UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unIMC

"Cyber and Information Security nell'Aerospace"

Tullio De Santis

Università Politecnica delle Marche

S1127068@studenti.univpm.it

Iacobucci HF Aerospace S.p.A.

tullio.desantis@iacobucci.aero

Venerdì 3 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Dal costo all’opportunità

Investimenti in tecnologia, sicurezza e formazione sempre visti dal Management come «costo», e considerarlo tale, sebbene questione comprensibile, rischia di lasciare le aziende vulnerabili in un ecosistema digitale sempre più interconnesso e minacciato.

Possiamo cambiare prospettiva cercando di trasformare la compliance in un motore di crescita e di riconoscere il valore intrinseco della resilienza digitale.

La sicurezza informatica non è un costo improduttivo, ma un vero e proprio **“business enabler”**, un vantaggio competitivo che abilita la trasformazione digitale.

Spesso solo dopo un incidente informatico l’imprenditore accetta di destinare risorse finanziarie, a causa della convinzione che “non capiterà mai a noi” **(“probability neglect”)**.

Nella mia esperienza, c’è stata una transizione graduale, grazie alla responsabilizzazione del Management, prima con GDPR, poi ISO27001 (Airbus in primis), ora con NIS2.

Dalla consuetudine operativa a procedure definite

Processi e procedure fino a qualche anno fa non avevano una applicazione e non erano documentate, bensì definite ed applicate per sola volontà o scelta del dipartimento, applicando quindi una **consuetudine operativa**.

Con GDPR, ISO27001 e NIS2, **la consuetudine si è ben definita in policy, procedure**, in ottemperanza a normativa vigente che ne definisce applicazione e sanzione in caso di mancato rispetto.

L'Unione Europea, con il **GDPR** e le varie **regolamentazioni di cybersecurity**, **stabilisce i requisiti in termini di gestione e salvaguardia di dati e sicurezza degli asset.**

Il GDPR è sostanzialmente al centro di tutto, da lì è iniziato il percorso.

GDPR – il primo approccio

Riferimenti normativi

Regolamento (UE) 2016/679; *Dlgs 196 del 2003*, aggiornato ad *agosto 2018 con il D. Lgs. 101*;

Codici di condotta ancora in vigore;

Provvedimenti (norme e sentenze) del Garante;

Ulteriori Direttive (2016/680 e 681) riguardano i dati usati per le indagini e il perseguimento di reati (recepiti con il Dlgs 51/2018);

Le norme italiane, se non sono in conflitto con il GDPR.

Definizioni dati personali - *"Dato personale*"; "*Dati personali appartenenti a categorie particolari (art. 9*)";

"Dati giudiziari" ("dati personali relativi a condanne penali e reati");

Soggetti – *Interessato; Titolare; Responsabile; Persona fisica autorizzata;*

Informativa per l'interessato Art. 13 - *le finalità e le modalità del trattamento*; *il periodo di conservazione; i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati; i propri diritti;*

Diritti dell'interessato Art. 15-21 – Diritto di accesso, rettifica, cancellazione «oblìo», limitazione di trattamento, portabilità, opposizione;

Consenso – espresso, può riguardare l'intero trattamento o una o più operazioni, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso, revocabile;

Notifica di violazioni - Notifica al Garante (Articolo 33 del GDPR); Notifica all'interessato (Articolo 34 del GDPR).

GDPR – il primo approccio

Articolo 25

Dicotomia concettuale piuttosto importante per comprendere la privacy, attraverso due sfere che servono a spiegare chiaramente in che modo e in che misura le aziende e le organizzazioni sono incoraggiate ad attuare **misure tecniche e organizzative** per salvaguardare il trattamento dei dati dell'utente.

("Privacy by design"): Protezione dei dati fin dalla progettazione

il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la **anonimizzazione** o la **pseudonimizzazione**, volte ad attuare in modo efficace i principi di protezione dei dati, quali la **minimizzazione** (limitato accesso, adeguatezza, pertinenza e non eccessiva), e ad **integrare nel trattamento le necessarie garanzie** al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati;

("Privacy by default"): Protezione per impostazione predefinita

il titolare del trattamento mette in atto misure tecniche e organizzative adeguate **per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento**.

