Offerta Gestione Sicurezza nella trattazione di accesso ai documenti

Allegato Tecnico A

Il presente documento descrive alcuni scenari applicabili al contesto AIFA per la revisione dell'attuale organizzazione e gestione della piattaforma ownCloud al fine di rendere ottimale la configurazione: attuare le politiche di classification e policy enforcement indicati dalla casa madre

https://doc.owncloud.com/server/next/admin_manual/enterprise/document_classification/classification_and_policy_enforcement.html

ed alle best practices di utilizzo, garantendo l'introduzione delle funzionalità richieste per il raggiungimento degli obiettivi condivisi.

Questo approccio garantisce di rispondere alle esigenze di:

- Compliance GDPR
- Gestione del rischio su potenziale data breach
- Maggiore consapevolezza dell'utenza sull'utilizzo dello strumento
- Maggiore consapevolezza dell'utenza sulla gestione del dato

La proposta prevede l'applicazione del modello di revisione per le sole aree coinvolte nel piano di riclassificazione, andando a definire in ambiente di PreProduzione le strutture e le configurazioni richieste per soddisfare i requisiti necessari a garantire una gestione adeguata ai livelli di compliance.

1 Organizzazione

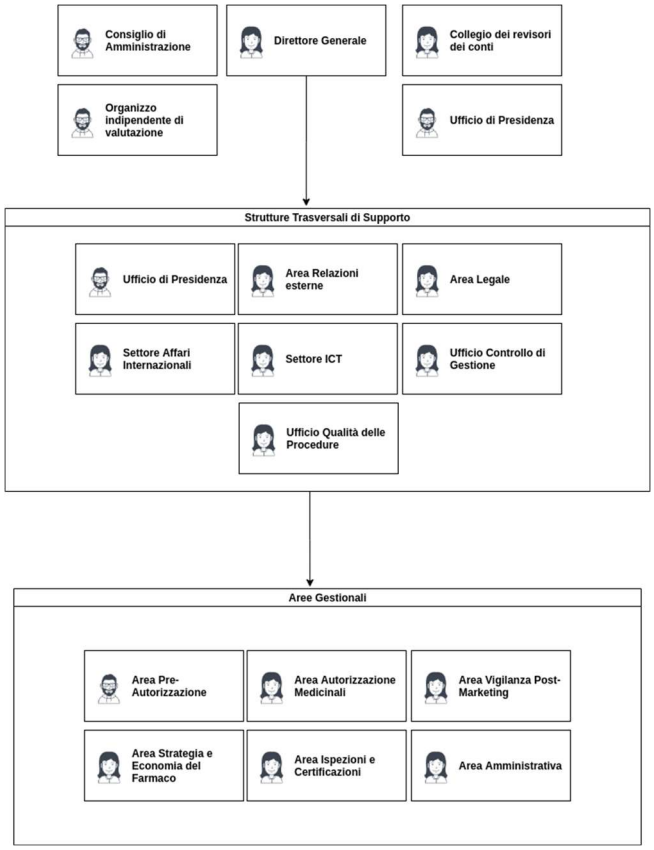
Il processo prevede per i soli documenti classificati la creazione di un'area suddivisa per Gruppi direzionali/unità organizzative sulle quali assegnare la visibilità per Gruppi/Entità in modo da non rendere vincolante la visibilità per singolo Utente.

Questo dovrebbe permettere di facilitare l'assegnazione dei privilegi ed il controllo sulle policy di accesso, andando ad esempio a prevedere un gruppo per ogni Ruolo/Struttura/Area Gestionale, con visibilità sulle proprie aree di lavoro dirette al primo livello.

