RICOH
imagine. change.

Atténuer les risques grâce à la gouvernance de l'information

Utiliser l'automatisation pour améliorer la stratégie d'entreprise, la conformité et les initiatives de sécurité de l'information

Transformer les données en informations

Dans de nombreux secteurs, de la santé à l'éducation en passant par l'administration, les services financiers, l'industrie manufacturière et bien d'autres encore, l'immense volume de données générées quotidiennement peut être écrasant. La quantité de données augmente si rapidement que l'on estime que 90 % des données mondiales ont été créées au cours des deux dernières années.[1]

Le déluge de données actuel peut être difficile à gérer sans les systèmes et les processus appropriés pour en discerner le sens. L'accélération des données est si choquante qu'elle est omniprésente que les organisations sont obligées non seulement de gérer et de sécuriser les données dont elles disposent, mais aussi de prendre de l'avance sur cette tempête de données qui ne cesse de s'intensifier.

La plupart de ces données peuvent être très précieuses pour une entreprise, mais seulement si vous disposez des outils et des processus nécessaires pour en tirer de la valeur et du sens. **En transformant des données brutes en informations structurées, consultables et exploitables, les entreprises peuvent découvrir des perspectives et favoriser une meilleure prise de décision.**

Mais comment? Pendant des années, les solutions de **gestion de contenu d'entreprise (GCE)** ont été couramment utilisées dans les secteurs de l'administration, de la santé et de l'éducation, où la conformité était une exigence clé. Les solutions GCE centralisent et organisent les informations et automatisent le stockage, la gestion, l'organisation et la distribution des documents et des fichiers multimédias.

Cependant, avec la prolifération du travail hybride et à distance, la GCE est devenue un avantage concurrentiel majeur pour de nombreux autres secteurs en raison de sa capacité à gérer efficacement les informations et permettre l'efficacité, augmenter la productivité, réduire les erreurs et améliorer les résultats commerciaux.

394 ZB

Croissance mondiale des données d'ici 2028.[2]

2,5 QN

Des quintillions de données sont créés chaque jour. [3]

[1] G2. « Plus de 85 statistiques sur les mégadonnées pour cartographier la croissance en 2025. » 11 décembre 2024.
[2] Statista. « Volume de données/informations créées, capturées, copiées et consommées dans le monde de 2010 à 2023, avec des prévisions de 2024 à 2028. » 1er novembre 2024.
[3] G2. « Plus de 85 statistiques sur les mégadonnées pour cartographier la croissance en 2025. » 11 décembre 2024.

Faire de la gouvernance de l'information une priorité

La protection de vos informations **commence par la connaissance de ce que vous possédez, de l'endroit où elles se trouvent et du risque qu'elles pourraient poser si elles ne sont pas protégées.** Une fois que les données sont transformées en informations, les organisations doivent comprendre comment et où ces informations entrent dans l'entreprise (informations entrantes) ; comment ces informations seront utilisées et par qui, et quelles applications devront utiliser ces données (transfert) ; et enfin, où ces informations iront ou seront stockées (sortantes). Tout au long de ce parcours, la conformité, le risque et la sécurité doivent jouer un rôle majeur.

Les entreprises doivent tenir compte des risques suivants : perte d'information, confidentialité, cybermenaces, vol, destruction accidentelle ou intentionnelle de données critiques, attaques par déni de service et code malveillant, entre autres. La sécurité ne consiste pas seulement à cocher les cases pendant le processus d'approvisionnement, elle devient rapidement un moteur important du marché, car de plus en plus d'entreprises exigent la conformité, exigeant que les partenaires et les fournisseurs respectent des normes strictes de sécurité et de confidentialité. Dans le monde actuel des cyberattaques de plus en plus complexes et sophistiquées, la sécurité devrait être attendue dans toute l'entreprise, mais pour beaucoup, il s'agit d'un avantage concurrentiel.