GDPR – il primo approccio

Registro dei trattamenti per organizzazioni con più di 250 "dipendenti" (art. 30 del GDPR):

diverso per titolari e responsabili; dati di contatto del titolare del trattamento; finalità del trattamento; categorie di interessati e delle *categorie di dati personali*; *categorie di destinatari* a cui i dati personali sono stati o saranno comunicati; trasferimenti di dati personali verso un paese terzo; *termini ultimi previsti per la cancellazione* delle diverse categorie di dati; *una descrizione generale delle misure di sicurezza tecniche e organizzative*.

Art. 32 dl GDPR Verifiche *dell'efficacia delle misure tecniche e organizzative* assicurando la riservatezza, integrità, disponibilità e resilienza dei sistemi di trattamento.

Art. 35 dl GDPR Valutazione d'impatto sulla protezione dei dati o *«privacy impact assessment (PIA)»* (quando il trattamento riguarda determinate informazioni, su larga scala o sistematicamente. Se emerge livello rischio elevato va consultata autorità di controllo (Art.36 dl GDPR).

Data protection officer (DPO) (art. 37-39 del GDPR) obbligo in casi particolari, ma anche volontariamente.

Il GDPR stabilisce posizione e compiti del DPO.

L’incipit «ISO27001» ….. «Assessment Airbus»

L’azienda è Supplier di OEM quali Airbus, Boeing, Bombardier, da questi ultimi, Audit periodici vengono eseguiti da anni, come da parte di altri soggetti.

Questionari o veri e propri Audit sul posto, previsti contrattualmente all’atto dell’accordo di fornitura.

«lo stimolo iniziale quindi è arrivato dall’esterno, da AIRBUS».

Scenario diffuso

In molte aziende anche strutturate, investimenti vengono approvati solo se il processo è Top Down, pertanto solo quando il TOP Management subisce un incidente informatico, una sanzione o si è costretti da Clienti o da normative, che prevedono sanzioni personali oltre che verso la Società di cui si è responsabili.

«ISO27001» ….. «Assessment Airbus»

AIRBUS

To

Airbus suppliers

Klaus Richter - Chief Procurement Officer
E klaus.k.richter@airbus.com

Our ref: P-200.083/2019

29 November 2019

Airbus Cyber Security – Supplier Risk Assessment

Dear Supplier,

Cyber Security is one of the top Airbus business risks and it is the responsibility of all actors. In recent years, the scale and robustness of cyber-attacks has significantly increased and Airbus has not been spared. In this context, it is becoming imperative that Airbus assesses its partners' IT operations sturdiness and reliability, with the concern of maintaining a healthy business environment and trustworthy collaborations.
It is essential that you reply in full transparency and honesty to the attached questionnaire, based on ISO/IEC 27001. We trust you to provide answers that reflect your actual levels of compliance since a recovery plan will be tailored to help you reach full compliance.

In that respect, please take particular notice of the following:

- This questionnaire is potentially addressed to more than one of your company-specific facilities (sites) as we follow the priorities of industrial risks (impact) to our Supply Chain.
- The questions are pertaining to all your office-, manufacturing- and transport systems. You are therefore required to assess the risk for all your operational units and consider the lowest security level.
- Efficient security policy and practices (not to be confused with safety aspects) are known and implemented throughout the company.

In each chapter of the assessment tab, please select the answer best fitting your situation. There should be exactly one answer per question (ungroup to see maturity level vs. criteria). In case of doubt, please do not hesitate to contact request.external.security@airbus.com

We rely on your support to provide the requested information by 31st December 2019in order to allow diligent implementation of the recovery plan.

This initiative is in a first wave limited to your ordering plant, as addressed above. We plan to extend this exchange to the next-tier level of suppliers in the course of the first semester 2020.

Thank you in advance for your cooperation.

