[IHFA_Cybersecurity]

[Public]

[Politica di Sicurezza delle Informazioni]

IACOBUCCI HF Aerospace SpA
Road SC ASI 1/S nos. 16-18 - 03013 Ferentino (FR) - ITALY
Tel: +39.0775.39251; Fax: +39.0775.390009 - www.iacobucci.aero

Revisions

Rev	Data	Causale	Editato	Verificato	Approvato
1	07/2023	Prima emissione	Gyala	Iacobucci	Iacobucci

Modifiche delle pagine

PAGINE	REV.	DATA

ALL.	REV.	DATE

SOMMARIO

1. DICHIARAZIONE DI PRINCIPIO 5
2. ASPETTI GENERALI 6
2.1 Esigenza di una Politica della Sicurezza delle Informazioni 6
3. IMPEGNI 7
3.1 Scopo 8
3.2 Revisione, controllo e gestione dei cambiamenti 8
3.3 Riferimenti normativi 9
4. ORGANIZZAZIONE E RESPONSABILITÀ DELLA SICUREZZA 10
Obiettivo 10
Direzione 10
4.1 Comitato Direttivo per la Sicurezza (CDS) 10
4.2 Responsabili di Funzione 10
4.3 Responsabile dei sistemi informativi 11
4.4 Responsabile del sistema di gestione della sicurezza delle informazioni 12
4.5 Dipendenti e collaboratori 12
5. FLUSSI INFORMATIVI CON ALTRE ORGANIZZAZIONI 13
6. GESTIONE DEI RISCHI 14
6.1 Obiettivo e metodologia 14
7. CONTINUITÀ OPERATIVA (BUSINESS CONTINUITY) 15
7.1 Obiettivo 15
7.2 Requisiti per l'operatività 15
7.3 Elementi di pianificazione 15
8. SICUREZZA FISICA ED AMBIENTALE 16
8.1 Obiettivo 16
8.2 Sicurezza delle aree 16
8.3 Sicurezza dei locali 16
8.4 Controllo accessi ai locali 16
9. CONTROLLO DEGLI ACCESSI LOGICI 17
9.1 Obiettivo 17

9.2 Accesso ai sistemi ed alle applicazioni..... 17

10. SICUREZZA DELLE RETI E DELLE COMUNICAZIONI..... 18

11. GESTIONE DEGLI INCIDENTI..... 19

1. DICHIARAZIONE DI PRINCIPIO

La Politica di Sicurezza delle Informazioni in Iacobucci HF Aerospace S.p.A. ha l'obiettivo di proteggere gli asset informativi dalle minacce, siano esse organizzative, tecnologiche, interne o esterne, accidentali o intenzionali.

A tal fine Iacobucci HF Aerospace S.p.A. approva il presente documento finalizzato a:

- garantire la riservatezza delle informazioni;
- mantenere l'integrità delle informazioni;
- assicurare la disponibilità dei servizi informatici;
- rispettare i requisiti normativi, legislativi e le regole interne;
- formare il personale sulla sicurezza delle informazioni;
- tenere traccia ed analizzare qualsiasi incidente, reale o presunto, che interessi la sicurezza delle informazioni;
- stabilire regole, elaborare piani e adottare misure per attuare una sempre più efficace politica di sicurezza delle Informazioni;

ed inoltre lo scopo è anche quello di:

- indicare la Direzione quale responsabile della attuazione della presente Politica;
- stabilire che i Responsabili di Posizioni Organizzative siano responsabili dell'applicazione e del rispetto della Politica di Sicurezza delle Informazioni;
- assegnare ad ogni dipendente e/o collaboratore la responsabilità per il rispetto della Politica di Sicurezza delle Informazioni.

2. ASPETTI GENERALI

La Politica di Sicurezza delle Informazioni di Iacobucci HF Aerospace S.p.A. è attuata per proteggere ad un livello ottimale e ad un costo compatibile con le nostre specificità, il Sistema di Gestione delle Informazioni, da eventi intesi come minacce o incidenti, esterni e/o interni, oggettivi e/o soggettivi, che possono compromettere riservatezza, integrità e disponibilità delle informazioni durante tutti i processi aziendali.

Lo scopo di questo documento è indicare le esigenze, gli obiettivi, le finalità, ed i modelli organizzativi della strategia di sicurezza che Iacobucci HF Aerospace S.p.A. intende perseguire, al fine di orientare lo sviluppo, la gestione, il controllo dello stesso.

