Progetto S3L5

GESTIONE DEL RISCHIO INFORMATICO AZIENDALE

Alex Fiorillo
Davide Di Turo
Lisa Bonato
Maria Flavia Minotti
Maria Huapaya
Angelo Di Mauro

BCC BANCA ICCREA

TRACCIA

La settimana scorsa abbiamo visto come strutturare il Risk Assessment NIST SP 800-30, che è utilizzato in diversi punti del NIST RMF SP 800-37 che a sua volta è una componente del NIST CSF 2.0 CSWP 29. In questo progetto andremo a sviluppare uno dei documenti fondamentali per la gestione del rischio:
• Politica di gestione del rischio: questo documento definisce gli obiettivi, i principi e le linee guida generali per la gestione dei rischi all'interno dell'organizzazione.

Scenario
FinCompany è un'importante istituzione finanziaria che offre servizi bancari tradizionali e digitali. Opera in diversi paesi con una vasta rete di filiali fisiche e sistemi informatici interconnessi.

Questi sistemi includono:
• Sistema bancario core per l'elaborazione di transazioni, gestione dei conti e servizi ai clienti
• Applicazioni bancarie online/mobile per l'online banking dei clienti
• Rete aziendale per operazioni interne, comunicazioni e gestione dei dati
• Infrastruttura di sicurezza come firewall, IDS/IPS, autenticazione, crittografia

Essendo un'istituzione finanziaria, gestisce dati altamente sensibili come informazioni finanziarie, identificative e di transazione dei clienti. È fondamentale proteggere questi sistemi e dati da minacce informatiche come attacchi di malware, accesso non autorizzato, furto di dati e interruzioni del servizio.
Scegliete uno o più step (in base alla numerosità del vostro gruppo) del NIST RMF, per ogni task degli step selezionati, definite la politica di gestione del rischio (basta una piccola descrizione) in linea con lo scenario organizzativo proposto, individuando nello specifico se il RA è utilizzato in quella attività e come.
Non va implementato il RA ma vanno definiti solo delle linee guida o dei principi (gli obiettivi sono un plus), su argomenti come:

• Ruoli, responsabilità, processi decisionali e requisiti di segnalazione per la gestione dei rischi.
• Metodologie e criteri per identificare, analizzare e valutare i rischi informatici, tenendo conto di minacce, vulnerabilità, probabilità e impatti.
• Procedure per selezionare, implementare e mantenere i controlli tecnici, operativi e gestionali per mitigare i rischi identificati.
• Processi di test, valutazione e autorizzazione per garantire che i sistemi soddisfino i requisiti di sicurezza e abbiano un livello di rischio accettabile.
• Procedure per monitorare continuamente i controlli di sicurezza, rilevare e rispondere agli eventi di sicurezza e mantenere un livello di rischio accettabile.
• Controlli e requisiti per proteggere la riservatezza, l'integrità e la disponibilità dei dati dei clienti. Formazione e consapevolezza
• Piani per formare e sensibilizzare il personale e gli utenti finali sui rischi informatici e le pratiche di sicurezza.
• Processi di risposta agli incidenti, contenimento, indagine, ripristino e comunicazione per fronteggiare efficacemente le violazioni di sicurezza.
• Cadenze e modalità per la revisione e il reporting della posizione di rischio dell'organizzazione ai dirigenti e alle parti interessate.
• Requisiti di sicurezza per le relazioni con i fornitori e l'approvvigionamento di servizi e tecnologie.

