Guida al fattore di rischio in ambito Aereonautico

Nel settore aeronautico, la protezione dei dati personali, delle specifiche tecniche, dei dati sensibili e della proprietà intellettuale è fondamentale per garantire sicurezza, conformità normativa e competitività sul mercato.
Data la complessità delle infrastrutture informatiche, oltre che dei sistemi e la rilevanza delle attività svolte, è opportuno adottare un approccio chiaro e esemplificativo nella valutazione del rischio legato al tema della privacy e della sicurezza aziendale.
Questo elaborato è una proposta metodologica per calcolare il fattore di rischio al contesto operativo specifico, tenendo in considerazione le fasi operative, le risorse strategiche e le normative di riferimento.

Definizioni Generali

Il primo passo per iniziare a comprendere l'argomento è definire la **Gestione del rischio**, immaginandolo come il cuore in un **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)**. L'obiettivo è proteggere la **riservatezza**, l'**integrità** e la **disponibilità** delle informazioni aziendali. Le fasi che articolano questo tema sono:

- **Valutazione dei Rischi**: Comprendere quali sono i rischi presenti in un'azienda che potrebbero esporla a pericoli.
- **Gestione dei Rischi:** Secondo la normativa I.S.O. 27001 essa rappresenta un approccio proattivo e sistematico per identificare, valutare e trattare i rischi legati alla sicurezza delle informazioni**;**
- **Identificazione del Rischio:** Riconoscere quali minacce (attacchi informatici, errori umani) e vulnerabilità potrebbero compromettere gli asset informativi (dati, server, software);
- **Analisi dei Rischi:** Valutare la probabilità che un rischio si verifichi e l'impatto che avrebbe sull'organizzazione;
- **Valutazione dei Rischi:** Confrontare i livelli di rischio calcolati per ottenere una priorità e decidere quali tipi di rischio devono essere trattati per primi.

In Italia, gli ambiti di applicazione della gestione del rischio sono distinti nel **Codice Privacy italiano** (D.lgs. 196/2003, modificato dal D.lgs. 101/2018) che tutela e riordina le disposizioni presenti. A seguito è stato introdotto a carattere europeo il Regolamento UE 2016/679 noto come **G.P.D.R**. che non solo amplia il raggio d'azione del Codice Privacy Nazionale ma controlla l'applicabilità negli Stati membri dell'Unione Europea disciplinando i ruoli, i trattamenti specifici, le sanzioni penali applicabili e le regole deontologiche utili per la tutela della privacy.

I soggetti interessati nel G.P.D.R. sono di seguito elencati:

- **Interessato**: la persona fisica cui si riferiscono i dati personali;
- **Titolare del Trattamento (Data Controller)**: il soggetto che determina le finalità e i mezzi del trattamento dei dati;
- **Responsabile del Trattamento (Data Processor):** colui che tratta i dati personali per conto del Titolare
- **Responsabile della Protezione dei Dati (Data Protection Officer – D.P.O.):** figura professionale specializzata che ha il compito di **vigilare sull'osservanza del G.D.P.R.** all'interno dell'organizzazione
- **Autorità di Controllo**: l'autorità pubblica indipendente che vigila sull'applicazione del GDPR in ciascuno Stato membro.

Il G.P.D.R. prevede l'osservanza attraverso i soggetti sopra menzionati a delle regole che mirano alla tutela della privacy in particolare:

- **Nomina di un Responsabile della protezione dei dati (D.P.O.):** incaricato a garantire il rispetto del Regolamento, informare e consigliare il titolare del trattamento, fornire consulenza nella valutazione d'impatto sulla protezione dei dati (D.P.I.A.), controllarne l'esecuzione e fungere da punto di contatto con il Garante per la protezione dei dati personali per le questioni relative al trattamento dei dati**;**
- **DPIA (Data Protection Impact Assessment):** strumento indispensabile per la valutazione della gestione del rischio, in un trattamento dati e utilizzato nel caso in cui un'analisi abbia portato al risultato di un **rischio elevato**, rispettando i punti all'art. 35 e 36 del G.P.D.R.;
- **Formazione del personale:** con questa regola si pretende che i soggetti coinvolti nel trattamento dei dati siano adeguatamente informati sulle normative vigenti e sui diritti dei titolari dei dati;
- **Monitoraggio e audit**: Il G.P.D.R. impone verifiche regolari sui processi aziendali al fine di mantenere una costante conformità con le normative.