2.1 ESIGENZA DI UNA POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

Il Patrimonio Informativo Aziendale rappresenta la risorsa principale per gestire correttamente le relazioni con i Clienti, per pianificare l'innovazione continua dell'offerta e garantire la qualità del servizio di Iacobucci HF Aerospace S.p.A. alla propria clientela; come tale, esso deve essere adeguatamente tutelato con un costante bilanciamento fra il livello di rischio accettato ed il corrispondente grado di protezione richiesto, coniugando correttamente l'esigenza di tutela del valore delle informazioni con la necessità di assicurare l'efficienza, l'efficacia e la continuità dei processi di business.

Le informazioni sono sempre più gestite in forma elettronica ed i sistemi vengono utilizzati da un numero crescente di stakeholder: questo, se da un lato consente una loro migliore accessibilità e disponibilità, dall'altro determina profondi e rapidi mutamenti degli scenari di rischio che richiedono la presenza di misure e strumenti idonei per rendere sicure le informazioni, garantendo la loro salvaguardia anche in risposta a una crescente domanda di sicurezza da parte della clientela.

In un simile contesto, Iacobucci HF Aerospace S.p.A. governa la Sicurezza del patrimonio Informativo aziendale nel rispetto e sulla base di standard riconosciuti, metodologie consolidate, obbligazioni contrattuali, Leggi e Regolamenti, richieste cogenti derivanti da audit di terze parti e operazioni di due diligence.

Tuttavia, la sicurezza delle informazioni è una responsabilità gestionale, e non un fattore esclusivamente tecnologico. Con questa convinzione accompagnata dall'esigenza costante di ricerca di nuove strategie di mercato volte a dare garanzie, non soltanto sulla qualità dei servizi erogati, ma anche sulle modalità di trattamento delle informazioni riguardanti clienti, fornitori e altre parti interessate, oltre che della propria struttura organizzativa, Iacobucci HF Aerospace S.p.A. ha deciso di implementare un Sistema di Gestione per la Sicurezza delle Informazioni modellato sulla base dello standard UNI CEI ISO/IEC 27001:2017.

3. IMPEGNI

Tutto ciò premesso, Iacobucci HF Aerospace S.p.A., nel rispetto dei requisiti cogenti e in particolare della normativa vigente in merito alla sicurezza delle informazioni e dei correlati sistemi informativi, si impegna ad assicurare che:

- Le informazioni siano protette da accessi non autorizzati, anche ricorrendo alla crittografia di dati e comunicazioni, nel rispetto della riservatezza e siano disponibili agli utenti autorizzati quando ne hanno bisogno, essendo questo un aspetto cardine del perimetro del SGSI;
- Le informazioni siano opportunamente classificate, in quanto la classificazione delle informazioni costituisce l'attività basilare per la valutazione del rischio e quindi del potenziale danno ai dati e alle informazioni aziendali;
- Le informazioni non vengano rivelate a persone non autorizzate a seguito di azioni deliberate o per negligenza e, nel rispetto dell'integrità, siano salvaguardate da modifiche non autorizzate;
- Vengano predisposti piani per la continuità dell'attività aziendale e che tali piani siano il più possibile tenuti aggiornati e controllati;
- Il Personale riceva addestramento e aggiornamento sulla sicurezza delle informazioni;
- I Fornitori di tecnologie e di servizi correlati all' erogazione/gestione dei sistemi e dei servizi, in particolare per ciò che concerne gli acquisti di componenti informatici per i data center e per i clienti, siano accuratamente selezionati e monitorati con i medesimi criteri e principi che Iacobucci HF Aerospace S.p.A. adotta per i propri processi interni;
- Tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano riferiti al Responsabile del SGSI ed esaminati;
- Siano rispettati i requisiti contrattuali;
- Nel porre in opera quanto sopra descritto sussista sempre e lungo tutta la catena del valore un impegno al miglioramento continuo, sia della gestione delle informazioni e dei dati che nell'infrastruttura tecnologica e documentale a supporto.

Attraverso l'attuazione di questa politica Iacobucci HF Aerospace S.p.A. intende ottemperare all'impegno di conformità alla norma UNI CEI ISO/IEC 27001:2017 nonché conseguire e mantenere tale certificazione.