Best regards

Klaus Richter

Airbus SAS
Société par actions simplifiée
au capital de 3 229 761 Euros
RCS Toulouse 383 474 814

Siège social :
2 rond-point Emile Dewoitine,
31700 Blagnac, France
www.airbus.com

<u>29.11.2019</u>

Airbus introduce nei contratti con i Suppliers, Audit e rispetto normativa EN ISO 27001 con una logica NIS, condizionando la qualifica del fornitore, già nel 2019.

Nei contratti stipulati c'era un Annex nel quale era esplicitamente rappresentato come parte integrante del contratto, l'accettazione da parte del fornitore, del potere conferito al «Cliente» di eseguire Audit, fino alla revoca della qualifica come fornitore:

- Sul prodotto fornito (EN AS9100);
- Sulla Sicurezza Informatica (ISO27001) e NIS.

ISO27001 «Assessment Airbus» Human Resources Security

Chapter 3	Human Resources Security
Q3.1	How do you cover the security aspects in your hiring process?
1	No hiring process covering security aspects
2	Identity checked, background only for sensitive customer projects
3	Identity & criminal background checked for all employees
4	Multi-Nationality checked
5	A check list is formalized to ensure security aspects in the hiring process

La sicurezza delle risorse umane (HR) nell'ambito della sicurezza informatica si concentra sulla gestione del fattore umano per proteggere un'organizzazione dalle minacce informatiche.

Ciò include il ruolo delle HR nell'acquisizione e nello sviluppo dei talenti, nella gestione dell'accesso ai dati sensibili dei dipendenti, nello sviluppo e nell'applicazione di policy di sicurezza, nella promozione di una cultura aziendale attenta alla sicurezza attraverso programmi di formazione e sensibilizzazione e nel garantire la conformità alle normative sulla privacy dei dati, come il GDPR.

Nello schema vediamo come Airbus inserisce in una scala da 1 a 5 il processo di assunzione, dimostrando molta attenzione alla richiesta di «**affidabilità del candidato**, previa valutazione»

ISO27001 «Assessment Airbus» Asset Management

Chapter 4	Asset Management
Q4.2	To what extent is your data classification and handling scheme formalized?
1	No data classification and handling scheme
2	Data classification is defined without formalized handling scheme
3	Data classification is defined with a formalized handling scheme. All documents are marked accordingly. Data classification scheme clearly includes customer data.
4	Data owners are nominated, trained and perform regular reviews of their data classification
5	Data tagging feeds security tools which prevents data exfiltration/data leakage

Classificazione dei dati

Processo che troviamo applicazione in tutti gli ambiti GDPR, ISO27001, IRP NIS2:

- Registro trattamento dati;
- Procedura e classificazione delle informazioni;
- Dal punto di vista tecnologico, possibilità di «vietare», «limitare» e tracciare azioni sui dati/documenti.

ISO27001 «Assessment Airbus» Access Control

Chapter 5	Access Control
Q5.4	How can you access your IT/OT systems remotely ? (from home, during travels, for remote administration and maintenance…)
1	The IT system is accessible remotely without any protection
2	Login/password only. Users connecting remotely (from home or hotel…) authenticate with their user ID and password to your IT systems
3	Users connecting remotely (from home or hotel…) use strong authentication (one-time password, digital certificate, smartphone…) to your IT systems
3	If third parties connect remotely for administration or maintenance of IT/OT systems, there is strong authentication required, as well as well-protected environments from where they connect.
4	Users and third parties connected remotely with strong authentication have also restricted access to IT/OT systems (e.g. software updates not authorized)
5	No remote connection authorized

L'Agid, l'Agenzia per l'Italia Digitale, ha elaborato 11 raccomandazioni:

- Seguire prioritariamente le policy e le raccomandazioni;
- Utilizzare i sistemi operativi supportati;
- Effettuare aggiornamenti di sicurezza del tuo sistema operativo;
- Firewall, Antivirus, ecc. siano abilitati e costantemente aggiornati;
- Sistema operativo protetti da una password sicura e comunque conforme alle password policy;
- Non installare software provenienti da fonti/repository non ufficiali;
- Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico in assenza da postazione di lavoro;
- Non cliccare su link o allegati contenuti in email sospette;
- Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;
- Collegamento a dispositivi mobili (pen-drive, hdd-esterno, ecc.) di provenienza nota;
- Effettuare sempre il log-out dai servizi/portali utilizzati, al termine della sessione lavorativa.

