienti strategici (settori critici come difesa, spazio o ferroviario).

Cultura della Sicurezza: Resistenza culturale nell'adozione di misure di sicurezza rigide (es. autenticazione a due fattori, blocco schermo automatico in officina) percepite come un rallentamento della produzione.

Documentazione dei Processi: Molte procedure operative sono storicamente basate sulla prassi e non formalizzate; questo aumenta il rischio di errore umano in caso di sostituzione del personale.

Asset rilevanti

- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- Database clienti (Database)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)
- PC e laptop dipendenti (Endpoint)
- Server / infrastruttura virtuale (Infrastruttura)
- Sito web aziendale (Sito web)

Rischi rilevanti

- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]
- Database clienti: Accesso non autorizzato ai dati [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- PC e laptop dipendenti: Smarrimento o furto del dispositivo [Alto]
- Asset: Accesso non autorizzato [Medio]

Controlli / SoA correlati

- A.5.1 Politiche per la sicurezza delle informazioni (implemented)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (implemented)
- A.5.7 Threat intelligence (in_progress)
- A.5.9 Inventario degli asset informativi (implemented)
- A.5.10 Uso accettabile degli asset (implemented)
- A.5.12 Classificazione delle informazioni (implemented)
- A.5.15 Controllo degli accessi (implemented)
- A.5.18 Diritti di accesso (implemented)

Piano di trattamento collegato

- Mitigare: Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per asset coinvolto, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.

Responsabilità

La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative

1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.