DocuWare

Archiviazione dei documenti

Standard di sicurezza

Violazioni della sicurezza, perdite di dati, difficoltà legate alla gestione delle versioni e contenziosi a seguito di violazioni delle normative: tutto ciò ormai sembra essere diventato di “ordinaria amministrazione”.

Spesso, però, questi problemi sono completamente autoinflitti. In molti casi, le aziende optano per standard di sicurezza meno rigidi per comodità o perché pensano sia un tema troppo complesso e non sanno da dove cominciare. Queste aziende a volte non riescono nemmeno a implementare processi che garantiscano l’integrità e la trasparenza delle informazioni perché non credono di essere esposte a rischi.

Le società più robuste che adottano misure serie per garantire la sicurezza dei documenti raramente devono fare i conti con errori di questo tipo.

L’importanza della sicurezza dei documenti

I documenti sono un elemento fondamentale per il funzionamento della tua azienda. È fondamentale che questo scrigno di dati sia sempre protetto. Prova a rispondere alle seguenti domande per capire a che punto sei in termini di sicurezza dei documenti.

Per le aziende:

- Siamo protetti contro le violazioni di sicurezza interne, intenzionali o accidentali?
- Siamo protetti contro le minacce esterne di hacking?
- Saremmo in grado di recuperare le nostre informazioni in caso di calamità naturale?
- Saremmo in grado di difenderci dalle accuse di cattiva gestione dei dati?
- Siamo protetti da pesanti sanzioni finanziarie?

Per gli utenti:

- Sono in grado di accedere in qualsiasi momento al documento di cui ho bisogno?
- Sono sicuro di usare la versione giusta?
- Sono in grado di archiviare in modo sicuro le mie informazioni aziendali senza che siano accessibili a persone non autorizzate?
- Dispongo di un processo per rispettare i periodi di conservazione delle informazioni sensibili dal punto di vista legale?
- So come prevenire gli attacchi di social hacking e social engineering?

Questo documento ti presenta i più moderni standard di sicurezza e protezione per l’archiviazione e l’utilizzo dei documenti e rappresenta una guida alla ricerca di un fornitore di software di gestione documentale.

1

Crittografia e diritti di accesso

Partiamo dalle fondamenta della piattaforma. Come sono protetti i dati digitali? Quali sono i punti più deboli tra i sistemi? In che modo è possibile controllare l'accesso alle informazioni? In che modo un'azienda può proteggersi dalle violazioni delle informazioni, dagli attacchi informatici e dai furti?

Crittografia e diritti di accesso

Autenticazione

Tutti i documenti devono essere accessibili esclusivamente tramite autenticazione con un nome utente e una password unici. Questo non solo consente di assegnare diritti di accesso specifici, ma garantisce una traccia di controllo totale relativa al documento consultato e da chi, nonché alle azioni eseguite.

Traffico di dati

L'intero traffico tra sistemi e componenti deve essere crittografato con HTTPS. Il traffico non protetto espone i sistemi a potenziali attacchi di pirateria informatica. L'HTTP non dispone del livello di sicurezza TLS/SSL e consente agli hacker di intercettare dati critici come password e dati finanziari.

Accesso controllato

L'accesso ai documenti prevede un controllo a più livelli. Da un lato, interi gruppi possono avere accesso a un'ampia categoria di documenti. Dall'altro, tali gruppi richiedono l'accesso a ciò che possono fare con un documento. I diritti di accesso devono essere possibili anche a livello individuale.

Per esempio, un dipendente delle risorse umane può accedere alla maggior parte dei documenti dei dipendenti come CV e valutazioni della performance. I dipendenti e i manager possono accedere alle valutazioni della performance. Inoltre, i dipendenti possono accedere personalmente alle informazioni finanziarie e assicurative.

Dovrebbe essere altresì possibile limitare l'accesso a un documento sulla base dei dati indicizzati del documento stesso, le caratteristiche principali dei metadati utilizzati per descrivere il contenuto e lo scopo di un documento.

Crittografia

I documenti devono essere crittografati con una chiave di almeno 256 bit. AES (256 bit), una crittografia di livello militare, rappresenta l'attuale standard del governo statunitense per i documenti classificati di livello top secret, a prova di attacchi futuri.

2

Ridondanza e protezione dai virus

La ridondanza dell'archiviazione dei dati rappresenta un altro pilastro della sicurezza delle informazioni. È importante chiedersi: in caso di interruzione del sistema, i backup potranno garantire la continuità delle attività aziendali? La ridondanza e la protezione dei dati dai malware sono necessarie per garantire la massima tranquillità a livello aziendale.