ISO27001 «Assessment Airbus» Cryptography

Chapter 6	Cryptography
Q6.2	How do you encrypt your sensitive information (e-mails, files)?
1	No sensitive information encrypted
2	Only some sensitive information are encrypted
3	All sensitive information are encrypted
4	All sensitive information are encrypted with certificates
5	A corporate PKI is in place

Crittografia e Protezione dei Dati

Implementazione nelle Infrastrutture aziendali. Per proteggere efficacemente i dati, la crittografia deve essere implementata in vari punti dell'infrastruttura aziendale:

- **Crittografia dei Dati a Riposo**: protezione dei dati memorizzati nei dispositivi di archiviazione;
- **Crittografia dei Dati in Transito**: protezione dei dati che vengono trasmessi attraverso le reti.

E' fondamentale che tutti i dispositivi, Fissi, Mobili, Server abbiano implementata la crittografia, come è fondamentale l'uso della crittografia nello scambio delle informazioni attraverso l'utilizzo della posta elettronica.

Non è sufficiente, ma resta una misura minima e richiesta, anche nel GDPR.

ISO27001 «Assessment Airbus» Supplier relationships

Chapter 11	Supplier relationships
Q11.1	What kind of security agreements do you have with your suppliers?
1	No security agreements are requested to the suppliers
2	A NDA is sometimes requested to the suppliers for critical projects or confidential data manipulation
3	A1015 Airbus security requirements are cascaded in contracts with your suppliers
4	Supplier's own security requirements (equivalent to A1015) are contractualized to your suppliers
5	Security requirements cascaded to your suppliers are regularly controlled and audited

Elemento presente, **ha di fatto anticipato quello che è previsto nella direttiva NIS2**, specie nel punto **5.**

«La novità NIS2»: estende il campo di applicazione a cascata **ai fornitori dei soggetti essenziali e importanti**, indipendentemente dalle dimensioni del fornitore.

Ogni anello della catena di approvvigionamento dovrà essere soggetto a rigorosi standard di cybersecurity, creando un effetto domino destinato a rafforzare la resilienza complessiva del sistema.

Questo amplia enormemente la platea dei soggetti che dovranno essere conformi alla NIS2, andando a **includere anche soggetti che ne sarebbero esclusi, ma che dovranno conformarsi.**

(I soggetti essenziali e importanti, devono monitorare e valutare continuamente le pratiche di cybersecurity dei fornitori e intervenire tempestivamente in caso di cambiamenti significativi o incidenti.
La direttiva NIS2 non solo protegge le infrastrutture critiche, ma promuove una cultura di sicurezza informatica che permea l'intera supply chain.

ISO27001 «Assessment Airbus» Incident Management

Chapter 12	Incident Management
Q12.2	What are the means (organization and process) in place to respond to security incident?
1	Neither organization or process to respond to security incident
2	Organization exists but no clear process defined to respond
3	Organization exists and the process is defined and followed. Clear roles and responsibilities formalized
4	Teams are centralized globally
5	Teams are company wide. Forensic experience and participation to security conferences

ISO27001 → Procedura Incident Management

La Procedura di Incident Management è un processo strutturato per identificare, analizzare, contenere, eradicare e recuperare gli incidenti di sicurezza, al fine di minimizzarne l'impatto e prevenirne il ripetersi, salvaguardando riservatezza, integrità e disponibilità delle informazioni. Questo processo è fondamentale per il Sistema di Gestione della Sicurezza delle Informazioni (ISMS) e prevede fasi operative precise, coinvolgendo anche personale e processi organizzativi.

