Regolamento del processo di Identificazione e classificazione degli asset

Procedura emessa il 27/09/2022

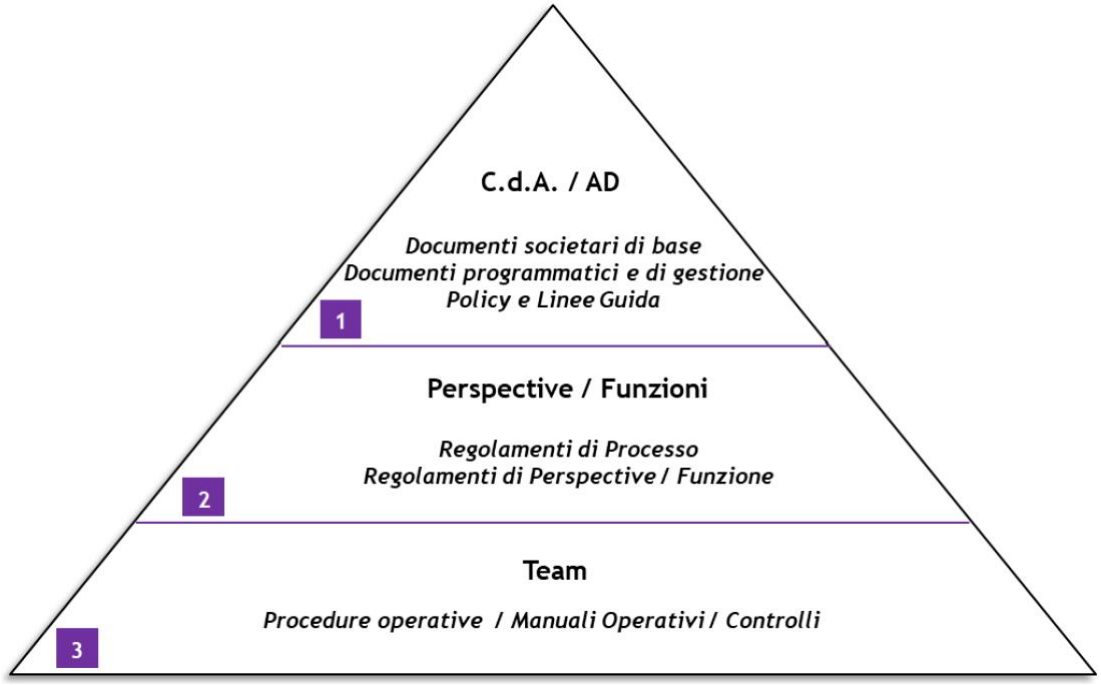
Owner della procedura: IT Operation Security and Governance

Indice

1 OBIETTIVO DEL DOCUMENTO

Obiettivo del presente documento è quello di definire il processo con la quale viene realizzata, nonché aggiornata, la mappatura degli asset aziendali a supporto dei Processi cd. "Core" e la relativa compilazione delle informazioni necessarie, al fine di determinare la classificazione di ciascun asset e di definire un adeguato livello di protezione delle informazioni ad essi associate.

Con riferimento alla "Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna", il presente documento si colloca al secondo livello della piramide documentale richiamata nello schema seguente.



2 AMBITO DI APPLICAZIONE

La presente procedura si applica a Flowe S.p.A. Società Benefit (qui di seguito Flowe o la Società).

3 AGGIORNAMENTO DEL DOCUMENTO

L'aggiornamento del documento è a cura di IT Operation Security & Governance che dovrà provvedere a revisionarlo con cadenza almeno annuale o qualora si verifichi un cambiamento sostanziale, che possa influire in modo diretto o indiretto sul processo qui descritto.

4 ATTORI, RUOLI E RESPONSABILITA'

Il modello organizzativo adottato dalla Società per l'identificazione e la classificazione degli asset prevede il coinvolgimento delle seguenti figure:

4.1 IT Operation Security & Governance

IT Operation Security & Governance ha la responsabilità di:

- Individuare, con il supporto delle Funzioni di Risk Management e dal Settore IT Security di Banca Mediolanum, in virtù del contratto di *outsourcer* in essere, i processi "Core" di Flowe;
- Identificare, con il supporto dei Key Users, gli Asset a supporto dei processi Core;
- Organizzare incontri con i Key Users per raccogliere tutte le informazioni necessarie alla compilazione della Matrice Applicativi;
- Coinvolgere le Funzioni Risk Management e il Settore IT Security di Banca Mediolanum per supporto nell'identificazione dei processi Core;
- Compilare la Matrice Applicativi con le informazioni raccolte ed, eventualmente, consolidare e/o richiedere ulteriori informazioni mancanti;
- Classificare gli asset in "Critico" o "Non critico" sulla base delle informazioni raccolte durante il processo definito nel presente documento;
- Aggiornare la mappatura degli asset almeno annualmente o in caso di cambiamenti rilevanti.

4.2 Key User

I *Key User* sono i responsabili per la gestione degli asset e vengono suddivisi in *Key Business User*, cioè l'owner dell'Unità Organizzativa (U.O. di Business impattata dal processo) fruitrice dell'asset per esercitare il processo aziendale, *e Key ICT User*, cioè l'utente tecnico IT identificato per la gestione e la manutenzione dell'asset.

Tali soggetti hanno la responsabilità di collaborare con IT Operation Security & Governance nella realizzazione dell'inventario degli asset e dovranno essere disponibili a fornire, nel corso dell'attività di assessment, tutte le informazioni richieste.

4.3 Funzione di Risk Management e Settore IT Security di Banca Mediolanum

La Funzione Risk Management ed il Settore IT Security della Capogruppo Banca Mediolanum, in virtù del contratto di *outsourcer* in essere, vengono coinvolte da IT Operation Security & Governance per supporto nell'identificazione dei processi "Core" per Flowe.