Ridondanza e protezione dai virus

Ridondanza attiva

Qualsiasi software di gestione documentale, sia in cloud che on-premise, dovrebbe avere almeno due livelli di ridondanza di archiviazione, oltre a un terzo livello di ridondanza delimitata geograficamente per una protezione dalle calamità naturali.

Queste protezioni rappresentano un vantaggio fondamentale nei moderni sistemi cloud. Puntando sui servizi di infrastruttura cloud di un provider come Microsoft, è possibile sfruttare i principali centri dati di tutto il mondo per garantire una protezione costante e sincronizzata delle informazioni. Altri fornitori di infrastrutture cloud sono Google, Amazon e Oracle.

Sovranità dei dati

Per molte aziende è estremamente importante garantire la sovranità dei propri dati all'interno di confini specifici. Per esempio, le aziende statunitensi di solito non vogliono che i propri dati siano archiviati in Sud America; le aziende dell'UE vogliono evitare che i propri dati siano archiviati in Nord America, a meno che non svolgano attività commerciali in questa regione.

I fornitori di cloud devono garantire che tutti i dati e relativi backup rimangano all'interno dei confini in cui il cliente e i suoi dati godono di protezione ai sensi della legge.

Protezione da virus e malware

I criptovirus si infiltrano nei documenti e si attivano una volta aperti sul dispositivo locale dell'utente. I sistemi di gestione documentale devono proteggere attivamente da queste potenziali minacce, sia per l'ambiente dell'utente che per la piattaforma software stessa.

3

Politiche di conservazione e conformità

Una volta che la crittografia, i diritti di accesso e la ridondanza dell'archiviazione sono stati definiti, l'azienda deve decidere come gestire le informazioni stesse. Le politiche di conservazione definiscono cosa viene salvato e quando i dati possono essere cancellati definitivamente. La conformità normativa fornisce indicazioni legali per la gestione delle informazioni.

Politiche di conservazione e conformità

Politiche di conservazione

Alcuni tipi di documenti devono essere conservati all'interno di un'azienda per un determinato numero di anni stabilito per legge. Ad esempio, le fatture devono essere conservate per dieci anni in Italia prima di poter essere eliminate.

In precedenza, le aziende avevano scaffali pieni di scatole in cui conservavano tali documenti, per poi passare pagina per pagina attraverso un dispositivo di monitoraggio. La gestione digitale dei documenti risolve questo problema, tuttavia continuano a vigere le stesse regole di conservazione. Un sistema di gestione documentale deve fornire gli strumenti di gestione del workflow per garantire la protezione o la cancellazione in momenti prestabiliti, al fine di assicurare la protezione dell'azienda in caso di controversie.

Principali iniziative e normative di conformità

Negli ultimi decenni abbiamo assistito a un rinnovato interesse nei confronti della sicurezza delle informazioni, sia in termini di protezione dei diritti individuali attraverso la gestione dei dati personali da parte di terzi, sia in termini di trasparenza fiscale e molto altro.

Per esempio:

- **GDPR:** il Regolamento generale sulla protezione dei dati è un insieme di norme e standard europei progettati per proteggere i dati personali o le informazioni personali identificabili attraverso la governance dei dati
- **Sarbanes-Oxley:** previene gli errori contabili e le pratiche di rendicontazione fraudolente attraverso un'accurata divulgazione delle informazioni.

4

Integrità e auditing

È fondamentale garantire la totale integrità dei documenti ogni volta che vi si accede. Anche gli standard di crittografia più sicuri e i diritti di accesso più rigidi servono a poco se non ci si può fidare dell'autenticità del documento stesso.

Integrità e auditing

Firme elettroniche

Gli utenti devono poter firmare i documenti con una firma elettronica legalmente valida. La **firma elettronica qualificata** è il livello di firma più sicuro. Secondo il regolamento europeo in materia di identificazione elettronica e servizi fiduciari per transazioni elettroniche (eIDAS), la validità legale di una firma elettronica qualificata corrisponde a quella di una firma autografa. Questo tipo di firma elettronica garantisce che la firma sia legittima e che il documento non sia stato manipolato, poiché una Certification Authority autorizzata ha emesso il certificato digitale e autenticato il firmatario.

Registrazione delle modifiche

L'unico modo per condurre verifiche accurate e approfondite è registrare ogni accesso e annotare lo stato del workflow di un determinato documento. In questo modo è possibile ricostruire un intero storico. Questo dovrebbe essere facilmente accessibile in formato CSV o in un altro formato di file diffuso.

Gestione delle versioni

Per mantenere l'integrità dei documenti è importante capire cosa è cambiato esattamente tra una versione e l'altra e garantire che gli utenti modifichino solo la versione più recente. Bloccando i documenti "check out" si evitano eventuali modifiche e si mantiene un registro accurato di chi ha modificato cosa.