Normative e standard applicabili:

- **Codice Privacy italiano** (D.lgs. 196/2003, modificato dal D.lgs. 101/2018): normativa italiana per la tutela e il trattamento dei dati personali;
- **Regolamento UE 2016/679 (G.D.P.R.)**: riferimento europeo agli obblighi per la protezione dei dati personali dei dipendenti, dei clienti e dei fornitori.
- **E.A.S.A.[1] Cybersecurity Framework**: linee guida per la sicurezza informatica e protezione dei dati nel settore aeronautico.
- **I.C.A.O.[2]:** agenzia specializzata delle Nazioni Unite che stabilisce standard globali. L'Annesso 19 - Safety Management, fondamentale per l'implementazione dei Sistemi di Gestione della Sicurezza (SMS)

- **E.N.A.C**[3].: autorità italiana che applica e supervisiona l'implementazione delle normative E.A.S.A. e I.C.A.O. sul territorio nazionale
- **L.V.S.**[4] **& I.S.O./I.E.C. 27001**: standard interno aziendale per la gestione della sicurezza delle informazioni basato sulla normativa Internazionale I.S.O./I.E.C. 27001
- **D.lgs. 81/2008** riferimento legislativo relativo alla sicurezza fisica e organizzativa dei lavoratori.
- **Standard interni di sicurezza e politiche aziendali** configurate seguendo le linee guida dell'Agenzia europea per la sicurezza aerea (E.A.S.A.) e degli enti nazionali di certificazione.

Ambito operativo e rischi tipici nel mondo aeronautico

In un'azienda operante nel settore, gli scenari di rischio sulla privacy e sulla sicurezza includono:

- **Accesso non autorizzato** a dati tecnici relativi a progetti aeronautici (disegni aereonautici e meccanici 3D e 2D su CAD e Katja e relative specifiche su componenti e fasi lavorative);
- **Furto o perdita di dati riservati** dei clienti, del personale dipendente, dei progetti e brevetti aereonautici;
- **Attacchi informatici** su sistemi di ricerca e sviluppo, ingegneria di produzione, cicli residenti, compresi strumenti di manutenzione, gestione magazzino o documenti relativi al controllo qualità;
- **Interruzioni o rallentamenti operativi causati da malware o ransomware**, in grado di bloccare processi critici produttivi, controllo qualità e la consultazione di specifiche tecniche interne o del committente;
- **Violazioni dei protocolli di sicurezza** negli accessi a sistemi aventi dati sensibili, con eventuale clonazione o distruzione dei dati.

Guida al Calcolo del Fattore di Rischio:

A seguito dell'analisi dei diversi ambiti in cui possono manifestarsi rischi in grado di compromettere i dati delle aziende del settore, è possibile calcolare il **Fattore di Rischio (R)** partendo dalla **Formula Generale**. In conformità alla norma **I.S.O. 27001**, che definisce la **Gestione del Rischio** come un insieme di processi strutturati volti a identificare, analizzare, valutare e ridurre le minacce che possono compromettere la riservatezza, l'integrità e la disponibilità delle informazioni. Considerando le nozioni teoriche è possibile definire la **probabilità come la possibilità o la frequenza con cui**

una determinata minaccia può sfruttare una vulnerabilità e causare un incidente, mentre è possibile identificare l'**impatto ad una serie di conseguenze negative** che un'organizzazione subirebbe se un incidente di sicurezza ai verificasse. È possibile affidarsi a tabelle apposite per definire i due indici che verranno successivamente esplicate.

Formula generale:

$$R = P \times I$$

- **R** = fattore di rischio;
- **P** = probabilità che si verifichi una violazione o un incidente di sicurezza;
- **I** = impatto o gravità con annesse conseguenze aziendali.