> **Le cadre et la pratique de l'intégration de la conformité et de la sécurité des informations de l'entreprise sont la définition que nous donnons à la gouvernance de l'information.**

Le maintien du contrôle de vos renseignements tout en respectant les règlements atténuera les risques. La gouvernance de l'information se concentre sur la façon de créer, de saisir, de gérer, d'administrer, de collaborer et d'éliminer l'information organisationnelle. Cela nécessite un effort coordonné et une stratégie d'orchestration des personnes, des processus et de la technologie. En termes simples, considérez-le comme une liste de contrôle géante pour assurer la sécurité et la conformité des informations des clients, des partenaires et des informations internes

Préparer le terrain : voici pourquoi c'est important

L'analyse des données, la recherche et les études sur la cybersécurité et la gouvernance de l'information nous indiquent que les renseignements commerciaux sont à risque. Une approche holistique et axée sur les données dans toute l'organisation est nécessaire pour réussir. Sinon, la confiance et l'expérience des clients, la conformité et la rentabilité sont à risque.

80 %

« D'ici 2027, 80 % des initiatives de gouvernance en matière de diversité et acquisition échoueront en raison de l'absence d'une crise réelle ou fabriquée. »[4]

21 jours

Une attaque par rançongiciel entraîne en moyenne 21 jours d'indisponibilité et le coût moyen d'une indisponibilité imprévue s'élève désormais à 14 000 dollars par minute.[7]

1 ECM

Un système de gestion d'entreprise centralisé serait avantageux pour les entreprises en améliorant la conformité de 42 %, la connaissance des clients de 38 % et la sécurité du contenu de 38 %.[5]

61 %

Plus de 61 % des organisations ont défini une initiative de sécurité Zero Trust avec une vérification et une validation continues pour protéger leurs informations[8]

Risque no 1

Les risques liés à la cybersécurité et aux données de tiers pour les entreprises se classent au premier rang en matière de préoccupations.[6]

34 %

Alors que les dépenses en matière de cybersécurité ont augmenté à un taux de croissance annuel composé d'environ 10 % au cours de la dernière décennie, le TCAC des violations a atteint le chiffre alarmant de 34 %.[9]

[4] Gartner®, Enhance D&A Governance With a Graduated Trust Model, 11 October 2024.
GARTNER est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses filiales aux États-Unis et dans le monde entier, et est utilisée ici avec leur autorisation. Tous droits réservés.
[5] IDC. « State of Content Services Survey. ». Juin 2023, n = 714.
[6] KPMG. « Board oversight of third-party risk management. » 2024.
[7] JumpCloud. « 2024 Ransomware Attack Statistics & Trends to Know. » 22 octobre 2024.
[8] SentinelOne. « 10 Zero Trust Solutions for 2025. 17 décembre 2024.
[9] Security Bouldevard. « Top 7 Critical Security Challenges (and How to Solve Them). » 19 décembre 2024.

Trois éléments clés de la gouvernance de l'informatione

Votre mantra en matière de gouvernance et de sécurité de l'information devrait être : sachez ce que vous avez, pourquoi vous l'avez et quel est le risque de le conserver.

Pour ce faire, des solutions d'automatisation comme le GCE, le traitement intelligent des documents (PPI) et l'automatisation robotisée des processus (ARP) sont utiles pour gérer vos données et vos informations tout au long de leur cycle de vie. Voici quelques-uns des éléments essentiels dont vous avez besoin pour créer votre approche de gouvernance de l'information, ainsi que d'autres éléments importants à prendre en considération :

1. Un système de gestion de l'information et des dossiers
2. Se concentrer sur la connaissance de l'emplacement de vos informations
3. Les processus automatisés font partie intégrante

1. Un système de gestion de l'information et des dossiers

Les informations et les dossiers nécessitent une solution ou un référentiel GCE où les documents et les fichiers sont classés ou indexés et consultables dans un format numérique. Les pratiques exemplaires et les processus de gestion des documents et de leur cycle de vie font partie intégrante de la gouvernance de l'information.