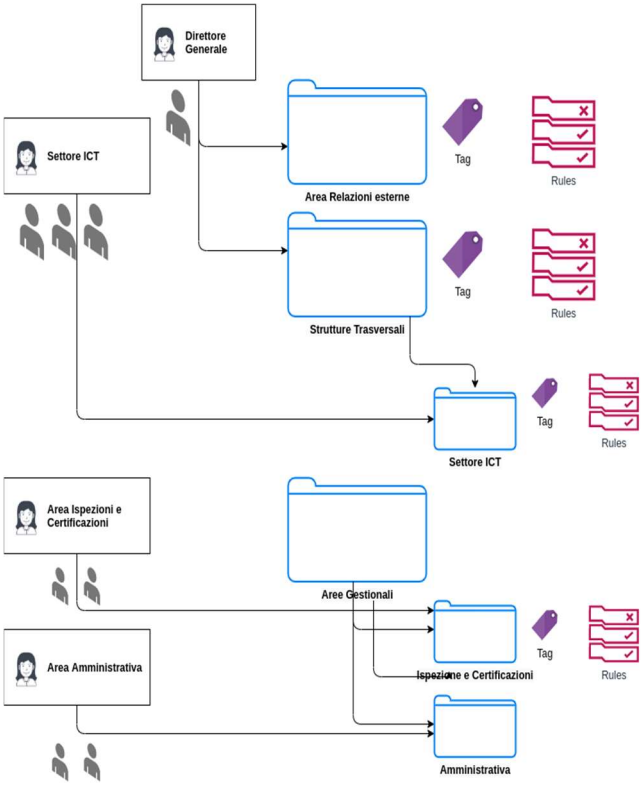
E' possibile definire una relazione diretta del tagging al folder in base al nome del folder o ad un tag (invisibile) assegnato al folder, in alternativa occorrerà definire una regola di utilizzo dei tag

- Adeguamento ambiente di collaudo ownCloud
- Revisione Gruppi e struttura gerarchica folder
- Revisione flusso provisioning Account

Organizzazione AIFA



Modello OwnCloud



2 Classificazione

Specifiche tecniche

❖ Classificazione Statica

Per quanto riguarda le regole di classificazione statica si applicano le tipologie di tag sulla base delle attuali funzionalità presenti

Visible

All users may see, rename, and apply these tags to files and folders.

Static

Only users in the specified groups can assign and un-assign the tag to a file. However, only admins can rename and edit the tag.

Restricted

Tags are assignable and editable only to the user groups that you select. Other users can filter files by restricted tags, but cannot tag files with them or rename them. The tags are marked (restricted).

Invisible

Tags are visible only to ownCloud admin.

❖ Classificazione automatica

Per quanto riguarda invece le regole di classificazione automatica, al fine di semplificare il processo di qualificazione del nuovo e del vecchio, suggeriamo di attuare un processo di revisione dei documenti attraverso l'utilizzo delle funzionalità libreoffice TSCP per tutti i documenti classificati, attraverso l'utilizzo di opportuni template

Il flusso prevede quindi

1. utilizzo di un modello di documento pre-classificato per tutto il nuovo prodotto
2. utilizzo di libreoffice per effettuare la classificazione del documento secondo gli standard già presenti, adeguando la nomenclatura in base alle proprie policy, secondo quanto indicato da https://wiki.documentfoundation.org/TSCP-classification

Al fine quindi di rendere il sistema coerente con le policy di classificazione attualmente in uso in AIFA e con i requisiti richiesti dagli standard ISO 27001 (A.8.1.1, A.8.2.1, A.8.2.2, A.8.2.3), si prevede di attuare i seguenti livello di classificazione

- uso interno
- confidenziale
- riservato

- segreto

una volta prodotto il file policy potrà essere utilizzato come base per il processo di classificazione del vecchio.

In questo modo sarà possibile soddisfare i requisiti per la classificazione automatica di ownCloud attraverso le property di workflow

property[@name='urn:bails:IntellectualProperty:BusinessAuthorizationCategory:Name']/vt:lpwstr

3 Policy di accesso

La definizione ed applicazione delle politiche di accesso e delle relative regole si suddivide sulla base del modello di classificazione adottato. Per tutto ciò che verrà classificato in automatico attraverso l'attribuzione via workflow o attraverso un processo manuale gestito sulla base dei tag indicati ai punti precedenti è possibile definire la regola che garantisca l'assegnazione delle sotto indicate policy

- Prevent upload
- Prevent link sharing
- Unprotected links expire

integrando attraverso opportune regole (access policy) del modulo file-firewall le restrizioni di accesso ai documento/cartelle, in modo tale da evitare che tali documenti possano essere acceduti da dispositivi esterni e/o da asset aziendali non compliance, per garantire il corretto collegamento occorre assegnare alla regola il *"tag di classificazione"*.