Come evidenziato dalla Formula, il Fattore di Rischio corrisponde al prodotto di due indici, Probabilità e Impatto, la cui determinazione si effettua mediante i criteri appositi illustrati nel paragrafo successivo

Fattori di probabilità in ambito aereonautico:

L'indice delle Probabilità (P) deve essere scelto considerando diversi fattori:

- **L'infrastruttura informatica aziendale**, normalmente composta da una rete LAN interna connessa ad una rete centrale gestita internamente o esternamente al sito di riferimento, tramite la quale le postazioni operative e tecniche, comprese le macchine C.N.C., accedono in tempo reale a software, tool e part program indispensabili per le attività quotidiane.
- **Il livello di protezione** garantito con sistemi hardware e software, come antivirus e firewall industriali applicati su diramazioni di reti wireless con antenne point to point o sistemi cablati smistati su rack contenenti switch appositi, accedibili con autenticazione tramite userid e password conformi ai criteri di complessità (lunghezza minima, uso di caratteri speciali, maiuscole/minuscole e cifre).
- **Frequenza di aggiornamento** e patch di sicurezza dei sistemi operativi, antivirus e tool per i disegni meccanici o software per la consultazione di specifiche tecniche aereonautiche nelle rispettive postazioni di lavoro.
- Sulla **base storica** di esperienze interne (Pomigliano D'Arco 2017 Leonardo AereostruttureS.P.A.) è possibile aumentare il livello di sicurezza e ridurre il rischio di data breach.

Valutazione delle probabilità:

Dopo un'attenta analisi delle considerazioni rilevanti, è possibile selezionare l'indice di Probabilità **(P)** osservando la frequenza del verificarsi di un evento, come indicato nella seguente tabella:

	Raro	Improbabile	Probabile	Quasi Certo
Livello	**1**	**2**	**3**	**4**
Periodicità	**10 Anni**	**5 Anni**	**1 Mese**	**1 Settimana**

La tabella evidenzia come il livello di Impatto diminuisca all'aumentare dell'intervallo temporale tra gli eventi potenzialmente dannosi per la sicurezza.

Valutazione dell'Impatto

L'impatto viene valutato considerando le possibili conseguenze derivanti da:

- **Perdita o manipolazione dei dati tecnici**, con ripercussioni sulla qualità e sicurezza dei prodotti, oltre alla perdita di fiducia del cliente finale e compromissione dell'immagine etica aziendale.
- **Mancata conformità con il G.D.P.R.**, che portano a sanzioni elevate emesse dal Garante per la protezione dei dati, e danni all'immagine aziendale a carattere internazionale, con impatti negativi sui ricavi e sulla stabilità del business
- **Interruzione della produzione**, con ritardi sulle linee produttive e non conformità imposte dagli enti certificatori come: E.N.A.C. (Ente Nazionale Italiano per l'Aviazione Civile e Militare), E.A.S.A. (European Union Aviation Safety Agency), F.A.A. (Federal Aviation Administration).
- **Violazione delle misure di sicurezza hardware o software** con impatti sulla continuità operativa dei siti produttivi e/o ingegneristici, sull'integrità delle infrastrutture e sulla protezione dei dati sensibili.

Alla base dei vari scenari possibili è possibile determinare l'indice dell'Impatto **(I)** attraverso la seguente tabella:

Indice	Impatto	Descrizione
1	Basso	Dati non critici e danni limitati
2	Medio	Dati tecnici parzialmente compromessi con leggeri ritardi operativi
3	Alto	Dati essenziali alterati o distrutti con ritardi produttivi e di consegna significativi e sanzioni da parte del Garante per la protezione dei dati
4	Critico	Perdita di dati sensibili con annesse conseguenze legali e danni etici e reputazionali gravi

Matrice per il Calcolo del Fattore di Rischio

Con l'intersezione degli indici delle relative tabelle sopra indicate è possibile consultare la matrice del rischio e calcolare il fattore di rischio con la Formula generale evidenziata in precedenza:

Matrice Calcolo Rischio				
Probabilità / Impatto	RARO 1	IMPROBABILE 2	PROBABILE 3	QUASI CERTO 4
ALTO 4	4	8	12	16
MEDIO ALTO 3	3	6	9	12
MEDIO BASSO 2	2	4	6	8
BASSO 1	1	2	3	4

La legenda allegata descrive le peculiarità di ogni risultato in tabella, basandosi sul colore dello sfondo e sul range numerico, che rappresenta il risultato del prodotto degli indici **P** e **I**:

DENOMINAZIONE	RANGE NUMERICO	DESCRIZIONE
RISCHIO BASSO	$1 \leq R \leq 2$	La tipologia di violazione e la natura dei dati coinvolti non determinano criticità rilevanti in termini di perdita di integrità, riservatezza o disponibilità delle informazioni.
RISCHIO LIMITATO	$3 \leq R \leq 4$	Si colloca ad un livello superiore rispetto al rischio minimo, pur rimanendo al di sotto della soglia del rischio medio. È consigliabile un monitoraggio costante e l'adozione di misure preventive proporzionate, per evitare che possibili vulnerabilità evolvano in criticità significative.
RISCHIO MEDIO	$4 \leq R \leq 6$	A questo livello le conseguenze non possono più essere considerate trascurabili e richiedono un'attenzione significativa. È necessario adottare strategie preventive mirate pianificando interventi correttivi, in modo tale da evitare che le vulnerabilità individuate si trasformino in minacce concrete per l'integrità, la riservatezza e la disponibilità delle informazioni.
RISCHIO MEDIO-ALTO	$8 \leq R \leq 9$	I potenziali effetti, pur non essendo ancora critici, richiedono un'attenzione prioritaria. Risulta essenziale implementare interventi correttivi strutturati e strategie preventive efficaci, al fine di ridurre la probabilità che le vulnerabilità identificate si trasformino in minacce significative per l'integrità, la riservatezza e la disponibilità delle informazioni.
RISCHIO ALTO	$12 \leq R \leq 16$	Le conseguenze attese sono gravi e richiedono un'attenzione immediata. Occorre implementare interventi correttivi prioritari e strategie preventive rigorose, al fine di ridurre in maniera significativa la probabilità che le vulnerabilità identificate compromettano l'integrità, la riservatezza e la disponibilità delle informazioni. In caso di violazione è prevista la notifica al Grante della Privacy da effettuare sul sito dell'Autorità e entro 72 ore dalla conoscenza della violazione

Esempio di Calcolo del Rischio in un'azienda aeronautica

Considerata un'azienda aeronautica nella quale l'infrastruttura informatica è nel complesso solida, grazie ad aggiornamenti periodici con cadenza trisettimanale e con una storicità di attacchi informatici considerata bassa, poiché avvenuta nel Settembre 2020, ma operante ancora con sistemi di autenticazione basati su user id e password complesse, senza crittografia avanzata dei dati sensibili. Si consideri inoltre che: durante l'ultimo tentativo di accesso non autorizzato ai dati sono stati clonati disegni aereonautici relativi alla fabbricazione e al montaggio in materiale composito dello stabilizzatore orizzontale del Boeing 743, di cui l'azienda è detentrice di brevetto. Considerando che dopo tale incidente l'azienda committente ha richiesto lo stop-work immediato per constatare che nessun brevetto o ciclo di lavorazione fosse stato reso noto ad aziende concorrenti. Alla luce delle informazioni sopra descritte si desidera effettuare un calcolo del fattore di rischio.

- **Probabilità (P):**
  Data l'improbabilità dell'evento, legata agli aggiornamenti frequenti e al tempo trascorso dall'ultimo attacco, si assegna un indice pari a **2** (vedi pagina 5);
- **Impatto (I):**
  Data la criticità dei dati trattati come progetti riservati e brevettati, e le possibili conseguenze economiche e reputazionali in caso di violazione, si assegna un indice pari a **4** (vedi pagina 6)

- **Fattore di rischio (R):**
  R = P × I = 2 × 4 = **8**
  Il rischio calcolato è quindi di livello **medio-alto** (vedi tabelle pagina 6 e 7)

Dato il fattore di rischio medio-alto, si consiglia di intervenire con le seguenti modalità:

- introdurre **autenticazione multi fattore o biometrica** per ridurre la probabilità di compromissione;
- implementare **crittografia dei dati sensibili e backup sicuri** per ridurre l'impatto di un eventuale attacco;
- rafforzare il **monitoraggio continuo della sicurezza** con strumenti capaci di rilevare accessi anomali e bloccare tempestivamente possibili intrusioni.
- attivare **programmi di formazione e informazione al personale** sulla riservatezza dei dati e sulle corrette pratiche di sicurezza, al fine di ridurre il rischio legato al fattore umano.

Con tali interventi il rischio stimato può essere ridotto a valori inferiori o uguali a 4, facendo rientrare così il fattore di rischio in una soglia media o limitata da considerare accettabile.

CENNI STORICI SUL DATA BREACH DI LEONARDO S.P.A.