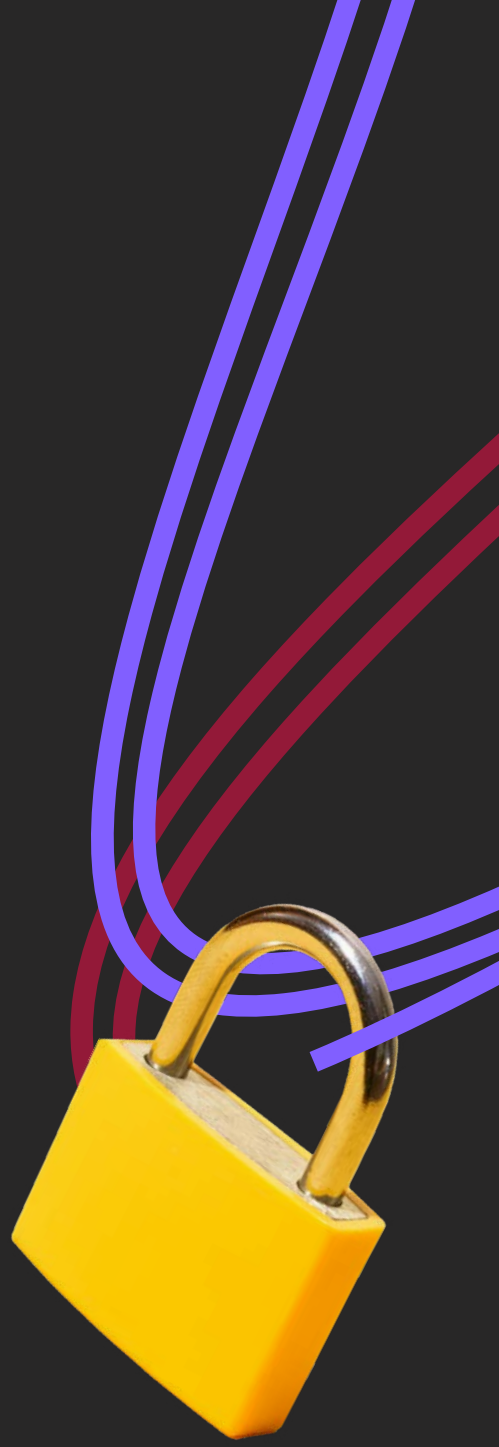
Voici comment un document typique suit son flux de travail et son cycle de vie :

1. Le document ou le support est numérisé ou scanné.

2. Le document est envoyé vers une solution PPI ou de capture, qui transforme les données non structurées, semi-structurées et structurées par classification, extraction, validation et exportation vers tout autre type d'application ou de flux de travail, tel qu'un GCE, ERP, CRM, ARP, iPaaS ou d'autres systèmes.

3. Le document numérique est ensuite géré dans le référentiel ou l'application, où ses informations peuvent être découvertes, suivies, analysées, gérées et, finalement, archivées, conservées ou éliminées en toute sécurité selon des règles commerciales ou des normes de conformité.

