POLICY DI SVILUPPO, INSTALLAZIONE E MANUTENZIONE

INTEGRATED MANAGEMENT SYSTEM - POLICY

Via Mozart, 47 – 20093
Cologno Monzese (MI), Italia
Contatti: info@nuvyta.com
www.nuvyta.com

SOMMARIO

Document Information

Title	Q_P_QualityManagementSystem_Development&Maintenance &Installation			Status	Published
Type	*Policy*	Version	1.1	Created	07/06/2022
DocCode	*Q_P_004*	Language	ITA	Modified	04/01/2023
Author	Chiara Savino	Reviewer	Vania Manzelli	Approver	Alice Magni

Document Control

Intended Audience	Employee, Auditor, All
Distribution List	Public

Revision History

Ver.	Publish Date	Note
1.0	07/06/2022	First Release
1.1	04/01/2023	Inserimento 5.3 Installazione software

1 OBIETTIVI (PURPOSE)

La necessità di proteggere le informazioni, piuttosto che un'opzione, oggi giorno è una necessità. Al fine di garantire il funzionamento, la gestione e la protezione delle informazioni e dei sistemi informativi di NUVYTA SRL, è necessario considerare ed includere i controlli di sicurezza all'interno dell'Information System dalla sua progettazione fino alla sua dismissione.

Le presenti procedure definiscono i controlli che devono essere presi in considerazione al fine di garantire che la sicurezza sia insita nell'Information System e che questo sia sviluppato e supportato in modo coerente, assicurando che siano soddisfatte le esigenze aziendali degli utenti finali e dei clienti. Lo sviluppo, l'aggiornamento e la manutenzione dei sistemi dovrebbero essere considerati in relazione ai possibili effetti sulla riservatezza, l'integrità e la disponibilità dei sistemi stessi e dei sistemi ad essi collegati, con l'obiettivo di assicurare un accesso continuo e sicuro alle risorse e alle informazioni aziendali.

Questo documento si riferisce ai dipendenti di NUVYTA che hanno accesso, sviluppano, mantengono o utilizzano i sistemi IT e le informazioni che appartengono ai clienti e che sono sotto il controllo aziendale.
Lo scopo di queste procedure è quello di garantire che, alla sicurezza delle informazioni e dei sistemi, sia data la dovuta importanza durante tutte le fasi del ciclo di vita e di sviluppo dei sistemi, compresa la fase di consegna. È essenziale che il personale abbia la consapevolezza che le procedure e le politiche siano comprese e rispettate.

2 CAMPO DI APPLICAZIONE (SCOPE)

L'ambito di queste procedure riguarda tutte le persone che progettano, costruiscono, commissionano, acquistano, modificano, manutengono, aggiornano e hanno accesso alle informazioni ai sistemi dell'azienda o a quelli dei clienti gestiti da NUVYTA Srl.

3 RESPONSABILITÀ (RESPONSABILITIES)

La direzione e il responsabile della sicurezza delle informazioni hanno la responsabilità di garantire che il personale tutto siano consapevoli delle politiche di sicurezza e che le rispettino che abbia le giuste conoscenze, consapevolezza e responsabilità circa la sicurezza delle informazioni e dei sistemi che essi sviluppano o manutengono.

4 DEFINIZIONI E ABBREVIAZIONI (DEFINITIONS)

RISCHIO: insieme potenziale di tutti gli eventi che possono cambiare l'andamento di un progetto rispetto a quanto previsto in fase di pianificazione.

5 POLITICA (POLICY)

Nuplatform è stata progettata secondo un approccio secure by design e secure by default e con una costante analisi del rischio in ogni fase del ciclo di vita del software. La soluzione offre l'adozione dei più recenti standard, sia in termini di sicurezza informatica (cifratura dei canali di comunicazione, HTTPS, TLS), sia in termini di modellazione dei dati, consentendo il soddisfacimento dei requisiti dettati dalle Direttive Europee e Italiane in merito alla gestione dei dati sensibili e personali.

Il servizio erogato da Nuvyta non si basa su macchine virtuali ma su servizi gestiti tramite container e le immagini dei tali container non vengono eseguite con utenze privilegiate. Le stringhe di connessione sono gestite da un configuration server che le salva in maniera cifrata.

Il sistema è architettato e progettato per scalare in base al carico (utenti concorrenti) e vengono schedulati test di performance per ogni release di prodotto.