Per il conseguimento di tale obiettivo, la Direzione di Iacobucci HF Aerospace S.p.A. si impegna a far sì che la presente politica sia diffusa, compresa e attuata non solo dal personale interno, ma anche da stagisti, collaboratori esterni, consulenti, fornitori, con particolare attenzione agli outsourcer che siano in qualsiasi modo coinvolti con la sicurezza delle informazioni aziendali.

La Direzione di Iacobucci HF Aerospace S.p.A. si impegna infine a riesaminare regolarmente la presente Politica ed eventuali modifiche che la influenzino, per accertarsi che permanga idonea all'attività e alla capacità aziendale di soddisfare i Clienti, i Fornitori e le altre parti interessate.

3.1 SCOPO

Iacobucci HF Aerospace S.p.A. considera il sistema di gestione e le informazioni gestite, per il particolare rilievo che assumono per il perseguimento dei propri fini aziendali, parte integrante del proprio patrimonio. È obiettivo di assoluta priorità per Iacobucci HF Aerospace S.p.A. salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

In tale contesto si intende per:

Riservatezza la garanzia che una determinata informazione sia preservata da accessi impropri e sia utilizzata esclusivamente dai soggetti autorizzati.

Integrità la garanzia che ogni informazione sia realmente quella originariamente inserita nel sistema informatico e sia stata modificata in modo legittimo da soggetti autorizzati.

Disponibilità la garanzia di reperibilità dell'informazione in relazione alle esigenze di continuità di erogazione del servizio e di rispetto delle norme che ne impongono la conservazione sicura.

Autenticità la garanzia che l'informazione ricevuta corrisponda a quella generata dal soggetto o entità che l'ha trasmessa.

Iacobucci HF Aerospace S.p.A. pone a base della politica di tutela delle informazioni un'idonea Analisi dei Rischi di tutte le risorse (asset) che costituiscono il sistema di gestione delle informazioni, al fine di comprendere le vulnerabilità, di valutare le possibili minacce e di predisporre le necessarie contromisure.

3.2 REVISIONE, CONTROLLO E GESTIONE DEI CAMBIAMENTI

La Direzione Iacobucci HF Aerospace S.p.A. è responsabile della revisione periodica della Politica affinché sia allineata agli eventuali e significativi cambiamenti intervenuti nell'organizzazione e/o nelle tecnologie utilizzate per la protezione delle informazioni. Nel caso di cambiamenti significativi, questi verranno gestiti, con dei progetti specifici, documentati a cura di un Responsabile definito, secondo l'ambito di competenza.

3.3 RIFERIMENTI NORMATIVI

La materia della sicurezza delle informazioni è disciplinata dalla legislazione comunitaria e dalla legislazione italiana. Qui si riportano le norme più recenti e più importanti in materia di protezione dei diritti personali e le norme che si riferiscono in modo specifico al Sistema ISO 27001.

Normativa sulla protezione dei diritti personali

Decreto Legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (GU n.205 del 4-9-2018) Vigente al: 19-9-2018.

Legge n. 163 del 25/10/2017 in particolare articolo 13 Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017.

Regolamento 2016/679 del Parlamento europeo e del Consiglio, del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) pubblicato su GUUE del 4 maggio 2016, entrato in vigore il 24 maggio 2016, applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Decreto legislativo n. 196 del 30/06/2003 Codice in materia di protezione dei dati personali.

Normativa riferita alla certificazione ISO 27001 degli organismi pagatori

Reg. (CE) 11/03/2014, n. 907/2014 “Regolamento delegato della commissione che integra regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio per quanto riguarda gli organismi pagatori e altri organismi, la gestione finanziaria, la liquidazione dei conti, le cauzioni e l'uso dell'euro”.

Norma ISO 27001 che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.

Linee guida ISO 27002 che costituiscono una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001:2017 al fine di proteggere le risorse informative.

Linee guida ISO 27005 “Information technology — Security techniques — Information security risk management”; il loro scopo è fornire le linee guida per l’information security risk management, definendo dei metodi rigorosi per l’analisi del rischio e la relativa creazione di un piano di prevenzione/contenimento del rischio stesso.

4. ORGANIZZAZIONE E RESPONSABILITÀ DELLA SICUREZZA

L'organizzazione e responsabilità della sicurezza è relativa all'individuazione delle procedure dirette alla gestione e controllo delle misure di sicurezza adottate e si concretizza nell'individuazione di ruoli, funzioni e responsabilità coinvolte nella realizzazione e gestione del Sistema di Sicurezza delle Informazioni.