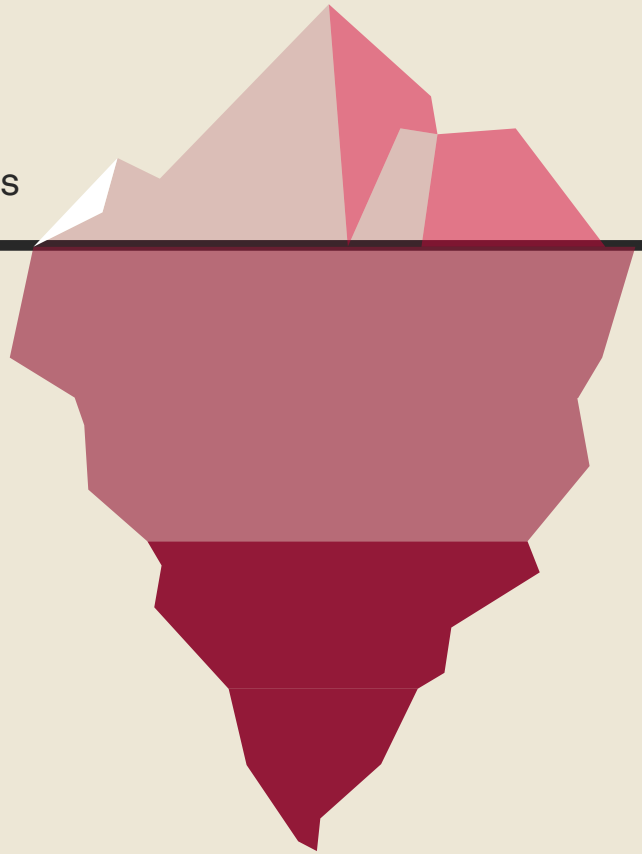
Environ 90 % des données d'entreprise sont non structurées (souvent des documents d'entreprise, des PDF et des fichiers multimédias), c'est-à-dire des informations qui ne sont pas structurées dans un format de base de données, ce qui les rend difficiles à rechercher, à gérer, à protéger et à utiliser.[10] La présence de données non structurées présente de nombreux risques, c'est pourquoi tout type de document ou d'image non structuré doit être converti et numérisé en informations structurées et géré de manière sécurisée dans toute l'organisation. La protection de vos données et la minimisation des risques ne sont pas seulement une responsabilité des TI; il doit s'agir d'un effort à l'échelle de l'entreprise.



[10] IDC. « IDC PlanScape : Dark Data Discovery », par Stanley B. Gibson et Amy Machado. 6 mai 2024.

2. Se concentrer sur la connaissance de l'emplacement de vos informations

10 %
Données structurées



90 %
Données non structurées, semi-structurées et ROT

Pour accroître la sécurité et optimiser les coûts de stockage, les services TI doivent connaître les informations de l'entreprise et savoir où elles se trouvent, quels risques elles présentent et si elles doivent être conservées.

Il est essentiel que les organisations comprennent la différence entre les informations (sensibles ou réglementées) et les documents, ainsi que les mesures de contrôle requises pour chacun d'entre eux, telles que : la sécurité, la confidentialité, la classification des découvertes, le stockage, l'accès, la récupération et l'élimination. Il est également important de mettre en place des pratiques permettant d'identifier les données ROT (redondantes, obsolètes ou inutiles) dont le stockage est coûteux et qui augmentent l'exposition de l'organisation aux cybermenaces.

On estime que les données ROT représentent au minimum 25 à 30 % des données d'entreprise, d'autres sources indiquant que ce pourcentage est souvent beaucoup plus élevé. Une fois qu'une organisation peut éliminer et réduire ses données ROT, elle peut réduire les coûts de stockage et investir dans la sécurité là où cela compte le plus.

La protection des données sensibles, telles que les informations personnelles identifiables (PII) et les informations relatives à l'industrie des cartes de paiement (PCI), est essentielle pour atténuer les risques potentiels. Ce type d'informations comprend généralement les noms, adresses, dates de naissance, numéros de sécurité sociale, mots de passe, numéros de carte de crédit, informations bancaires ou contrats. Par conséquent, la mise en place d'une infrastructure informatique et de gestion sécurisée permettra de maintenir la conformité des données structurées et non structurées. Cela nous amène à un examen plus approfondi des pratiques de sécurité de l'information.

1

Chiffrement

Le chiffrement des données doit être appliqué aux documents, fichiers, messages ou toute autre forme de communication sur un réseau. De plus, il est recommandé d'avoir un chiffrement de bout en bout pour tous les appareils, logiciels et solutions de stockage.