Linee guida: **https://learn.microsoft.com/it-it/azure/aks/developer-best-practices-pod-security**

5.1 Sviluppo

- All'inizio di qualsiasi progetto devono essere definiti i requisiti di sicurezza al fine di garantire la loro efficacia per evitare che ci siano impatti negativi sul prodotto realizzato.
- I requisiti di sicurezza non devono essere considerati avulsi dai requisiti di sistema.
- Per considerare efficacemente la sicurezza, è necessario pianificarla fin dall'inizio del processo di sviluppo e / o manutenzione al fine di assicurare che sia insita nel contesto dell'Information System.
- La sicurezza nello sviluppo dei sistemi non solo enfatizza la difesa da accessi e abusi impropri, ma anche che:
    - Il codice garantisca che il sistema elabori solo dati validi e coerenti ed in linea con le aspettative dei clienti
    - Vengano eseguiti test unitari, funzionali e di integrazione per garantire che i processi si comportino come previsto dai requisiti e dai criteri di progettazione.
    - Vengano prese in considerazione le tecniche più appropriate per garantire il back-up e proteggere i dati da perdite o danneggiamenti.
    - Le funzioni di archiviazione debbano essere prese in considerazione al fine di garantire le prestazioni del sistema e l'archiviazione delle informazioni.
    - Siano in essere accordi e/o procedure di Disaster Recovery.
    - Ci siano adeguate garanzie di disponibilità degli ambienti HW e RDBMS sul cloud
    - Sia garantito il rispetto di eventuali requisiti legali e normativi.
    - Sia garantita la sicurezza nelle comunicazioni e nel trasferimento dei dati da e verso i clienti.
    - Ci sia consapevolezza e formazione sulla sicurezza.
    - Ci sia una verifica efficace e gestionale delle attività.
    - Il sistema preveda meccanismi di reporting per soddisfare i requisiti di controllo.
- Durante lo sviluppo di un prodotto e/o sistema devono essere valutati i potenziali effetti sia diretti che indiretti (in combinazione con altri sistemi e/o risorse) sulla riservatezza, integrità e disponibilità delle informazioni

- Un ambiente di test separato dovrebbe, se possibile, essere utilizzato per replicare il sistema di produzione al fine di consentire ed effettuare, in caso di modifiche, valutazioni preventive al fine di evitare possibili impatti negativi sull'ambiente di collaudo e di produzione del cliente.
- Non è consentito l'utilizzo di informazioni personali o sensibili a scopo di test.
- I test devono essere eseguiti se possibili su viste logiche di DB preparate e consegnate dal cliente
- Il responsabile della sicurezza delle informazioni nonché direttore tecnico supervisiona la gestione della sicurezza
- Durante le fasi iniziali del ciclo di sviluppo dei sistemi, i rischi per la sicurezza delle informazioni devono essere valutati in base alla probabilità e al potenziale impatto su riservatezza, integrità e disponibilità. È opportuno assegnare categorie o livelli di rischio (come basso, medio, alto). Una valutazione del rischio deve definire anche il livello di minaccia per il sistema in funzione dell'ambiente in cui opera.
- È necessario attuare controlli per ridurre la possibilità che i rischi identificati per la sicurezza raggiungano livelli non accettabili.
- Durante le fasi di sviluppo, ed in funzione dell'analisi dei rischi effettuata, dovrebbero essere utilizzare le opportune procedure di backup recovery.
- Le verifiche effettuate durante le fasi iniziali avvantaggiano gli utenti finali circa le funzionalità richieste garantendo allo stesso tempo l'opportuno livello di sicurezza integrato.
- L'accesso agli strumenti di sviluppo e alle utility di sistema dovrà essere limitato al personale di NUVYTA SRL così come l'accesso al codice sorgente dei programmi dovrà essere limitato ai soli tecnici o comunque alle sole persone incaricate.
- Si deve applicare un efficace processo formale di controllo delle modifiche al fine di gestire opportunamente sia i rischi reputazionali che quelli specifici relativi alle risorse informatiche.
- Se vengono rilevati bug in un'applicazione o in un sistema, che possano avere un impatto sulla riservatezza, la disponibilità o l'integrità, la loro risoluzione deve essere testata ed installata nel più breve tempo possibile.
- È necessario prendere in considerazione l'uso di un accordo di garanzia per mitigare eventuali problemi che possano verificarsi con la gestione del codice dei clienti gestiti da NUVYTA SRL.
- Percorsi di sensibilizzazione del personale vanno effettuati per consentire loro di essere consapevoli delle proprie responsabilità verso la sicurezza dei sistemi e delle informazioni durante le attività di sviluppo dei sistemi.
- Tutto il personale è responsabile della salvaguardia della riservatezza delle informazioni durante il ciclo di sviluppo dei sistemi ICT. I livelli concordati di disponibilità e integrità dell'intero sistema o sottosistema devono essere garantiti durante tutte le fasi di sviluppo.
- Le misure di pianificazione della sicurezza dovranno garantire l'attuazione dei controlli di sicurezza concordati che includano tutti gli aspetti della sicurezza di un sistema. I requisiti di sicurezza che possono essere validati e verificati includono controlli di sicurezza logica e fisica nel sito.
- Deve essere garantita l'integrità, la riservatezza e la disponibilità dei dati durante e dopo le fasi di dismissione dei vecchi sistemi e transizione ai nuovi, come durante e dopo i processi di archiviazione.