5 STRUMENTO A SUPPORTO DEL PROCESSO

Lo strumento utilizzato a supporto dell'attività di identificazione e classificazione degli asset è la Matrice Applicativi in cui vengono raccolte tutte le informazioni inerenti agli asset aziendali, sottostanti ai processi Core, e ai dati in essi trattati.

6 FASI DEL PROCESSO DI IDENTIFICAZIONE E CLASSIFICAZIONE DEGLI ASSET

La Società, nell'osservare il flusso previsto per l'identificazione e la classificazione degli asset, è tenuta a rispettare i principali requisiti normativi e gli standard internazionali che suddividono le aree tematiche da trattare come segue:

- **Anagrafica**, che fa riferimento alle informazioni specifiche relative all'asset;
- **Third Party Management**, che fa riferimento alla gestione delle interazioni con tutti i soggetti esterni che includono sia le terze parti contrattuali sia quelle extracontrattuali;
- **Ownership e Accountability**, che indica i Key User (sia Business che ICT);
- **Continuità Operativa**, che descrive le capacità intrinseche degli asset di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente;
- **Incident**, che fornisce informazioni rispetto alla gestione degli incidenti e il corrispettivo ambito normativo;
- **Cyber Security**, che analizza il livello di protezione delle applicazioni da eventuali minacce;
- **Dependecies**, che delinea i flussi di trasferimento automatico e schedulato di dati e di informazioni sia in input che in output;
- **PSD2**, che fa riferimento alla parte normativa dei servizi di pagamento connessi alle app;
- **Data Governance**, che indica la tipologia dei dati trattati dall'asset e se rispettano le policy interne in ambito di Data Governance;
- **Privacy & GDPR**, che si occupa dell'analisi sulla protezione dei dati personali e della privacy dei dati trattati da ogni asset.

IT Operation Security & Governance procede all'identificazione e classificazione degli asset osservando le seguenti fasi:

1. Identificazione dei processi Core di interesse;
2. Individuazione degli Asset che impattano sui processi Core;
3. Classificazione degli Asset;
4. Aggiornamento dell'inventario e della classificazione.

6.1 IDENTIFICAZIONE DEI PROCESSI CORE DI INTERESSE

IT Operation Security & Governance, supportata dalle Funzioni Risk Management e dal Settore IT Security di Banca Mediolanum, in virtù del contratto di *outsourcer* in essere, procede all'identificazione dei processi Core di interesse di Flowe e dei relativi Key Business Users tenendo conto della Tassonomia dei processi aziendali e della struttura organizzativa.

6.2 INDIVIDUAZIONE DEGLI ASSET IMPATTANTI

6.2.1 ASSESSMENT CON I KEY BUSINESS USERS

Una volta definiti i processi Core e individuati i rispettivi referenti, è necessario procedere con l'individuazione degli asset per i quali esiste un impatto sulla sicurezza delle informazioni.

In primo luogo, IT Operation Security & Governance dovrà pianificare ed avviare un'attività di assessment che verrà realizzata tramite incontri con i Key Business Users referenti di processo, al fine di raccogliere la lista degli asset impattanti sul processo di riferimento e le relative informazioni.

6.2.2 DEFINIZIONE DELL'INVENTARIO DEGLI ASSET

IT Operation Security & Governance, raccolte tutte le informazioni necessarie nel corso delle fasi precedenti, dovrà procedere a inserire tali dettagli all'interno della "Matrice Applicativi", che costituisce l'inventario degli Asset.

Al fine del consolidamento dell'inventario, IT Operation Security & Governance, qualora fosse necessario, pianificherà un ulteriore incontro con i Key Business Users per condividere e consolidare le informazioni raccolte nel precedente incontro e/o richiedere ulteriori informazioni mancanti.

6.3 CLASSIFICAZIONE DEGLI ASSET

IT Operation Security & Governance, dopo aver compilato l'inventario degli asset con tutte le informazioni, classificherà ogni information asset al fine di identificare per ciascuno di questi le misure di sicurezza da implementare.

IT Operation Security & Governance dovrà, quindi, associare ad ogni asset il livello di criticità emerso dalla Business Impact Analysis per il processo di riferimento, attribuendo uno dei seguenti valori:

- Critico
- Non Critico

La presente classificazione determinerà la prioritizzazione degli Asset.

6.4 AGGIORNAMENTO DELL'INVENTARIO E DELLA CLASSIFICAZIONE

IT Operation Security & Governance procederà all'aggiornamento dell'inventario almeno annualmente o nel caso di variazioni degli asset o delle informazioni ad essi relative.

7 NORMATIVA

Nel presente capitolo si richiama il contesto normativo di riferimento per le attività in esame. L'elenco fornito non si ritiene esaustivo e viene riportato principalmente allo scopo di richiamare l'attenzione sui principali riferimenti, della normativa generale ed interna aziendale, sui quali si fonda la presente procedura.

Normativa interna:

- Policy di Sicurezza di Flowe
- Tassonomia dei processi aziendali
- Flowe_Relazione Struttura Organizzativa

Normativa esterna:

- EBA/GL/2017/05 “Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell’informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP)” e successivi aggiornamenti;
- Banca d’Italia Circolare n. 285 del 17 dicembre 2013 – Disposizioni di vigilanza per le Banche
- EBA/GL/2019/02 - Orientamenti in materia di esternalizzazione e successivi aggiornamenti;
- Direttiva (UE) 2015/2366 PSD2 – (Payment Services Directive 2) e successivi aggiornamenti;
- Provvedimento Della Banca d’Italia de 23 luglio 2019, Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica e successivi aggiornamenti;
- *Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 e successivi aggiornamenti*.