1.1.1 Obiettivo

Assicurare che i dirigenti ed i collaboratori, considerato che la sicurezza delle informazioni sia una responsabilità comune, siano adeguatamente informati e formati sul ruolo che possono svolgere al fine di minimizzare i rischi derivanti dalle minacce alla sicurezza del sistema di gestione delle informazioni.

1.1.2 Direzione

La Direzione è responsabile dei contenuti della Politica di Sicurezza delle Informazioni, della sua emanazione, attuazione ed aggiornamento. La Direzione si avvale del supporto tecnico ed organizzativo del Comitato Direttivo per la Sicurezza (CDS) per la definizione e attuazione della politica di sicurezza delle Informazione.

4.1 COMITATO DIRETTIVO PER LA SICUREZZA (CDS)

Il CDS (Comitato Direttivo per la Sicurezza) è l'organo decisionale in termini di politiche ed investimenti da sostenere e la sua composizione, definita in armonia all'organizzazione di Iacobucci HF Aerospace S.p.A., è descritta di seguito in questo paragrafo.

La partecipazione al CDS può essere ampliata di volta in volta qualora ci sia l'esigenza di esaminare temi specifici. Il CDS ha la funzione di supportare la Direzione nella ricerca e indicazione delle linee guida e delle migliori modalità di applicazione della Politica di Sicurezza delle Informazioni.

Il CDS è composto da:

- Direzione Aziendale
- Responsabile del sistema di gestione della sicurezza delle informazioni

Il CDS si riunisce con cadenza annuale, salvo necessità specifiche. In assenza di problematiche di sicurezza specifiche la riunione di Riesame di Direzione ha valenza di riunione annuale.

4.2 RESPONSABILI DI FUNZIONE

È responsabilità dei responsabili di funzione assicurarsi che:

a) i propri collaboratori
   - siano informati delle clausole di riservatezza facenti parte integrante del contratto di lavoro;
   - siano istruiti, tramite appositi corsi, previsti nel "*Piano annuale di Formazione*", circa la loro responsabilità rispetto alla sicurezza delle informazioni;
   - siano autorizzati all'accesso a sistemi o applicazioni o dati a seguito dei profili di autorizzazione definiti, coerenti con il ruolo e le attività svolte. La comunicazione per l'autorizzazione dei diritti di accesso viene effettuata nel rispetto delle procedure specifiche di accesso dei sistemi o applicazioni o dati;
   - siano addestrati all'uso dei sistemi di elaborazione all'uso dei quali sono stati autorizzati;
   - abbiano accesso e abbiano preso conoscenza delle politiche di sicurezza dell'informazione di Iacobucci HF Aerospace S.p.A.;

b) la documentazione dei processi inerenti alle attività di gestione dell'informazione sia aggiornata affinché tutte le attività di lavoro ritenute critiche possano svolgersi con continuità nel caso di indisponibilità dei collaboratori addetti;

c) i cambiamenti nelle mansioni o attività dei collaboratori (per esempio in caso di spostamenti organizzativi) che comportano variazioni del profilo d'accesso ai sistemi, applicazioni e dati, siano comunicati al Responsabile della Sicurezza delle informazioni, per variare o, se necessario, cancellare il profilo e le credenziali di accesso. La comunicazione deve essere effettuata nel rispetto delle procedure specifiche di accesso.

4.3 RESPONSABILE DEI SISTEMI INFORMATIVI

Cura lo sviluppo e la manutenzione evolutiva e correttiva dei sistemi informatici di Iacobucci HF Aerospace S.p.A.. È responsabile delle attività previste dalle procedure di back up ed accessi logici e delle attività inerenti alla business Continuity e al Disaster recovery di pertinenza.

Collabora nella gestione degli incidenti relativi alla sicurezza delle informazioni e nella gestione dei cambiamenti dell'infrastruttura tecnologica, valutandone i rischi ed i relativi impatti.

Come Amministratore di Sistema e per la Sicurezza delle Informazioni effettua la gestione, sotto il profilo degli aspetti di sicurezza, dei sistemi deputati al trattamento dati gestiti per conto del Titolare e secondo indicazione di quest'ultimo.