Bien que la sécurité des données et des informations doive être une priorité absolue pour l'ensemble du personnel, vous ne pouvez pas compter sur eux pour savoir quand ou comment les données doivent être chiffrées. Lors de l'élaboration de la politique de chiffrement de votre organisation, vous devrez d'abord obtenir une image précise de l'emplacement de toutes vos données, de la quantité de données confidentielles ou précieuses (une cible potentielle pour les cyberattaques ou les personnes mal intentionnées) et des risques qu'elles présentent pour votre organisation. Le nettoyage des données non structurées et la réalisation d'une évaluation de l'impact sur la protection des données vous permettront d'élaborer une stratégie complète de sécurité des données. Le chiffrement aidera à renforcer la sécurité globale de votre entreprise.

2

Protection et confinement des rançongiciels

La sécurité des rançongiciels comporte deux aspects essentiels : la prévention et l'atténuation. Les solutions préventives détectent les signatures et les comportements des rançongiciels, les empêchant ainsi de franchir le périmètre, tandis que le confinement des rançongiciels stoppe les épidémies de cryptage malveillant s'il parvient à passer outre les mesures de protection. Le logiciel se concentre sur le résultat des rançongiciels et du chiffrement illégitime rapide. Il arrête le chiffrement au niveau du fichier source ou racine, l'isolant et le contenant pour empêcher toute propagation ultérieure.

La protection contre les rançongiciels est une dernière ligne de défense essentielle pour l'infrastructure de sécurité d'une entreprise. Elle comble le dangereux fossé entre les appareils et les partages de fichiers, là où les entreprises manquent souvent de défenses essentielles. Disposer d'une solution de confinement garantit qu'en cas d'attaque, vous pouvez réagir suffisamment rapidement pour protéger la majorité de vos informations.

3

Authentification

L'authentification multifacteur (MFA) pour les applications et les appareils professionnels est essentielle pour les organisations, car elle ajoute une couche de sécurité essentielle au-delà des simples mots de passe, réduisant ainsi le risque d'accès non autorisé. En exigeant plusieurs formes de vérification (telles qu'un mot de passe, une application d'authentification mobile ou un facteur biométrique), l'AMF contribue de manière significative à la protection des données commerciales sensibles, des informations sur les clients et des actifs financiers.

La prévention de la mauvaise utilisation des ressources permet de réduire les coûts d'exploitation, de restreindre l'activité des utilisateurs pour renforcer la responsabilisation et de fournir des informations permettant de repérer les irrégularités grâce à des rapports. Un domaine souvent négligé est l'impression, au bureau et à distance. Par exemple, les règles d'impression peuvent inclure la définition de limites de pages par périphérique, la restriction de l'utilisation des couleurs, l'application du recto verso, la restriction de l'accès à certains paramètres, etc.