5

Importanti standard di settore

Esistono numerosi standard specifici per ciascun Paese e riconosciuti a livello internazionale in termini di qualità, sicurezza e completezza di funzioni del sistema. Quando cerchi il sistema più adatto per conservare i documenti importanti per la tua azienda, assicurati che il tuo fornitore soddisfi questi standard fondamentali.

Esempi di standard di sicurezza e normative ufficiali

Qualità complessiva del software e del cloud provider

- **ISO 9001:** valutazione eccellente nel controllo della qualità nella produzione/manifattura del software
- **ISO 15489:** strategie e principi comprovati, affidabili e consolidati per la gestione dei documenti aziendali
- **ISO 27001:** standard di massima qualità per la produzione, l'introduzione, il funzionamento, il monitoraggio, la manutenzione e il miglioramento di un sistema di gestione documentale per la sicurezza delle informazioni
- **ISO 27017:** massima sicurezza dei dati per il cloud; i dati sono protetti dall'accesso di terzi e solo il cliente può accedervi in qualsiasi momento
- **CSA:** requisiti di hosting per la sicurezza, la privacy, la conformità e la gestione del rischio definiti nella Cloud Controls Matrix della Cloud Security Alliance
- **Keypoint Intelligence / Buyer's Laboratory:** analisi indipendente per il settore dei prodotti specializzati per ufficio
- **SOC:** i Service Organization Controls sono una serie di standard che si concentrano sui controlli di una società di servizi relativi a sicurezza, disponibilità, integrità dell'elaborazione, riservatezza e/o privacy.

  Esistono diversi livelli di conformità SOC. Per esempio, lo status SOC 2 di tipo 1 dimostra la conformità in un momento specifico. L'audit di tipo 2, più rigoroso, misura la conformità continua. Le società di servizi includono i fornitori di software cloud (SaaS).
- **NIST SP 800-171:** standard e linee guida per la protezione dei sistemi informativi delle agenzie federali statunitensi

Per la gestione dei documenti finanziari

- **GoBD (Germania):** archiviazione a lungo termine e senza manomissioni ai sensi dell'HGB (Codice commerciale tedesco) e del codice fiscale AO
- **Agencia Tributaria (Spagna):** requisiti delle autorità fiscali spagnole in termini di archiviazione di documenti cartacei digitalizzati
- **GeBüV/AccO (Svizzera):** ordinanza sulla tenuta e conservazione dei conti

6

Requisiti dei fornitori di gestione documentale

Quando si valuta un software di gestione documentale e di workflow, si parte dalla sicurezza del sistema candidato. Questa base deve essere totalmente affidabile: supporta le informazioni che contano per la tua azienda. Senza di essa, le altre caratteristiche e funzionalità non hanno alcuna importanza.

Requisiti dei fornitori di gestione documentale

Potrebbe aiutarti una checklist per fare una valutazione equa tra i sistemi candidati in termini di caratteristiche di sicurezza, conformità e protezione.

Il sistema ...

- ✓ Prevede l'autenticazione con nome utente e password?
- ✓ Invia tutti i dati tra i componenti web-based via HTTPS?
- ✓ Abilita i diritti di accesso per gruppi, ruoli, individui e diritti basati sui documenti?
- ✓ Fornisce una crittografia moderna a 256 bit?
- ✓ Esegue attivamente il backup di tutti i dati e li conserva in un'area geograficamente separata?
- ✓ Conserva i dati entro confini legalmente sovrani?
- ✓ Protegge da criptovirus e malware dannosi?
- ✓ Abilita il workflow per l'applicazione di misure di conservazione?
- ✓ Ti aiuta a soddisfare gli standard di conformità specifici per la gestione delle informazioni?
- ✓ Conserva l'integrità del documento utilizzando le firme elettroniche?
- ✓ Registra tutte le modifiche per creare una traccia di controllo completa?
- ✓ Gestisce le versioni attive e precedenti dei documenti?
- ✓ Soddisfa gli standard di sicurezza e qualità di terzi riconosciuti?
- ✓ Consente un'integrazione sicura con altri sistemi aziendali come CRM e ERP?
- ✓ Assicura il non ripudio?
- ✓ Garantisce la massima operatività e disponibilità?
- ✓ Fornisce assistenza 24/7?

DocuWare

Chi è DocuWare

DocuWare è un fornitore leader di soluzioni per la gestione documentale e l'automazione del workflow. Con una rete di oltre 800 partner validi e affidabili, DocuWare aiuta circa 19.000 clienti in oltre 100 paesi a semplificare i processi attraverso digitalizzazione, automazione e trasformazione.

start.docuware.com

DocuWare rispetta le persone e i gruppi di persone di qualsiasi genere, garantendo un uso non sessista e non discriminatorio del linguaggio, sia nella comunicazione interna che esterna, passata e futura.