4.4 RESPONSABILE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Il Responsabile del sistema di gestione della sicurezza delle informazioni definisce, di concerto con CDS, il Piano di sviluppo del Sistema di Gestione per la Sicurezza delle Informazioni nel rispetto degli obiettivi della Iacobucci HF Aerospace S.p.A..

Il Responsabile fornisce inoltre idonea garanzia del pieno rispetto delle disposizioni vigenti in materia di sicurezza dell'informazione e dei suoi trattamenti. Organizza e sovrintende, in collaborazione con la Direzione, la realizzazione della "struttura di sicurezza" finalizzata a prevenire e proteggere gli asset informativi aziendali da minacce ed eventi critici al fine di garantire la continuità del core business aziendale.

4.5 DIPENDENTI E COLLABORATORI

Ogni dipendente o collaboratore, a qualunque titolo, è tenuto:

- al rispetto, nello svolgimento delle sue attività lavorative, delle misure di sicurezza delle informazioni e della applicazione delle relative procedure;
- a segnalare violazioni delle misure di sicurezza delle informazioni, adottando la procedura in vigore.

5. FLUSSI INFORMATIVI CON ALTRE ORGANIZZAZIONI

Gli scambi di informazioni con determinate strutture esterne, enti e/o organizzazioni pubbliche e private sono gestiti senza compromettere l'integrità e la riservatezza delle informazioni, garantendo la sicurezza e la correttezza dell'operatività dei sistemi di elaborazione e di comunicazione.

I flussi informativi con i soggetti esterni sono caratterizzati dalla conformità alle regole concordate al fine di preservare l'integrità, la riservatezza, l'autenticità delle informazioni scambiate e la sicurezza dei sistemi di elaborazione nel rispetto della normativa, nazionale e comunitaria, vigente.

6. GESTIONE DEI RISCHI

6.1 OBIETTIVO E METODOLOGIA

L'obiettivo dell'Analisi dei Rischi è identificare e contrastare le possibili minacce alla sicurezza dei sistemi e delle informazioni aziendali, al fine di predisporre adeguate misure di prevenzione e protezione.

L'Analisi dei Rischi è l'elemento principale da cui discendono tutte le attività di controllo, le Politiche in merito alla sicurezza e le procedure operative legate alla sicurezza delle informazioni.

A tale proposito Iacobucci HF Aerospace S.p.A. adotta una propria metodologia che le consente di:

- Analizzare e gerarchizzare i rischi e le opportunità nell'organizzazione (*Analisi a livello di processo di security: che cosa è accettabile e che cosa non lo è*);
- Valutare e pianificare azioni per affrontare i rischi (*evitare, eliminare o mitigare i rischi*);
- Attuare il piano definito (*Condurre le azioni*);
- Controllare l'efficacia delle azioni;
- Apprendere dall'esperienza (*Miglioramento continuo*).

L'Analisi dei Rischi viene condotta con cadenza periodica e regolare, a garanzia del permanere dell'efficacia delle misure di mitigazione identificate e attuate.

7. CONTINUITÀ OPERATIVA (BUSINESS CONTINUITY)

La responsabilità della "Continuità Operativa" è della Direzione che predispone il Business Continuity Plan - BCP, inteso come indicazione delle attività organizzative e tecnologiche, finalizzate alla continuità dei processi che concorrono alla missione di Iacobucci HF Aerospace S.p.A..

Nella predisposizione del suddetto Piano la Direzione si avvale del supporto tecnico ed organizzativo del Comitato Direttivo per la Sicurezza (CDS).

7.1 OBIETTIVO

L'obiettivo della Gestione della Continuità Operativa è assicurare la continuità dei processi/servizi essenziali dell'organizzazione (processi critici) ad un determinato livello di servizio, nell'eventualità di un evento disastroso.

7.2 REQUISITI PER L'OPERATIVITÀ

Iacobucci HF Aerospace S.p.A. mediante le precauzioni contenute nel BCP ritiene di poter contenere l'impatto di eventuali avvenimenti disastrosi, nell'ambito dei requisiti di ripristino definiti.