Tra maggio 2015 e gennaio 2017, Leonardo S.P.A. ha subito un grave attacco informatico interno nella divisione aeronautica (Aerostrutture e Velivoli), eseguito tramite un trojan diffuso attraverso pendrive USB. Il malware "**cftmon.exe**", non identificato dai sistemi antivirus, è stato installato su 94 postazioni di lavoro, di cui 33 nello stabilimento di Pomigliano d'Arco.
L'attacco informatico ha portato ad una trafugazione di circa **10 GB di dati**, pari a **100.000 file**, comprendenti progetti tecnici, documenti amministrativi e credenziali di accesso.
Leonardo ha dichiarato che **non erano stati coinvolti dati soggetti a segreto di Stato**, in quanto tali materiali erano conservati in apposite aree prive di connettività esterna.
Le indagini, condotte dalla Polizia Postale su impulso del pool Cybercrime della Procura di Napoli, hanno portato all'arresto di due persone:

- **Arturo D'Elia**, ex responsabile della sicurezza informatica: accusato di accesso abusivo, intercettazione illecita e trattamento illecito di dati, per il quale è stato disposto il carcere.
- **Antonio Rossi**, dirigente del CERT (Cyber Emergency Readiness Team) di Leonardo, accusato di depistaggio e trattenuto agli arresti domiciliari.

L'attacco è stato smascherato grazie al sistema di Sicurezza Informatico di Leonardo S.P.A. che analizzando dei file di log interni che monitorano il traffico e dettagliano le

varie connessioni dei sistemi con l'esterno, hanno messo in evidenza il traffico anomalo su un dominio sospetto, successivamente bloccato e sequestrato.
Dopo il data breach, Leonardo S.P.A. ha rafforzato il suo sistema interno di protezione dei dati, basandosi sulle normative vigenti creando uno standard proprietario intitolato L.S.M.S.(Leonardo Security Management System), creando inoltre un progetto laboratoriale intitolato L.V.S. (Leonardo Security Evaluation Facility) che opera in conformità agli standard internazionali ISO/IEC IS-15408 (Common Criteria) e I.S.O./I.E.C. 27001, ottenendo la qualifica dall'Organismo di Certificazione della Sicurezza Informatica (O.C.S.I.).

Best practice consigliate nel mondo aeronautico

- **Miglioramento continuo sulla base di L.V.S. e O.C.S.I.** per garantire efficacia e conformità agli standard di sicurezza del trattamento e della manutenzione dei dati elettronici., per affrontare nuove minacce e vulnerabilità in risposta ai requisiti normativi e ai possibili attacchi di Cyber Security.

- **Formazione** continua e specializzata, con corsi incentrati sulle procedure e le politiche di L.V.S., per offrire maggiore consapevolezza, in ambito di sicurezza informatica e regolamentazione privacy, nel settore aereonautico all'intera popolazione aziendale.

- **Controllo rigoroso degli accessi fisici ai sistemi**, con autenticazione biometrica e limitazione dei privilegi utente ispezionato da un monitoraggio continuo degli accessi e rilevazione anomalie interne.

- **Definizione di Recovery Plant e Incident Response** da adottare nel settore aereonautico, aerospaziale e della difesa, per garantire continuità operativa e sicurezza dei dati trattati ed elaborati, e delle informazioni.

- **Audit regolari e valutazioni di rischio aggiornate,** in linea con i riferimenti normativi e tecnologici nel settore aeronautico.

- **Collaborazione con enti regolatori e certificatori** (E.A.S.A., E.N.A.C., F.A.A.) e partecipazione a incontri di settore per aggiornamenti costanti sulle minacce emergenti.

Nel delicato contesto di un'azienda aeronautica come Leonardo Aerostrutture S.P.A. e l'esempio posto nel documento con il calcolo ipotetico del fattore di rischio in materia di privacy e sicurezza aziendale, mette in focus le vulnerabilità specifiche del settore, si vuole proporre l'adozione di misure preventive volte a garantire la protezione dai dati grezzi, all'elaborazione di informazioni terminando ai processi critici di lavorazioni e di ingegnerizzazione protetti anche da brevetti industriali.

L’ approccio è basato su normative e legislazioni con focus su best practice del settore, rappresentando una soluzione efficace al fine di ottenere elevati standard di sicurezza rispettando le specifiche tecniche imposte anche dagli enti certificatori.