NIS2 → IRP ed obbligo di notifica (dal 01/01/2026)

Il National Institute of Standards and Technology – NIST, definisce l'Incident Response come un processo strutturato che le organizzazioni utilizzano per identificare e gestire gli incidenti di sicurezza informatica. La risposta comprende diverse fasi, tra cui la preparazione agli incidenti, il rilevamento e l'analisi di un incidente di sicurezza, il contenimento, l'eradicazione e il recupero completo, nonché l'analisi e l'apprendimento post-incidente.

E' di fondamentale importanza la **definizione di incidente di sicurezza.**

Information Security (SGSI/ISMS) e Cybersecurity

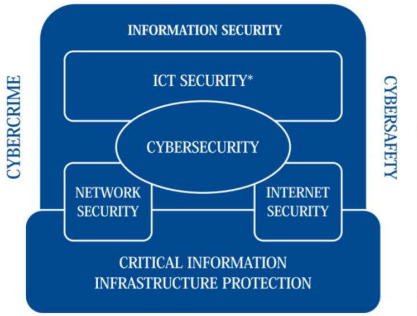
Cybersecurity e Information Security sono termini spesso considerati sinonimi, tuttavia differiscono per diversi aspetti. Sono materie strettamente connesse che si occupano di proteggere le informazioni, ma si differenziano nella loro applicazione.

- La Sicurezza dell'Informazione si occupa di proteggere tutte le forme di informazione, indipendentemente dalla loro natura fisica o digitale.

- La Cyber Sicurezza si concentra sulla protezione delle informazioni digitali e dei sistemi informativi.

la Cybersecurity e l'Information Security garantiscono la sicurezza di tutte le informazioni e i dati aziendali e non solo, adottando strategie complete che tengano conto sia dei dati fisici che di quelli digitali.

Information Security (SGSI/ISMS)



L'information Security si occupa di proteggere la **disponibilità**, l'**integrità** e la **confidenzialità** delle informazioni di qualsiasi organizzazione.

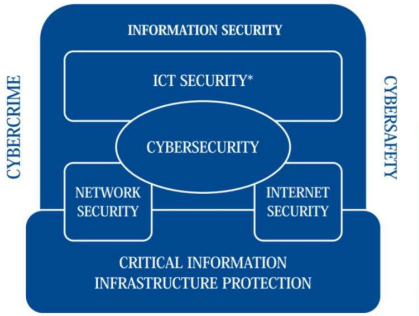
L'Information Security propone una serie di misure che devono essere messe in atto per prevenire, rilevare e rispondere alle minacce a cui i dati sono sottoposti.

Questo significa, ad esempio, implementare in azienda il controllo degli accessi, una gestione sicura delle password e l'uso consapevole dei dispositivi.

Inoltre contribuisce alla formazione continua dei dipendenti, al fine di promuovere sempre di più le pratiche per la sicurezza delle informazioni.

È fondamentale quindi avere una strategia più chiara possibile e continuamente aggiornata che comprenda la protezione individuale e collettiva, la gestione dei rischi e la conformità normativa.

Cybersecurity



La **Cybersecurity** si concentra sulla protezione di tutta la sfera IT presente in azienda e in generale delle reti, per prevenire possibili attacchi e intrusioni informatiche. L'obiettivo è quello di mantenere al sicuro le risorse digitali, contrastando gli accessi non autorizzati che potrebbero acquisire dati e divulgarli per scopi criminosi o di lucro.

Previste una serie di strategie architettate per diminuire i rischi associati alle attività online:

- Identificazione e autenticazione per dare accesso ai tools solo alle persone autorizzate;
- Protezione da malware, installando software antivirus e anti malware;
- Monitoraggio delle attività sospette attraverso software specifici in grado di controllare le reti e le attività degli utenti;
- Protezione delle reti da accessi non autorizzati;
- Una corretta gestione delle vulnerabilità dei sistemi, in modo tale da coprire eventuali falle utilizzabili da malintenzionati.

NIS2

NIS 2 (Direttiva UE 2022/2055) entrata in vigore il 17 gennaio 2023.