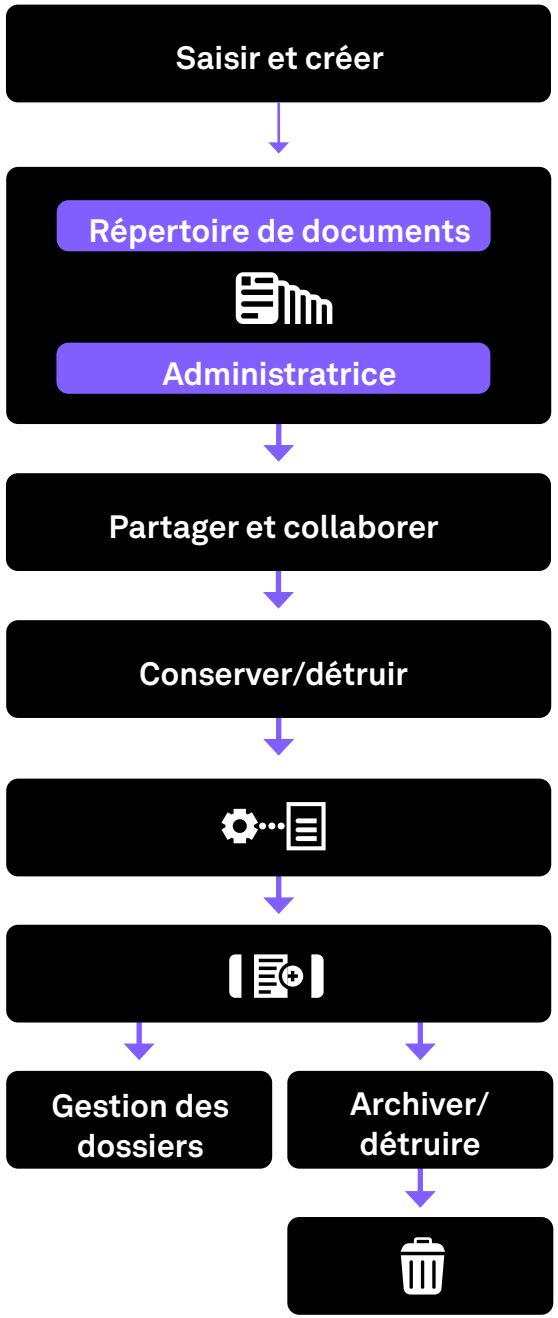
Si les utilisateurs doivent s'authentifier pour imprimer, les règles d'impression que vous avez définies sont automatiquement appliquées et l'activité est attribuée à l'utilisateur. Cela permet d'associer l'impression, la numérisation et la télécopie de documents à un client/sujet spécifique à des fins de facturation, ce qui permet d'obtenir des rapports d'activité détaillés sur un projet ou un sujet confidentiel.

3. Les processus automatisés font partie intégrante

De nombreuses tâches quotidiennes impliquent des processus métier, des flux de travail et des transactions, dont une grande partie peut être automatisée. Les processus courants dans lesquels des plateformes commerciales intelligentes, telles que les applications de saisie de données et de gestion des flux de travail, peuvent être appliquées sont les suivants :

- Traiter les factures
- Traitement des prêts
- Gestion des réclamations
- Intégration des ressources humaines
- Dossiers et formulaires du patient
- Relevés de notes et dossiers des étudiants
- Entretien et commandes clients

L'automatisation des processus offre une multitude d'avantages et peut ouvrir de nouvelles possibilités en matière de méthodes de travail. Cependant, les données numérisées doivent être protégées de manière ciblée, depuis leur point d'origine et tout au long de leur cycle de vie. Par exemple, la réduction des tâches répétitives (grâce à des outils d'automatisation tels que l'ARP et les flux de travail) contribuera à atténuer les risques, à obtenir des résultats plus rapidement et à accélérer les approbations.



40 %

Économies réalisées par les clients de Ricoh qui utilisent la gouvernance de l'information, tout en atteignant les objectifs de sécurité, de durabilité et de conformité.[11]

La création d'une stratégie et de règles de gouvernance de l'information concernant les processus d'affaires profitera à votre organisation de plusieurs façons :

- Éviter les pénalités et les amendes
- Bâtir la confiance des clients et des fournisseurs
- Maintenir la conformité et les vérifications
- Combattre les atteintes potentielles à la sécurité, les menaces et les attaques
- Meilleure gestion des coûts TI
- Accélérer les processus pour améliorer l'expérience client
- Aider les employés à éliminer les obstacles à la productivité pour devenir plus efficaces
- Intégration facile à d'autres applications
- Favoriser une culture axée sur les données avec une amélioration continue des processus opérationnels

[11] Ricoh Document Governance. https://www.ricoh.co.uk/business-services/all-services/application-services/document-governance/.

Que devez-vous faire ensuite?

Bien que la gouvernance, la gestion et la sécurité de l'information soient des sujets complexes, il est essentiel de comprendre de quelles informations, documents et données vous disposez, et comment elles sont utilisées et gérées tout au long de leur cycle de vie. Une fois que vous aurez fait cela, vous serez mieux à même d'atténuer les risques et de relever les défis de conformité.