5.2 Manutenzione

- Per considerare efficacemente la sicurezza, è necessario pianificarla fin dall'inizio del processo di sviluppo e / o manutenzione al fine di assicurare che sia insita nel contesto dell'Information System.
- Sarebbe necessario stabilire e concordare con il cliente la criticità del sistema in termini di tempo massimo tollerabile per ripristinarne la piena funzionalità a fronte di un evento critico (SLA) ma questo dipende dalla volontà del cliente definirlo negli accordi contrattuali.
- Al momento di individuare gli aspetti di sicurezza vanno considerate le verifiche interne ed esterne più i requisiti legali e statutari dei sistemi ausiliari e/o associati:

- Continuità di servizio
- Backup and recovery dei dati
- Controlli di accesso ai sistemi
- Controlli dell'elaborazione dei dati
- Documentazione delle misure di sicurezza
- Opportunità di effettuare l'archiviazione dei dati di backup ed il posizionamento di un'infrastruttura di emergenza al di fuori della sede principale per fronteggiare situazioni di emergenza (Cloud Google)

- Durante le fasi di manutenzione, ed in funzione dell'analisi dei rischi effettuata, dovrebbero essere utilizzare le opportune procedure di backup recovery.
- Percorsi di sensibilizzazione del personale vanno effettuati per consentire loro di essere consapevoli delle proprie responsabilità verso la sicurezza dei sistemi e delle informazioni durante le attività di manutenzione dei sistemi.
- Tutto il personale è responsabile della salvaguardia della riservatezza delle informazioni durante il ciclo di sviluppo dei sistemi ICT. I livelli concordati di disponibilità e integrità dell'intero sistema o sottosistema devono essere garantiti durante tutte le fasi di manutenzione.
- Quando un sistema viene dismesso, è necessario adottare misure di sicurezza per consentire la rimozione sicura di apparecchiature e del software in modo tale da non compromettere la riservatezza dei dati.
- Durante la dismissione di qualsiasi sistema, se necessario, i dati e le informazioni devono essere archiviati in linea con i requisiti di legge e secondo le procedure messe in atto dall'organizzazione. L'archiviazione dei dati dovrà essere controllata dal responsabile del sistema di gestione della sicurezza e direttore tecnico al fine di garantire che i requisiti siano stati soddisfatti.
- È necessario effettuare un'attenta pianificazione per la dismissione dei sistemi includendo la rimozione dei diritti di accesso e la disinstallazione del software dai PC e dai server.
- Le procedure riportate devono essere applicate durante le fasi di modifica e manutenzione dei sistemi esistenti al fine di assicurare che tutte le modifiche aderiscano e garantiscano i corretti livelli di sicurezza.

5.3 Installazione software

- L'aggiornamento del software di produzione, delle applicazioni e delle librerie deve essere effettuato solo da amministratori formati sulle tematiche di sicurezza.
- Sul sistema di produzione deve essere presente solo codice eseguibile approvato: Nuvyta ha implementato uno storage dedicato dove tenere tracciare di tutte le immagini del prodotto ufficialmente rilasciato.
- I sistemi e le applicazioni possono essere installati solo previo test completato con successo tramite convalida delle procedure di testing
- Deve essere attuato un sistema di controllo delle configurazioni su tutto il software
- Deve essere presente una strategia di rollback
- Le versioni precedenti del software devono essere mantenute fino al termine ufficiale del supporto da parte di Nuvyta
- Deve essere mantenuto un log di audit di tutti gli aggiornamenti alle librerie di produzione
- Deve essere riportata la modalità di archiviazione di precedenti versioni obsolete dei software

5.3.1 Gestione delle vulnerabilità tecniche

- Devono essere definiti ruoli e responsabilità per la gestione delle vulnerabilità tecniche