TASK	RESPONSIBLE	POLICY	RA USAGE	GOALS
R-1 Authorization Package	System Owner; Common Control Provider; Senior Agency Official for Privacy	Stabilisce i requisiti e i processi per la creazione e la gestione dei pacchetti di autorizzazione, che includono piani di sicurezza e privacy, report di valutazione della sicurezza e della privacy, piani d'azione e milestone e un riassunto esecutivo	Utilizzati come base per prendere decisioni informate e basate sul rischio da parte degli ufficiali autorizzati. Essi contengono informazioni essenziali sulla sicurezza e sulla privacy dei sistemi, consentendo agli ufficiali autorizzati di valutare la conformità, gestire i rischi e prendere decisioni di accettazione dei rischi.	Raccogliere il pacchetto di autorizzazione e presentarlo al funzionario ordinatore per una decisione sull'autorizzazione.
S-5 Continuous Monitoring Strategy-System	System Owner, Common Control Provider	Sviluppare e implementare una strategia a livello di sistema per monitorare l'efficacia del controllo coerente ed integra la strategia organizzativa di monitoraggio continuo.	identifica i controlli di sicurezza più appropriati per mitigare i rischi associati alle risorse critiche. Implementando questi controlli, l'organizzazione può proteggere meglio i dati sensibili dei clienti, garantire la continuità operativa e mantenere la conformità con le normative di sicurezza	Identificare Controlli Efficaci; Proteggere le Risorse Critiche; Mantenere la Conformità; Ridurre il Rischio Residuo; Garantire l'Efficacia dei Controlli; Promuovere la Consapevolezza della Sicurezza
R-4 Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable.	Authorizing Official	Valutare se il rischio identificato è accettabile per l'organizzazione, bilanciando protezione e funzionalità; Definire chiaramente i termini e le condizioni dell'autorizzazione, inclusi limiti di accesso, procedure operative e requisiti di reporting; Implementare le misure di sicurezza definite e monitorare regolarmente le attività dei sistemi informativi e dei controlli comuni per identificare e mitigare eventuali rischi aggiuntivi o anomalie; Rivedere e aggiornare regolarmente la politica di autorizzazione in base all'evoluzione delle minacce, delle tecnologie e delle esigenze operative dell'organizzazione	L'utilizzo della valutazione del rischio (RA) è fondamentale per determinare se il rischio associato all'operazione o all'uso dei sistemi informativi o dei controlli comuni è accettabile per l'organizzazione. La RA fornisce le informazioni necessarie per prendere decisioni informate sull'autorizzazione, aiutando a identificare e valutare i rischi e le misure di mitigazione appropriate.	Garantire un'adeguata sicurezza delle informazioni attraverso la valutazione e la gestione del rischio derivante dall'operazione o dall'uso dei sistemi informativi o dei controlli comuni, bilanciando le esigenze di sicurezza con le esigenze operative e di business dell'organizzazione.
P-7 Continuous Monitoring Strategy-Organization	Senior Accountable Official for Risk Management or Risk Executive (Function)	La politica verte sull'importanza di monitorare costantemente la sicurezza e la privacy dell'organizzazione, sia a livello interno che nella catena di fornitura. Una strategia di monitoraggio continuo efficace permette di garantire l'autorizzazione continua dei sistemi e l'utilizzo efficiente delle risorse. La strategia deve definire la frequenza del monitoraggio, il metodo di valutazione dei controlli e i requisiti di reportistica. La frequenza minima di monitoraggio deve essere approvata da funzionari senior. L'automazione può essere utilizzata per facilitare un monitoraggio più frequente.	Il Risk Assessment è un elemento cruciale per una strategia di monitoraggio efficace. Permette di: Identificare i rischi da monitorare con priorità; Valutare l'efficacia dei controlli implementati per mitigare i rischi; Informare le decisioni sulla gestione del rischio in modo consapevole; Dimostrare la conformità ai requisiti normativi e agli standard di settore.	Garantire l'autorizzazione continua dei sistemi; Utilizzo efficiente delle risorse; Riduzione del rischio; Migliorare la conformità; Aumentare la fiducia
P-3 Risk Assessment - Organization	Senior Accountable Official for Risk Management or Risk Executive (Function), Senior Agency Information Security Officer, Senior Agency Official For Privacy	Valutare il rischio di sicurezza e privacy a livello organizzativo. Aggiornare i risultati della valutazione del rischio su base continua.	L'organizzazione valuta l'intero panorama dei rischi derivanti dall'operazione dei sistemi informativi, dagli scambi di informazioni e dalle connessioni con altri sistemi e fornitori esterni. Questo processo aiuta a identificare e mitigare i rischi, assicurando che l'organizzazione mantenga un profilo di sicurezza informatica adatto alle sue esigenze e obiettivi aziendali.	Valutazione completa del rischio; Aggiornamento continuo dei risultati; Considerazione delle minacce attuali; Supporto agli obiettivi aziendali; Identificazione dei rischi della catena di fornitura; Definizione di profili di sicurezza informatica; Collaborazione tra le parti interessate; Miglioramento continuo della sicurezza e della privacy
P-2 Risk Management Strategy	Head of Agency	La politica verte sull'importanza di stabilire una strategia di gestione del rischio che includa la determinazione della tolleranza al rischio dell'organizzazione. La strategia di gestione del rischio guida e informa le decisioni basate sul rischio, inclusi come il rischio di sicurezza e privacy viene inquadrato, valutato, risposto e monitorato. La strategia deve definire esplicitamente le minacce, le assunzioni, i vincoli, le priorità, i compromessi e la tolleranza al rischio utilizzati per prendere decisioni di investimento e operative.	Identificare i rischi da monitorare con priorità; Valutare l'efficacia dei controlli implementati per mitigare i rischi; Informare le decisioni sulla gestione del rischio in modo consapevole; Dimostrare la conformità ai requisiti normativi e agli standard di settore	Garantire che la tolleranza al rischio dell'organizzazione sia esplicitamente definita; Utilizzare metodi di valutazione del rischio e strategie di risposta al rischio accettabili; Stabilire un processo per valutare in modo coerente i rischi di sicurezza e privacy in tutta l'organizzazione; Implementare approcci per monitorare il rischio nel tempo