Des solutions modernes et automatisées, associées au GCE, de la capture et des flux de travail aux appareils, en passant par la sécurité et la gestion globale, peuvent non seulement être un avantage concurrentiel, mais aussi servir à protéger toute entreprise. Les recherches des analystes suggèrent que si tous les renseignements, documents et applications étaient intégrés et centralisés, les trois principaux avantages seraient la conformité, la connaissance des clients et la sécurité du contenu.[12]

La direction devra faire comprendre l'importance de la gouvernance de l'information et des protocoles de sécurité en faisant en sorte que l'ensemble de l'entreprise respecte ses directives. Ce n'est pas seulement l'équipe des TI qui devrait être à la table, mais l'organisation collective. La promotion d'une culture axée sur les données doit être une priorité. Cela implique souvent d'adopter une mentalité « Zero Trust », qui nécessite une approche de la sécurité à plusieurs niveaux, comprenant des cadres d'authentification, de chiffrement et de cybersécurité. De même, créer une stratégie qui permette la libre circulation de l'information vers ceux qui en ont besoin, tout en la protégeant.

[12] IDC.« State of Content Services Survey. ». June 2023.

7 étapes pour relancer votre programme de gouvernance de l'information

Ces étapes vous aideront à construire, promouvoir et entretenir une culture de la gouvernance de l'information à mesure que vous progressez dans votre continuum de maturité numérique.

1. Identifiez vos informations personnelles identifiables (PII), les informations relatives à l'industrie des cartes de paiement (PCI) et les informations relatives à la propriété intellectuelle (PI).

2. Comprendre et se conformer au RGPD, à la HIPAA, à la SEC, à la LPRPDE/DCIA/CCPA et à d'autres règlements.

3. Identifier et corriger le ROT.

4. Isoler les renseignements qui ne sont pas requis au-delà de l'objectif de leur collecte, comme les numéros de carte de crédit ou une pièce d'identité spécifique.

5. Archiver ce qui a une valeur commerciale ou culturelle.

6. Surveiller régulièrement les magasins de données.

   Réviser continuellement les politiques de l'entreprise en matière de dossiers et de sécurité.

Atténuer les risques grâce à la gouvernance de l'information

La gouvernance et la sécurité de l'information sont ancrées dans nos valeurs, un engagement que nous ne prenons pas à la légère. Que vous soyez submergé de données, que vous travailliez dans un secteur hautement réglementé, que vous manquiez de ressources ou d'expérience, ou que vous souhaitiez avoir l'assurance d'utiliser des services, des logiciels et des appareils hautement sécurisés, nous visons à gagner votre confiance en appliquant les normes de sécurité les plus strictes du secteur.

Notre vaste expérience en matière de conseil et d'application d'une approche multicouche peut être mise à profit dans toute votre organisation, qu'il s'agisse de stratégie, de dispositifs, de logiciels, de services, d'assistance, de formation, etc. Laissez-nous vous aider dans votre évolution vers de meilleurs services d'information numérique.

Vous souhaitez en apprendre davantage? Visitez ricoh.ca ou communiquez avec un expert en gestion de contenu d'entreprise, en gouvernance de l'information ou en sécurité de Ricoh dès aujourd'hui.

Ricoh, un partenaire de confiance

Aujourd'hui, pour plus de 1,4 million de clients dans le monde, Ricoh libère le pouvoir de l'information pour créer de meilleures expériences de travail, rationaliser et connecter les flux de travail grâce à l'automatisation des processus, et stimuler l'efficacité opérationnelle. Travaillons ensemble pour découvrir comment nous pouvons mettre l'information à votre service.

RICOH
imagine. change.

Ricoh Canada Inc. 400-5560 Explorer Drive, Mississauga, ON L4W 5M3, 1-888-742-6417