- Devono essere identificate risorse informative utilizzate per individuare le vulnerabilità tecniche
- Deve essere definita una scala temporale per reagire alle vulnerabilità tecniche
- Una volta identificata la vulnerabilità devono essere verificati i rischi e le azioni da intraprendere
- In base all'urgenza, le vulnerabilità devono essere gestite in modo coerente con i controlli collegati
- Se una patch è resa disponibile da una sorgente legittima, i rischi legati alla sua installazione devono essere valutati
- Devono essere fatti log di audit a tutte le procedure intraprese
- Il processo di gestione delle vulnerabilità va monitorato
- I sistemi a rischio alto vanno valutati per primi

5.4 Documenti Procedure di riferimento

Documento / Nome registrazione	Posizione di memorizzazione	Proprietario	Controllo di protezione	Tempi di conservazione
D_PR_Product&ServiceDevelopment_ ApplicationLifecycleManagement	Sharepoint – IMS	ISM	Internal	Illimitato
D_PR_Product&ServiceDevelopment_ Quality&SecurityAssurance	Sharepoint – IMS	ISM	Internal	Illimitato
O_PR_Product&ServiceSupport_ Support&FeedbackManagement	Sharepoint - IMS	ISM	Internal	Illimitato
User Stories, Requirements	Microsoft Azure Devops	SDM	Internal	Illimitato
User manual, Release Note	ReadtheDocs	SDM	Customer	Illimitato
Tickets	Zendesk	OM	Internal	Illimitato

6 RIFERIMENTI (REFERENCES)

CONTROLLI ISO 27001 APPLICATI

Riferimento Controllo	Titolo
A.6.1.1	RUOLI E RESPONSABILITÀ PER LA SICUREZZA DELLE INFORMAZIONI
A.7.2.1	RESPONSABILITÀ DELLA DIREZIONE
A.7.2.2	CONSAPEVOLEZZA, ISTRUZIONE, FORMAZIONE E ADDESTRAMENTO SULLA SICUREZZA DELLE INFORMAZIONI
A.9.2.1	REGISTRAZIONE E DE-REGISTRAZIONE DEGLI UTENTI
A.9.2.2	PROVISIONING DEGLI ACCESSI DEGLI UTENTI
A.9.2.3	GESTIONE DEI DIRITTI DI ACCESSO PRIVILEGIATO

A.9.2.4	GESTIONE DELLE INFORMAZIONI SEGRETE DI AUTENTICAZIONE DEGLI UTENTI
A.9.2.5	RIESAME DEI DIRITTI DI ACCESSO DEGLI UTENTI
A.9.4.1	LIMITAZIONE DELL'ACCESSO ALLE INFORMAZIONI
A.9.4.4	USO DI PROGRAMMI DI UTILITÀ PRIVILEGIATI
A.9.4.5	CONTROLLO DEGLI ACCESSI AL CODICE SORGENTE DEI PROGRAMMI
A.12.1.2	GESTIONE DEI CAMBIAMENTI (SISTEMISTICI)
A.12.1.3	GESTIONE DELLA CAPACITÀ
A.12.1.4	SEPARAZIONE DEGLI AMBIENTI DI SVILUPPO, TEST E PRODUZIONE
A.12.3.1	BACKUP DELLE INFORMAZIONI
A.12.5.1	INSTALLAZIONE DEL SOFTWARE SUI SISTEMI DI PRODUZIONE
A.14.1.1	ANALISI E SPECIFICA DEI REQUISITI PER LA SICUREZZA DELLE INFORMAZIO
A.14.2.1	POLITICA PER LO SVILUPPO SICURO
A.14.2.2	PROCEDURE PER IL CONTROLLO DEI CAMBIAMENTI DI SISTEMA
A.14.2.3	RIESAME TECNICO DELLE APPLICAZIONI IN SEGUITO A CAMBIAMENTI NELLE PIATTAFORME OPERATIVE
A.14.2.4	LIMITAZIONI AI CAMBIAMENTI DEI PACCHETTI SOFTWARE
A.14.2.5	PRINCIPI PER L'INGEGNERIZZAZIONE SICURA DEI SISTEMI
A.14.2.6	AMBIENTE DI SVILUPPO SICURO
A.14.2.7	SVILUPPO AFFIDATO ALL'ESTERNO
A.14.2.8	TEST DI SICUREZZA DEI SISTEMI
A.14.2.9	TEST DI ACCETTAZIONE DEI SISTEMI
A.14.3.1	PROTEZIONE DEI DATI DI TEST