NIS2 è recepita dal 17 ottobre 2024 in Italia con il D. Lgs. 138 del 2024.

Rispetto alla NIS1:

- Aumentano i soggetti;
- Richiede un'analisi dei rischi;
- Le misure dovrebbero essere adeguate al contesto, considerando quindi anche la capacità di spesa.

L'autorità italiana per la NIS2 è ACN.

Scadenze:

- Entro il 17 gennaio 2025 bisognava valutare se si è soggetto essenziale o importante e registrarsi sulla piattaforma ACN.
- Entro il 15 aprile, ACN ha comunicato l'esito della valutazione;
- Entro il 1 gennaio 2026, bisogna adeguarsi all'art. 25 (notifica incidenti, stabilendo il processo);
- Entro il 1 gennaio 2026, bisogna essere adeguati all'art. 30 (aggiornare le informazioni richieste dalla piattaforma ACN con l'elenco di attività e servizi e la descrizione delle loro caratteristiche);
- Entro ottobre 2026, bisogna adeguarsi agli artt. 23, 24 (gestione dei rischi e misure di sicurezza) e 29 (banca dati nomi a dominio).

NIS2

La NIS2, idealmente, dovrebbe includere le **aziende già presenti nel PNSC** (perimetro nazionale per la sicurezza cibernetica, da DL 105 del 2019).

I soggetti sono quindi suddivisi in (art. 6):

- soggetti essenziali (essential entities);
- soggetti importanti (important entities).

La differenza pratica riguarda i controlli e le sanzioni.

Valutazione del rischio

NIS2, come da art. 24, è multirischio: logico, fisico, governo, lock in tecnologico, utilities. Considera l'impatto "sociale ed economico" e richiede un "livello appropriato" di sicurezza.

Esempi: sabotaggi, furti, incendi, inondazioni, problemi di telecomunicazione, interruzioni di corrente, qualsiasi accesso fisico non autorizzato che compromette disponibilità, autenticità, integrità o la riservatezza dei dati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi, guasti del sistema, errori umani, azioni malevoli, fenomeni naturali.

NIS2

Misure di sicurezza

Il D. Lgs. 138 identifica le misure di gestione del rischio (fino al 2055), ossia:

- politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
- gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli artt. 25 e 26;
- continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;
- sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto ed i suoi diretti fornitori o fornitori di servizi;
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
- politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;
- pratiche di igiene di base e di formazione in materia di sicurezza informatica (NOTA: L'art. 23, correttamente, impone agli organi di amministrazione e gli organi direttivi dei soggetti NIS2 una formazione in materia di sicurezza informatica);
- politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura (NOTA: non chiara la differenza tra crittografia e cifratura, presente anche nella Direttiva tra cryptography e encryption);
- sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;
- uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

NIS2

Catena di approvvigionamento

La NIS2 descrive più approfonditamente le **necessità di controllo della catena di approvvigionamento**:

I soggetti devono tenere conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi, della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro.

Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

Per questo sarà sicuramente necessario migliorare le pratiche di selezione, valutazione e rivalutazione dei fornitori e delle forniture.

Purtroppo ritorneranno in voga gli inefficaci e inefficienti questionari, quando invece si dovrà pensare a qualcosa di meglio.

NIS2

Gestione degli Incidenti

Come già previsto dalla Direttiva NIS1, anche NIS2 prevede l'obbligo di notifica al CSIRT e alle autorità competenti (oltre che ai destinatari stessi del servizio) degli incidenti significativi (incidenti informatici capaci di impattare in modo significativo sulla fornitura del servizio).

È da notare la confusione in materia, visto che anche la Legge 90 del 2024 fornisce obblighi sulla notifica e gestione degli incidenti a soggetti a cui è applicabile anche la NIS2.

Ovviamente le disposizioni sono diverse e il D. Lgs. 138 del 2024 cita la Legge 90 solo come "vista".