7.3 ELEMENTI DI PIANIFICAZIONE

Le metodologie che consentono di redigere, realizzare e mantenere un BCP sono diverse e fanno riferimento a standard emanati da importanti istituti internazionali. Gli elementi comuni sono:

- identificazione delle strutture di coordinamento della strategia di ripristino;
- valutazione dei risultati della Business Impact Analisys per l'individuazione dei processi e dei servizi critici e delle priorità di intervento;
- predisposizione delle procedure da effettuare in caso di attuazione del BCP;
- sviluppo, documentazione e verifica del BCP.

8. SICUREZZA FISICA ED AMBIENTALE

Costituisce la forma di tutela che attiene alla protezione dei sistemi di elaborazione delle informazioni e si manifesta con misure fisiche dirette a garantire i servizi di controllo contro accessi non autorizzati ai locali ove sono ubicati i sistemi di gestione dell'informazione, al fine di preservare l'integrità e la disponibilità dei sistemi di elaborazione dell'informazione di Iacobucci HF Aerospace S.p.A..

8.1 OBIETTIVO

Minimizzare gli impatti delle minacce ai sistemi di elaborazione delle informazioni dovuti a danni o intrusioni.

8.2 SICUREZZA DELLE AREE

Le aree che comprendono i locali ove risiedono i sistemi di gestione dell'informazione di Iacobucci HF Aerospace S.p.A. sono dotate di porte ad accesso controllato.

8.3 SICUREZZA DEI LOCALI

I locali sono dotati di sistemi atti a garantire e mantenere la sicurezza e l'integrità delle apparecchiature e degli impianti, al fine di evitare guasti che possono causare interruzione fisica al funzionamento delle attività.

8.4 CONTROLLO ACCESSI AI LOCALI

Tutti i sistemi e le apparecchiature di rete sono ubicati in edifici sicuri e con accesso vigilato. In particolare, l'area ove risiedono i sistemi server del sistema informativo presso il CED è identificata come "area ad accesso ristretto" e l'ammissione è consentita solo in presenza di personale interno autorizzato, come previsto dalle procedure interne.

9. CONTROLLO DEGLI ACCESSI LOGICI

9.1 OBIETTIVO

Impedire accessi non autorizzati tramite procedure di controllo, proteggere le informazioni e i sistemi di elaborazione e di comunicazione con misure tecnologiche e organizzative atte a garantire il controllo degli accessi, la qualità delle informazioni, nonché la loro riservatezza ed integrità.

9.2 ACCESSO AI SISTEMI ED ALLE APPLICAZIONI

Accesso alle applicazioni (autorizzazioni)

Iacobucci HF Aerospace S.p.A. definisce le autorizzazioni e le policy di accesso in relazione al ruolo in azienda e alle attività di pertinenza.

Iacobucci HF Aerospace S.p.A. adotta la profilazione degli utenti, sia interni che esterni, per la concessione della credenziale d'accesso alle applicazioni ed utilizza a tal fine una "procedura formale" mantenendo documentazione delle autorizzazioni concesse.

Il Responsabile della Sicurezza delle Informazioni controlla periodicamente, almeno una volta all'anno, la validità funzionale di tutte le autorizzazioni attive per l'accesso alle applicazioni di Iacobucci HF Aerospace S.p.A..

La revoca all'accesso ai sistemi di elaborazione delle informazioni di Iacobucci HF Aerospace S.p.A. viene attuata qualora decadano le caratteristiche di abilitazione di un utente.

10. SICUREZZA DELLE RETI E DELLE COMUNICAZIONI

Per garantire la sicurezza delle reti e delle comunicazioni occorre prevenire l'accesso alle reti e l'utilizzo illegale di informazioni da parte di soggetti non autorizzati al fine di preservare la riservatezza dei dati e la disponibilità del servizio.

Il "Disciplinare interno" contiene le raccomandazioni sulla sicurezza della rete interna, le regole per la navigazione in Internet e le indicazioni per l'uso appropriato della posta elettronica e la protezione contro il software malevolo.

11. GESTIONE DEGLI INCIDENTI

Un incidente, nell'ambito della sicurezza dell'informazione è un evento sospetto o una vulnerabilità tale da violare l'integrità, la riservatezza e/o la disponibilità delle applicazioni, dei dati e/o dei sistemi di elaborazione delle informazioni.

Tutti gli utenti devono attenersi alle indicazioni ricevute in materia di sicurezza delle informazioni e contenute nel "Disciplinare interno" e nella procedura di gestione incidenti per la sicurezza delle informazioni.

Tullio De Santis

IT, Security and Information Compliance Officer