Notifica

Le comunicazioni al CSIRT dovranno avvenire:

entro 24 ore dalla conoscenza dell'incidente, con una notifica di preallarme che deve riportare i dati strettamente necessari se l'incidente significativo sia sospettato di essere il risultato di atti illegittimi o malevoli o se possa avere un impatto transfrontaliero; inoltre deve contenere una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

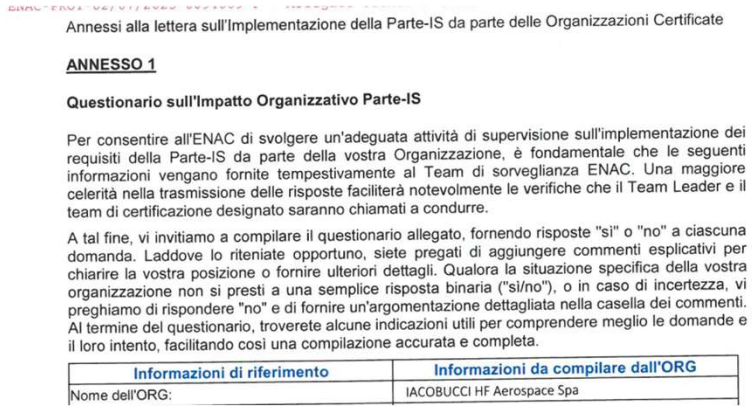
entro 72 ore dalla conoscenza dell'incidente va trasmessa una **notifica completa** con aggiornamenti rispetto alle informazioni fornite con il preallarme;

entro 1 mese dalla conoscenza dell'incidente con una relazione finale a completamento del processo di segnalazione; la relazione deve essere comprensiva della sua gravità e del suo impatto, il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente, le misure di mitigazione adottate e in corso e, se opportuno, l'impatto transfrontaliero dell'incidente.

Se in 1 mese l'incidente non sia ancora risolto, la normativa fornisce indicazioni su come procedere.

E' prevista la possibilità di chiedere assistenza al CSIRT.

ISMS : ENAC ed EASA



Annessi alla lettera sull'Implementazione della Parte-IS da parte delle Organizzazioni Certificate

ANNESSO 1

Questionario sull'Impatto Organizzativo Parte-IS

Per consentire all'ENAC di svolgere un'adeguata attività di supervisione sull'implementazione dei requisiti della Parte-IS da parte della vostra Organizzazione, è fondamentale che le seguenti informazioni vengano fornite tempestivamente al Team di sorveglianza ENAC. Una maggiore celerità nella trasmissione delle risposte faciliterà notevolmente le verifiche che il Team Leader e il team di certificazione designato saranno chiamati a condurre.

A tal fine, vi invitiamo a compilare il questionario allegato, fornendo risposte "sì" o "no" a ciascuna domanda. Laddove lo riteniate opportuno, siete pregati di aggiungere commenti esplicativi per chiarire la vostra posizione o fornire ulteriori dettagli. Qualora la situazione specifica della vostra organizzazione non si presti a una semplice risposta binaria ("sì/no"), o in caso di incertezza, vi preghiamo di rispondere "no" e di fornire un'argomentazione dettagliata nella casella dei commenti. Al termine del questionario, troverete alcune indicazioni utili per comprendere meglio le domande e il loro intento, facilitando così una compilazione accurata e completa.

Informazioni di riferimento	Informazioni da compilare dall'ORG
Nome dell'ORG:	IACOBUCCI HF Aerospace Spa

ISMS applicato a POE e MOE (procedure ed informazioni di produzione e manutenzione) – Quality System

In ambiente Aerospace, le stesse procedure ISO27001 devono essere contestualizzate ed integrate nel Manuale della Qualità di Sistema.

Una novità è rappresentata dal fatto che il Senior Person (AD e Quality Manager) attualmente previsto in POE e MOE, non può più assumere tale ruolo nell'ISMS, in quanto sono richieste competenze in ambito Cybersecurity e informatiche, obbligando di fatto alla «sostituzione» e nomina di una figura Dirigenziale con deleghe e poteri attribuiti dal CDA alla nuova figura.

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unimc

Grazie

Tullio De Santis

Venerdì 3 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection