O GUIA DO CIO PARA REPENSAR A CONFORMIDADE

COMO TRANSFORMAR SUA ORGANIZAÇÃO DE TI COM MELHOR CONTROLE DE PROCESSOS EM 2020

ManageEngine

Um guia CIO para repensar a

Capítulo 01

Capítulo 02

Capítulo 03

1 VAMOS ENTRAR EM SINTONIA

Este livro é para você?

Considere as perguntas abaixo:

- Você é um líder de TI que deseja simplificar seus processos e garantir que eles sejam mais confiáveis?
- Se lhe fosse oferecida uma estrutura para tornar os processos da sua empresa mais eficientes e eficazes, você aceitaria?
- Você está interessado em saber se realmente deve se preocupar com o cumprimento da lei internacional?

Se você respondeu "sim" a uma ou mais perguntas acima, este e-book é para você.

Como este e-book transformará seus processos para sempre

Este e-book é uma visão geral abrangente e transparente da abordagem de conformidade da Zoho. O conteúdo deste e-book é o resultado de entrevistas com nossos líderes de conformidade.

Neste e-book, compartilhamos tudo o que aprendemos por tentativa e erro durante nossa jornada rumo à conformidade para que você possa assimilar métodos viáveis e soluções práticas para resolver os problemas baseados em processos da sua organização. Isso nos serviu de estratégias quando começamos nossos esforços de conformidade.

Compartilhamos nosso conhecimento acumulado com você agora para que não precise passar por todas as dificuldades pelas quais passamos. Esperamos que, quando terminar de ler, você consiga criar sua própria estrutura que tornará a conformidade uma jornada eficiente, mais fácil e mais agradável para sua organização.

Em conformidade com o quê?

Chamamos isso de "organização" porque algumas pessoas trabalham juntas de forma coerente para fornecer valor aos clientes. Essa criação de valor seria possível se as pessoas não aderissem a nenhuma regra?

- Quem toma decisões na empresa e quem as segue?
- Em que base a organização lança novos produtos ou serviços ou desiste dos antigos?
- Quais são as várias funções que um funcionário pode ter?
- Como os funcionários devem utilizar os recursos da empresa?

A resposta a cada pergunta acima torna-se uma regra e cada funcionário de uma organização a segue. Em outras palavras, você está em conformidade com as regras definidas por sua organização. Mas se tão somente essa conformidade fosse o necessário para sobreviver e prosperar no mundo corporativo, você não estaria lendo este e-book.

As regras estabelecidas pelos governos e pelas organizações internacionalmente reconhecidas são uma extensão, e uma melhor definição, das questões mais simples acima formuladas. Esse é o tipo de conformidade sobre a qual falaremos: conformidade com o direito internacional.

À medida que você avança neste e-book, verá como você pode levar sua conformidade atual a um padrão globalmente aceito.

Ei! Eu sou Con-FORMI! Experimente o seguinte...

Liste todos os países em que você faz negócios. Onde está a maioria dos seus clientes? Quais são as regras desse país?

Por que a conformidade é tão urgente hoje em dia?

Há muito tempo temos leis que exigem conformidade. Mas o Regulamento Geral sobre a Proteção de Dados (GDPR) afetou o mundo corporativo de forma inédita devido a suas multas, sua ênfase nos direitos dos titulares dos dados e a forma como ele expandiu o escopo dos dados pessoais (os direitos exercidos por cada um dos indivíduos sob a jurisdição do GDPR), o que significa que as empresas tiveram de analisar os seus processos de forma mais profunda e abrangente.

Quando uma regulamentação estabelece um padrão tão alto para controles de processo, como as empresas podem imaginar voltar ao modo como as coisas eram? O impacto do GDPR foi primeiramente temido, depois respeitado e finalmente aceito pelo mundo corporativo. E as empresas agora percebem o valor da conformidade e a diferença que ela pode fazer na satisfação de seus clientes.

Por enquanto, você pode estar satisfeito com a certificação de seus auditores internos, mas em breve haverá um momento em que todos os desenvolvedores, profissionais de RH e até mesmo guardas de segurança devem ter um certificado de conformidade autorizado para realizar suas tarefas.

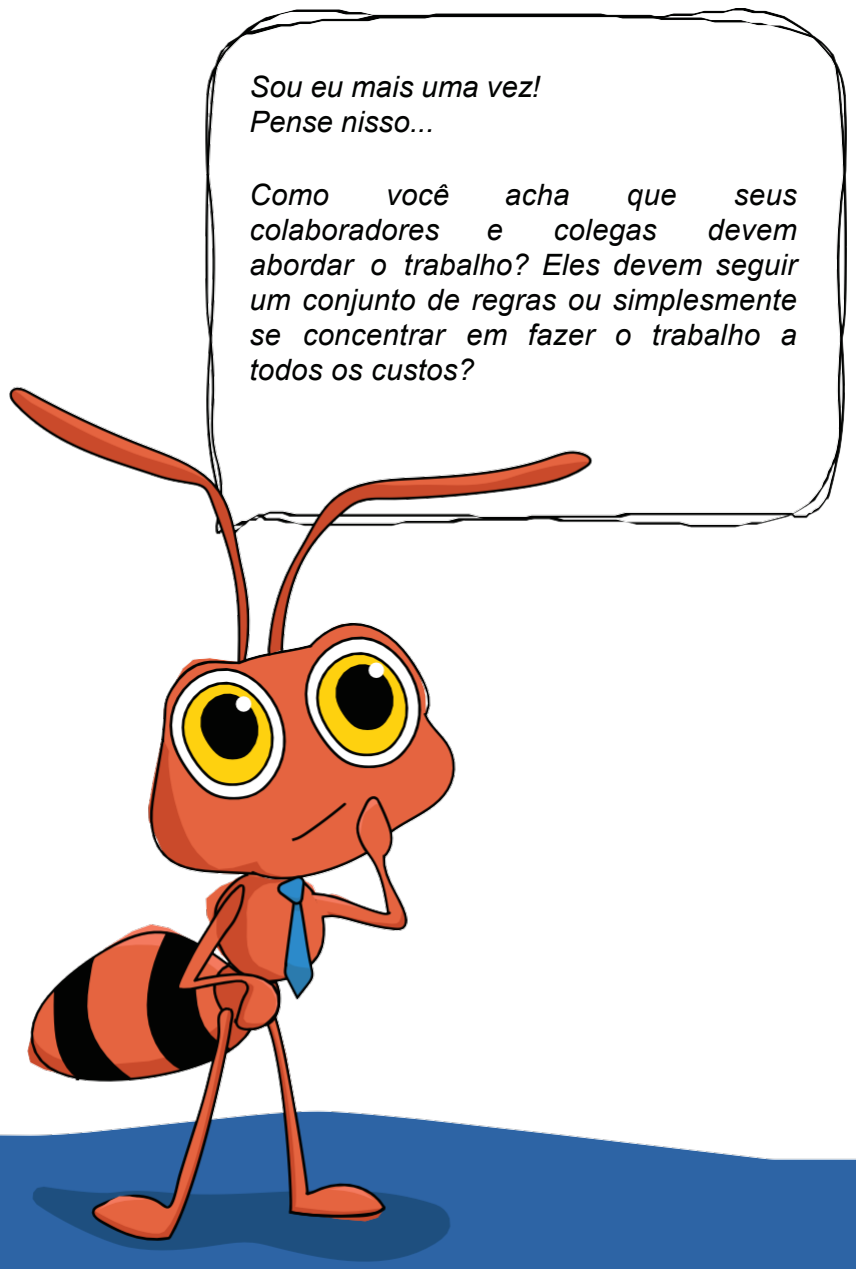
Por enquanto, seus clientes atuais e potenciais podem estar interessados em sua conformidade com um padrão específico; mas em breve haverá um momento em que cada organização deve demonstrar conformidade antes mesmo de iniciar o faturamento de seus clientes.

Se você estava planejando tornar a conformidade um grande impulsionador nos processos da sua empresa, não há momento melhor do que agora.

HISTÓRIA DA ZOHO

A Zoho é um exemplo clássico de uma empresa que adota a cultura de startup. Temos mais de 90 produtos e quase 100 times para gerenciá-los. No entanto, cada time trabalha como uma empresa individual com a máxima liberdade, encorajamento de ideias inovadoras e uma cultura que está enraizada na independência e individualidade de cada funcionário. Conseguir que todas esses times estejam em consonância não é apenas uma revolução processual, mas também cultural. O entendimento de que a conformidade não é um obstáculo à liberdade, mas um aspecto crucial de usar essa liberdade da melhor maneira possível tem sido fundamental para nós. Se milhares de pessoas divididas em centenas de times que foram expostas a regras mínimas até o momento puderem concordar que a conformidade é mais um facilitador do que um impedimento, qualquer empresa pode cumprir suas metas de conformidade.

2 CONFORMIDADE E AS REGRAS



Conformidade: Liberação por meio de regras

Vamos considerar o caso da Zylker Corporation, um provedor de software que começou há alguns anos. A Zylker, apesar de ser uma startup, chamou a atenção de muitos devido à sua expansão de cinco funcionários para 500 em poucos anos. Sua receita multiplicou-se, e as pessoas agora a procuram como um símbolo de crescimento e cultura dinâmica de trabalho.

Um dos principais motivos pelos quais startups como a Zylker são inovadoras é a cultura de liberdade e flexibilidade que elas têm. Esses traços os ajudam a sobreviver no mercado porque são capazes de se adaptar às alterações de forma eficaz e eficiente. Essa cultura obviamente tem funcionado, pois um número crescente de empresas semelhantes à Zylker vem crescendo nos últimos anos.

Quando a cultura flexível da Zylker se encontra com a obrigação de conformidade, ela enfrenta, e não é surpresa, alguma resistência. Sua cultura de liberdade, na qual os funcionários podem fazer as coisas à sua maneira, de repente precisa introduzir regras como:

- Sempre que quiser contratar um novo funcionário, faça uma verificação completa do histórico.
- Sempre que quiser acessar seu próprio data center, siga um rigoroso processo de verificação de identidade.
- Sempre que quiser trabalhar com um novo fornecedor, faça uma abrangente avaliação de riscos.
- Sempre que você quiser que um cliente faça login em sua aplicação usando um novo dispositivo, certifique-se de que ele use a autenticação de vários fatores.
- Sempre que você quiser adicionar um campo que possa conter informações confidenciais a um formulário, use criptografia.

Um funcionário típico pode ver cada regra como as acima como um obstáculo ou mesmo um sinal de opressão. Se você fosse um membro da alta administração da Zylker, talvez até acredite que essas regras irão cercear a liberdade de seus funcionários e atrasar seu progresso.

Mas o cumprimento é, na verdade, uma forma de libertação através de regras.

- Se fizer uma verificação de antecedentes, nunca terá de se preocupar com a integridade de um recurso crucial.
- Se você fizer do controle de acesso rígido um hábito, não precisará vasculhar sua própria organização em busca de uma violação de dados.
- Se você tiver um procedimento rigoroso de integração de fornecedores, poderá dizer aos seus clientes com confiança que os dados deles estão seguros, mesmo quando não estão com você.
- Se você tornar a autenticação de vários fatores uma configuração padrão, poderá lidar com impostores com mais eficiência.
- Se você usar criptografia, seus clientes vão se sentir muito mais seguros, mesmo quando seus sistemas forem violados.

A liberação que a conformidade traz ajuda você a avançar nos negócios com confiança e autoridade. Aceitar isso é a chave para deixar a conformidade enraizada em sua organização.

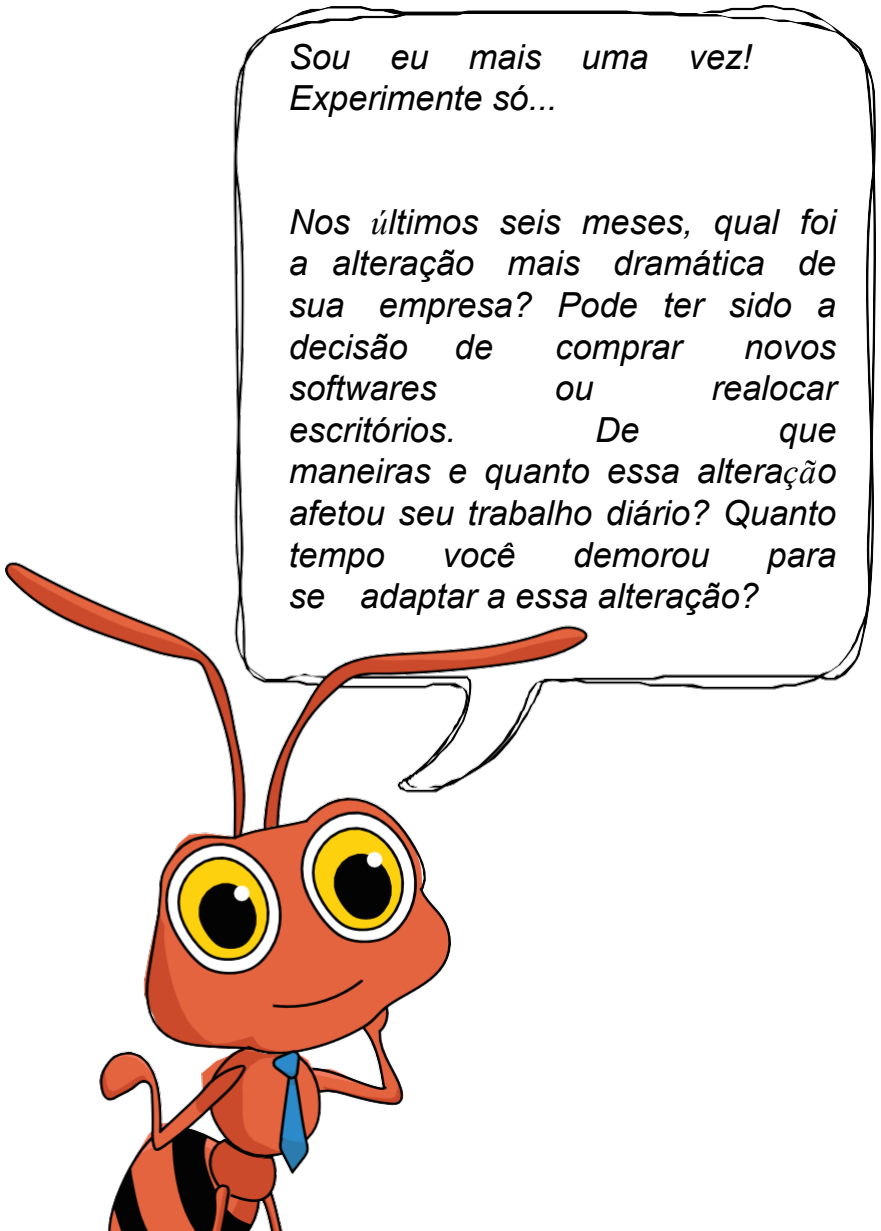
A conformidade e a necessidade de controle de processos

Fundamentalmente, a conformidade é apenas um conjunto de regras. Mas ela se resume a isso? Para nós, a conformidade é muito mais do que isso. Ela também é:

- Uma afirmação, uma garantia de que seu processo está funcionando da maneira que deveria e está alcançando seus objetivos.
- Um freio muito necessário para sua empresa. Imagine o que aconteceria se a sua organização não tivesse nenhum tipo de freio. Você teria que manter um ritmo mais lento para evitar obstáculos ou colocar os que estão ao seu redor em risco.
- Uma verificação de realidade permanente para lembrá-lo de que seus processos devem sempre ser trabalhados.
- Acima de tudo, um bilhete de entrada: Algo que seus clientes usam para permitir que você faça parte de seus negócios.

Mais do que uma regra, a conformidade é uma plataforma que literalmente eleva seus padrões. Seus esforços com relação à conformidade melhorarão seu controle de processo. Quando tudo corre de acordo com o planejado, o processo parece estar no controle. Mas, na realidade, as coisas podem sair do controle. Ao cumprir essas regras, você aumenta suas chances de colocar o processo de volta no controle da forma mais suave e rápida possível.

Quando você estiver em conformidade, poderá impulsionar seus negócios com confiança e sua conformidade responderá à maioria das perguntas feitas a você.



É necessário mudar drasticamente?

Quando você introduz essas regras, você é obrigado a pensar que há uma grande mudança chegando. Mas a mudança está apenas na forma como as coisas são feitas, e não no que é feito. As regras da seção anterior são pequenas modificações e melhorias nos processos que sua empresa já possui.

Há uma boa chance de que você já tenha o que a maioria do exigido por lei.

As mudanças necessárias para que as organizações se tornem compatíveis estão longe de serem drásticas, mas exigem um nível mais alto de entendimento e uma nova abordagem aos processos.

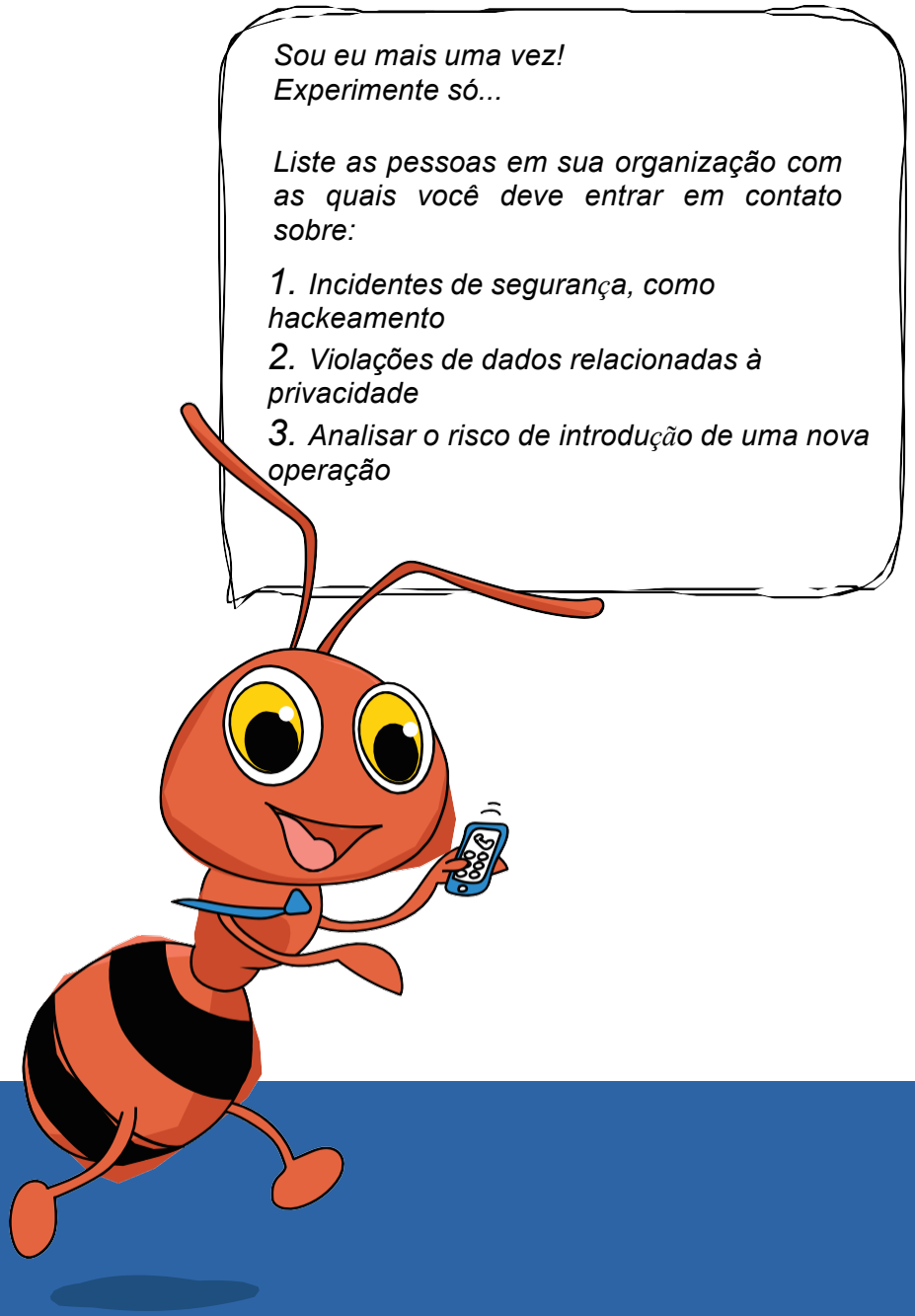
HISTÓRIA DA ZOHO

A Zoho fez mudanças rápidas e drásticas em seus processos? A resposta é um grande “não”. Assim como qualquer organização bem-sucedida, já tínhamos nossos controles de processo, aqueles necessários para administrar a empresa de forma tranquila e eficiente. Graças às certificações ISO, temos uma noção dos padrões internacionais. No entanto, ainda tivemos que adaptar nosso trabalho a uma nova onda de conformidade com o crescente número de leis e padrões internacionais.

Como nos adaptamos? Percebemos o valor do que já tínhamos. Depois de obter uma compreensão completa dos controles exigidos pelo GDPR e outras leis com as quais precisávamos estar em conformidade, construímos esses controles sobre os que já tínhamos. O resultado? As mudanças que precisávamos fazer eram suaves, simples e graduais.

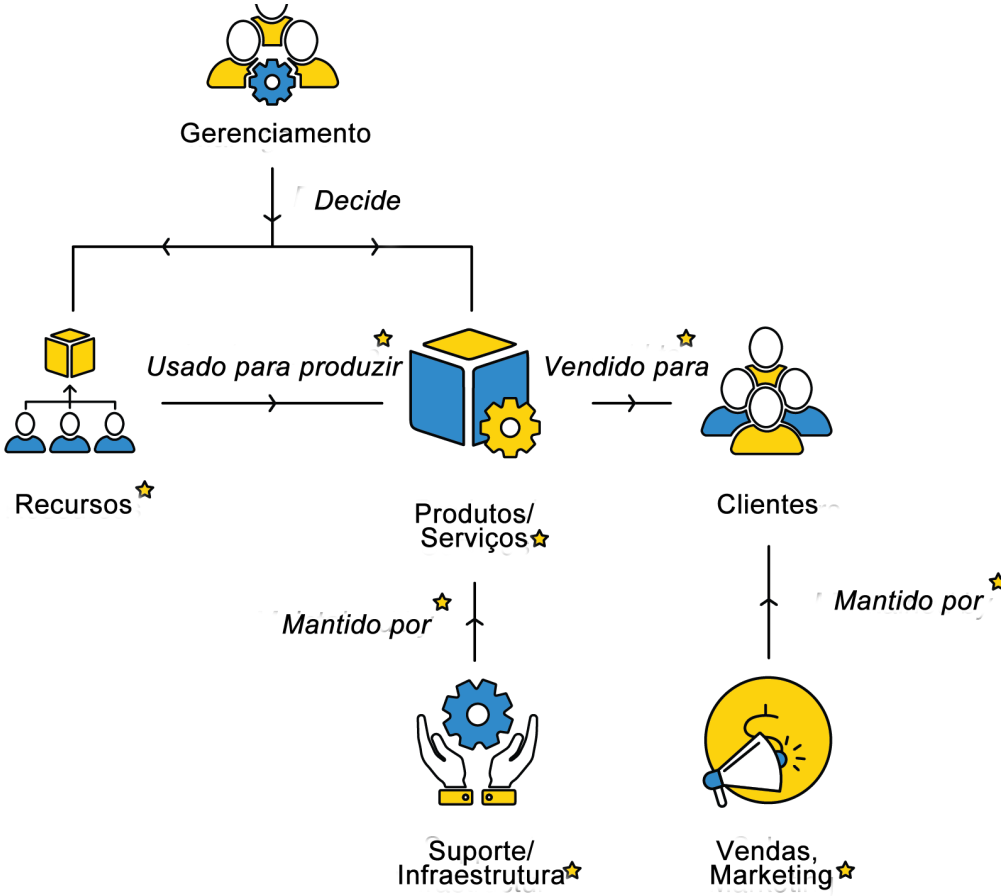
A conformidade não exige que você refaça tudo e cause estragos. Ela simplesmente pede que você revise seus processos, adicione controles e fortaleça esses controles para elevar sua organização aos padrões internacionais. E foi exatamente isso que fizemos.

3 CONSIDERAÇÕES DOS AGENTES INTERMEDIÁRIOS



Os condutores

O que você precisa para gerar uma onda que alcance cada canto de um sistema? Um epicentro. Nesse caso, você deseja garantir que todos os departamentos, funcionários e funções de sua empresa estejam em conformidade. O epicentro da conformidade é um time central.



Este diagrama ilustra exatamente o que é necessário para criar um produto, e você pode desenhá-lo para cada um dos produtos da sua empresa. Veja o que você deve observar:

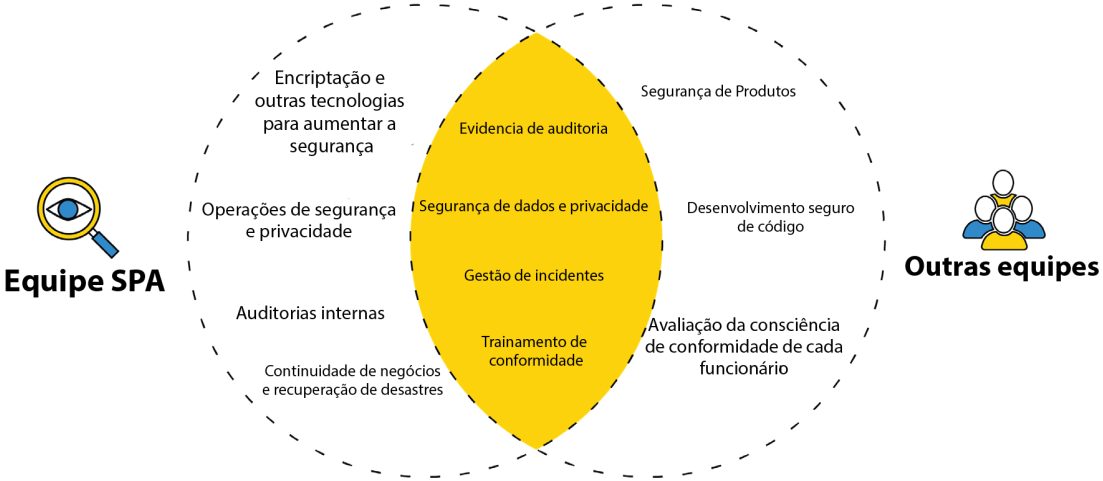
- Cada caixa envolverá um conjunto de times. A conformidade geral só pode ser obtida quando cada uma desses times garantir que suas atividades estejam em conformidade.
- As estrelas no diagrama acima indicam o time de segurança, privacidade e auditoria (SPA), que é o time motivador da conformidade:
  - São partes interessadas em todos os processos.
  - Garantem que cada time esteja ciente de suas responsabilidades de conformidade e esteja realizando as atividades necessárias para a conformidade.
  - Facilitam e organizam auditorias externas.
  - Gerenciam qualquer desvio dos padrões nos processos.

O time SPA e as responsabilidades compartilhadas

E como o próprio nome diz, o time SPA facilita a experiência de conformidade de uma organização. Mas não pode fazê-lo sozinho. Cada time deve fazer sua parte para a conformidade.

A segurança é uma responsabilidade compartilhada.

Para cada função de segurança, privacidade e auditoria dentro de uma organização, há responsabilidades que o time SPA deve conduzir e aquelas que os outros times apontados na Ilustração 1 devem realizar. A Zylker, nossa empresa de exemplo de antes, tem um time SPA que possui três divisões, mas todas elas trabalham juntas. Veja como seria o modelo de responsabilidade compartilhada da Zylker:



Nota: Há mais atividades para conformidade além das mencionadas acima e, como a responsabilidade é compartilhada, varia de acordo com a organização. No entanto, deve-se observar que a criação desse modelo e a comunicação das responsabilidades compartilhadas com a alta gerência e os times individuais são essenciais.

Em que o time SPA deve se concentrar?

A conformidade é uma responsabilidade compartilhada entre cada membro da organização, mas precisa ser orientada e gerenciada por um time central. As três divisões do time SPA são como guerreiros que defendem um castelo do mesmo inimigo, mas em frentes diferentes. Considere este cenário:

A Zylker quer obter a certificação ISO 27001, e eles se deparam com o seguinte controle:

"Os contratos sobre transferência de informações devem abordar a transferência segura de informações comerciais entre a organização e terceiros"

Esse controle fala sobre a segurança da transferência de informações quando a Zylker compartilha dados com terceiros e como o compartilhamento de dados deve estar previsto no contrato celebrado entre as duas organizações. O time SPA da Zylker trabalhará para esse controle, mas cada divisão terá suas próprias perguntas.

A segurança está a falar sobre o acordo

- As informações estão seguras em nossa empresa? Elas estão criptografadas?
- Os terceiros têm tecnologia e procedimentos suficientes para manter as informações seguras?
- Por meio de qual mídia as informações serão transferidas?
- Se forem transferidas on-line, a comunicação será criptografada em trânsito?
- Se as informações estiverem em um lugar comum (como a nuvem) e fornecermos o acesso a terceiros, temos controle de acesso suficiente para garantir que eles não as usem indevidamente?
- Se as informações forem comprometidas por um hacker de alguma forma, como respondemos imediata e efetivamente?

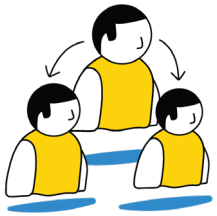
As considerações da privacidade sobre o contrato

- Qual é a categoria das informações em questão? Trata-se de dados pessoais?
- Quem, da organização terceirizada, consegue ver essas informações? Isso é realmente necessário?
- Se as informações estiverem relacionadas a pessoas que não têm ligação com a organização terceirizada, essas pessoas devem ser informadas sobre o tratamento de dados primeiro?
- Podemos obter informações sempre que possível para minimizar o risco de violação de dados pessoais?
- Qual é o objetivo deste subsídio? Temos sido transparentes sobre essa finalidade?
- Para que o terceiro usará os dados? Temos controles para garantir que eles não façam uso indevido dessas informações?
- O terceiro armazenará essas informações? Isso é realmente necessário? Em caso afirmativo, quanto tempo eles vão armazenar?
- O terceiro compartilhará essas informações com mais alguém? Se isso acontecer, como eles garantirão que as informações permaneçam privadas?

Considerações da auditoria sobre o contrato

- Qual é a política da Zylker sobre a transferência de informações? As transferências estão de acordo com essa política?
- Quem na Zylker é responsável por essa transferência?
- Que procedimento eles seguem? Como eles garantem que estão seguindo o procedimento?
- Como medimos a eficácia da transferência?
- Temos evidências suficientes de que essa transferência é segura de acordo com o controle ISO?

Embora as divisões do time SPA lidem com perguntas diferentes, elas assumem funções semelhantes:



Facilitadores: Como seus membros têm um conhecimento significativo de conformidade, o time SPA é competente para ajudar qualquer processo a ficar em conformidade. Um padrão como o ISO 27001 ou um regulamento como o GDPR são quase determinantes sobre a melhor forma de funcionamento de uma empresa. O time SPA pode aplicar esse conhecimento a cada processo para que ele aconteça da melhor maneira possível e também esteja em conformidade.

Críticos: Os padrões são ideais, e os membros do time SPA são obrigados a ser idealistas quando se trata de processos, o que também os torna os maiores críticos da empresa. Eles examinam cada processo e orientam os indivíduos e os times responsáveis para melhorá-lo até que o processo esteja o mais próximo possível de seu estado ideal.

Consultores: O time SPA tem especialistas cujas opiniões devem ser procuradas quando da implementação de qualquer novo processo. Pode ser uma alteração de local, migração para um novo provedor de serviços, introdução de um novo recurso em uma oferta ou descontinuação de um produto. Em todos esses casos, os especialistas em SPA devem ser consultados para que você conheça as implicações, os riscos e os controles necessários.

HISTÓRIA DA ZOHO

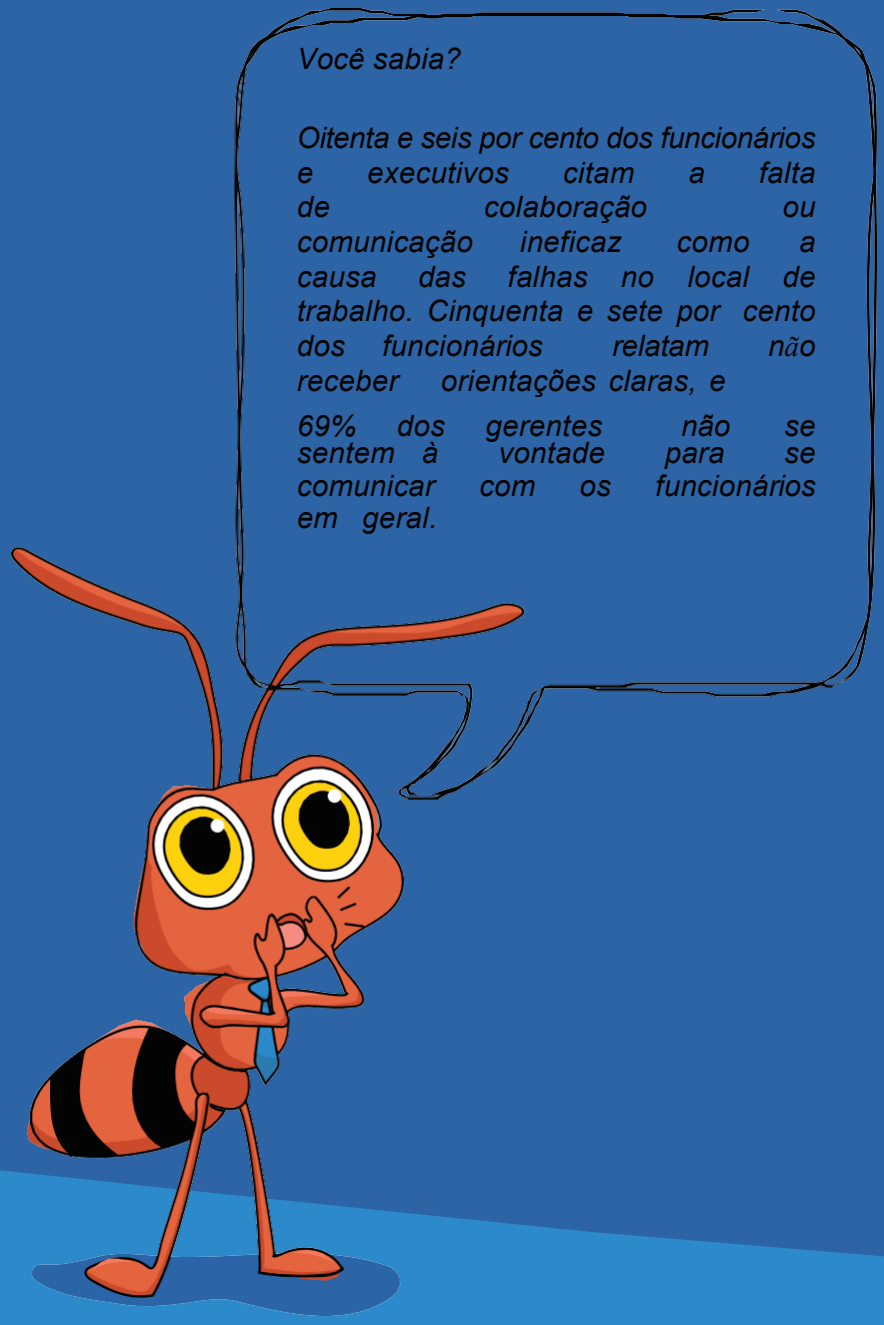
O time SPA da Zoho facilita todos os tipos de processos problemáticos. Um time de segurança com mais de 30 profissionais cria tecnologia interna para verificação de código, gerenciamento de vulnerabilidades, educação, estruturas e auditorias. O time de privacidade tem analistas que se coordenam com todos os times de produtos e operações para garantir que a privacidade seja combinada com nossos processos e produtos. O time de auditoria possui auditores internos certificados que mantêm guias sobre os processos.

Todos esses times trabalham juntos quando uma auditoria, um incidente ou uma nova regulamentação surgir. O motivo é simples: a menos que colaborem, a conformidade não é completa. Os requisitos de segurança de um padrão desempenham um papel crucial nos requisitos de privacidade e auditoria. Da mesma forma, as implicações de privacidade afetam a forma como os controles de segurança e os requisitos de auditoria são tratados. As três divisões são inter-relacionadas, mas diferentes. Para configurar uma infraestrutura que esteja continuamente em conformidade, o time SPA deve ser um grupo grande, mas com clara divisão de responsabilidades e propriedade entre os times de segurança, privacidade e auditoria.

Agora estamos avançando para um sistema em que estabelecemos expertise em conformidade em cada time. Esses especialistas realizam atividades típicas de necessárias para seu time. O time SPA agora precisa se coordenar somente com esses especialistas quando necessário. O foco principal do time SPA agora será a melhoria contínua dos processos e o aprimoramento do perfil de conformidade da Zoho.

4 SERVINDO A CONFORMIDADE

EM UMA BANDEJA



A educação prevalece sobre a força

A criação do time SPA e a definição das responsabilidades compartilhadas são apenas o começo. Se a conformidade for fazer parte da cultura da sua empresa, você deve perceber que:

- *A conformidade deve ser ágil. Ela deve evoluir com a sua empresa; configurar a estrutura é apenas o começo.*
- *A conformidade deve ter raízes profundas. Cada funcionário deve adotá-la e torná-la uma parte contínua de seu trabalho.*

É por isso que forçar a conformidade não funcionará a longo prazo. Em algum momento, você pode ter que sacrificar a conformidade para atender às suas metas da empresa, apenas para que essa decisão afete você posteriormente.

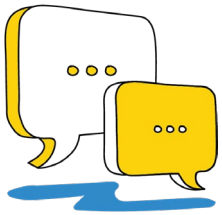
Ficar em conformidade exige que você apresente algumas regras. Educar seus funcionários sobre o motivo de essas regras fazerem sentido é muito mais importante do que simplesmente tentar aplicá-las.

Marketing sutil

Marketing significa informar as pessoas de que você pode resolver seus problemas. Você deve ir ao lugar onde as pessoas que você está interessado em alcançar estão falando e falar mais eloquentemente do que elas para que escutem. E melhor não significa necessariamente mais alto.

Vender uma ideia como a conformidade para quem não gosta de regras não é uma tarefa fácil. É por isso que você deve lidar cuidadosamente com os três principais componentes do marketing sutil interno:

Profissionais de marketing



Meios

Materiais

Profissionais de marketing são os membros cruciais da hierarquia organizacional que têm voz. Cada gerente é um profissional de marketing nesse sentido, assim como qualquer um a quem as pessoas deem ouvidos. A alta gerência deve agir como os primeiros profissionais de marketing, e o time SPA deve continuar o bom trabalho.

Você deve identificar esses participantes cruciais em sua organização e garantir que eles entendam por que devem adotar a conformidade e como podem fazer isso. O time SPA tem competência para agregar jogadores cruciais. Em seguida, esses jogadores devem assumir o controle para garantir que todas as pessoas com quem conversam falem sobre conformidade.

Os **meios** são a arena onde as conversas em grupo acontecem. Pode ser um grupo de bate-papo, pseudônimos de e-mail, mídia social interna, um espaço de gerenciamento de projetos e qualquer outro espaço colaborativo. Você deve identificar cada um desses meios e pedir aos seus profissionais de marketing para usá-los todos.

Materiais são o que transmitem a mensagem. Pode ser um e-mail simples, uma apresentação, um e-book, a ATA de uma reunião ou um vídeo de alta qualidade. Tudo se resume ao que seu time SPA pode gerenciar e ao que funciona melhor para seu público (colaboradores).

Estes três aspectos do marketing devem funcionar em uníssono:

- Um time de produtos tem um grupo de bate-papo (meio) que discute os novos recursos que estão sendo planejados. O gerente de produto (profissional de marketing) pode compartilhar diretrizes de segurança (material) para criar um novo recurso preparado pelo time SPA.
- Um time de suporte tem um fórum (meio) para discutir questões desafiadoras que enfrentam. O chefe de suporte (profissional de marketing) pode compartilhar uma apresentação ou um e-book (material) que discute as diretrizes de privacidade ao mesmo tempo em que soluciona problemas críticos.
- O time jurídico quer fazer uma apresentação (meio) aos times de operações sobre os desafios processuais envolvidos na mudança para um novo prédio. O apresentador (profissional de marketing) pode incluir capturas de tela (material) dos controles de gerenciamento de mudanças mencionados no ISO 27001 na apresentação.

Depois de ter utilizado todos os M's de marketing de forma eficaz e eficiente durante um longo período, a ideia de conformidade irá se tornar uma segunda natureza para sua força de trabalho.

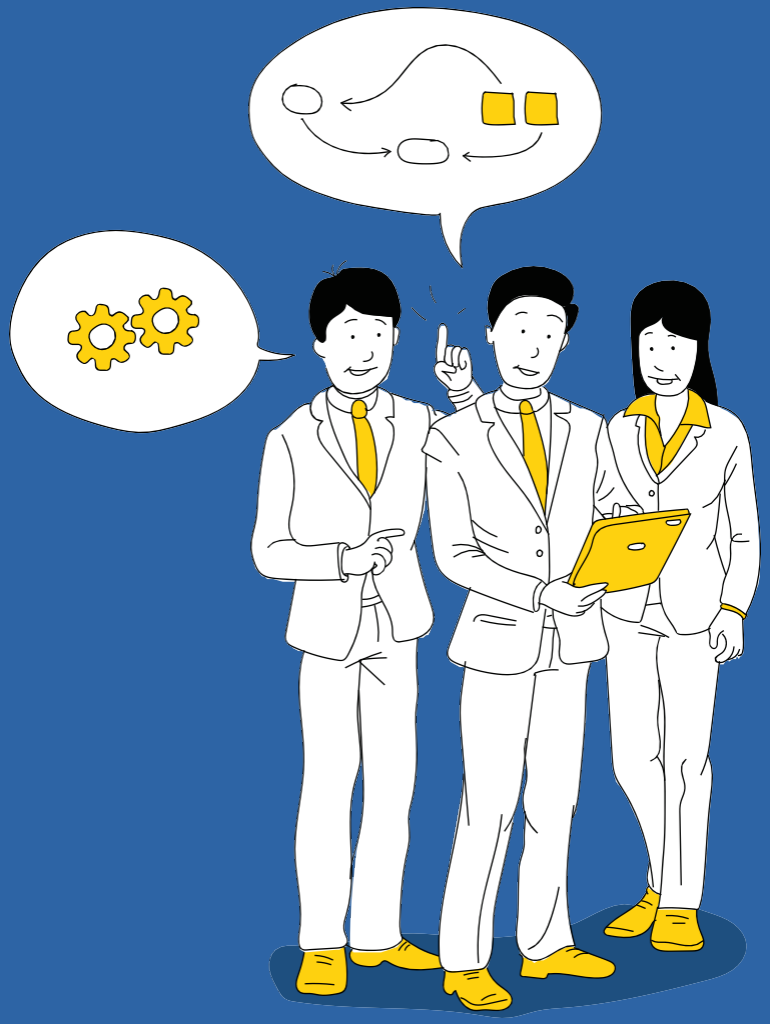
GDPR-IZANDO A ZOHO

O time SPA da Zoho enfrentou seu maior desafio com o GDPR. Embora houvesse bastante falatório sobre o GDPR, nenhuma organização poderia estar 100% pronta para essa mudança de paradigma. O time SPA da Zoho assumiu esse desafio e iniciou uma pesquisa para ter uma compreensão completa dos requisitos do GDPR e como a regulamentação mudaria a maneira de trabalhar da empresa. Uma vez que esse processo começou, os três M's de marketing tiveram que entrar em jogo.

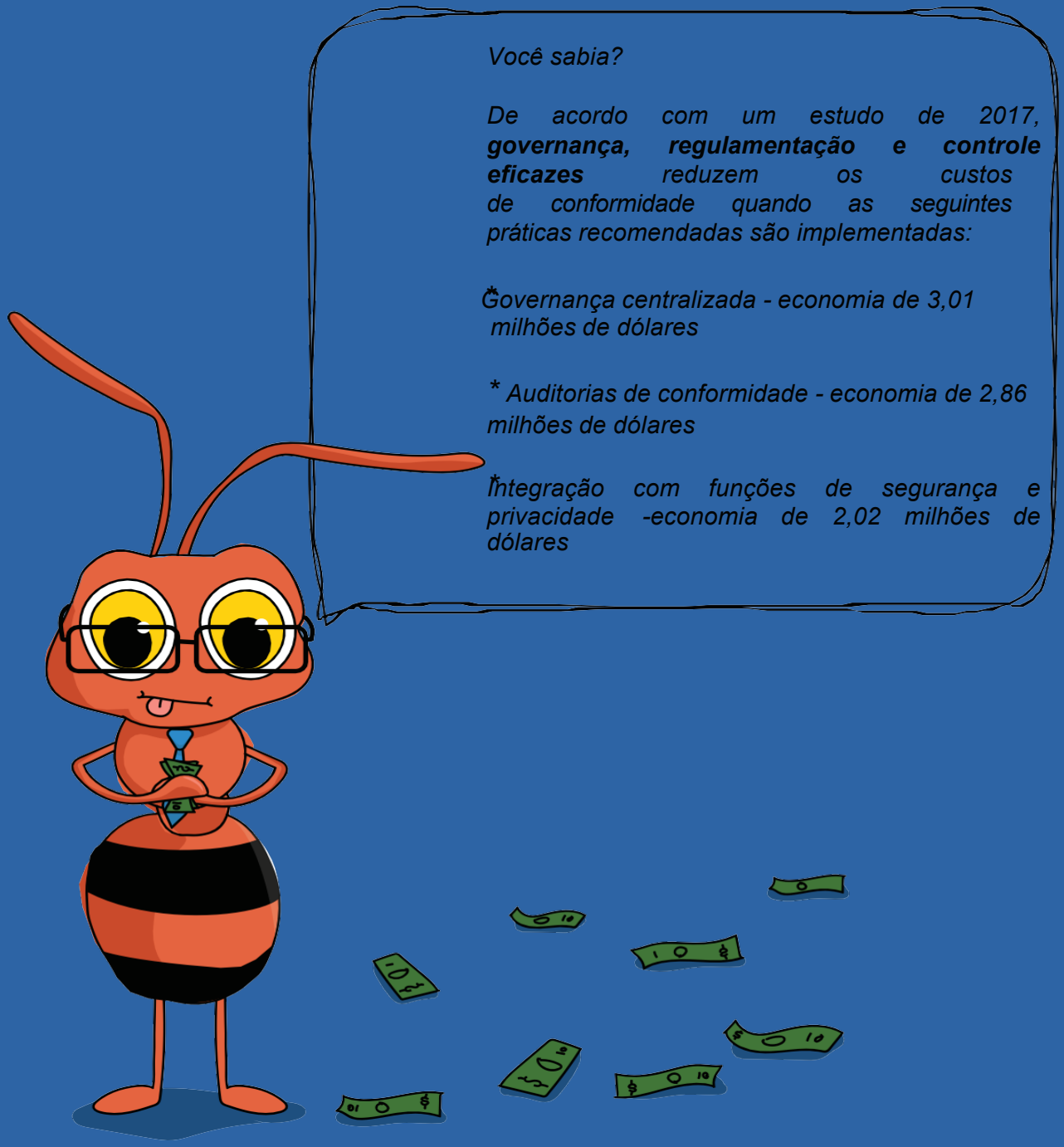
A Zoho tem uma estrutura horizontal em que cada time de produto tem seu próprio método de trabalho. O time SPA primeiro visou todos os canais de comunicação interna que envolviam o time em posições de liderança; eles eram nosso primeiro grupo de profissionais de marketing. Para ensinar a esses profissionais de marketing qual era a conformidade e como lidar com ela, o time SPA chegou até eles através dos nossos meios favoritos:

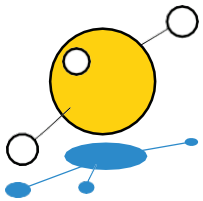
1. Apresentações: Estas foram feitas em grande escala, às vezes três vezes por semana, e direcionadas a diferentes gerentes de produtos.
2. Campanhas: Isso incluiu uma campanha de conscientização e uma campanha para lançar iniciativas de documentação.
3. Mídia social: Nosso portal de mídia social interno baseado no Zoho Connect foi nossa maneira de alcançar cada funcionário. Nós criamos conscientização com publicações envolventes, pesquisas, breves discussões e até mesmo memes e convidamos os funcionários a participar.
4. Auditorias: Como nosso time SPA é responsável pelas auditorias de segurança, privacidade e conformidade de cada recurso do produto, ele usou essas auditorias como uma oportunidade de educação. Eles fizeram breves apresentações para fazer com que vários times percebam as implicações que as auditorias tiveram em sua função específica.
5. Cultura e eventos: Nós usamos festividades locais, como Pongal em nossos escritórios da Índia, e ocasiões internacionais, como o Data Privacy Day, para levar a maior participação. Cartazes, competições e brindes nos ajudaram a chamar a atenção de todos.

Acima de tudo, o elemento crucial para preparar a Zoho para o GDPR foi um esforço consistente durante um período.



5 OS TRÊS Ps DA CONFORMIDADE


Você sabia?
De acordo com um estudo de 2017, governança, regulamentação e controle eficazes reduzem os custos de conformidade quando as seguintes práticas recomendadas são implementadas:
* Governança centralizada - economia de 3,01 milhões de dólares
* Auditorias de conformidade - economia de 2,86 milhões de dólares
* Integração com funções de segurança e privacidade -economia de 2,02 milhões de dólares



As conexões entre pessoas, processos e produtos

A frase "As pessoas executam processos para criar produtos" descreve com precisão qualquer negócio. Modelar essa declaração em uma estrutura é onde está a chave para a governança, a regulamentação e o controle (GRC) eficazes. Abaixo está uma representação lógica desta estrutura:

***(1,n)** - Um objeto na categoria esquerda pode ser mapeado para qualquer número de objetos na categoria direita*

***(1,1)** - Um objeto na categoria esquerda pode ser mapeado para apenas um objeto na categoria direita*

- Pessoas, Processos e Produtos são entidades. Cada instância de uma entidade é um objeto. Por exemplo:
  - Em Pessoas, um executivo de RH ou um desenvolvedor é um objeto.
  - Em Processos, uma atividade (como contratação) ou uma função de negócios (como desenvolvimento de produto) é um objeto.
  - Em Produtos, uma aplicação ou infraestrutura que sua empresa produz é um objeto.

- **Pessoas (1,n) Processos:** Cada objeto em Pessoas pode ser mapeado para qualquer número de objetos em Processos.
  - Uma pessoa ou departamento pode estar envolvido em muitos processos. Por exemplo, um executivo de RH pode estar envolvido na contratação, integração e gerenciamento de reclamações. Um profissional de marketing pode estar envolvido na geração de leads, bem como nas relações públicas.
  - Por que não é "(n,1)"? Embora logicamente faça sentido que mais de uma pessoa ou departamento possa estar envolvido em um processo, essa abordagem não se adapta à conformidade. As pessoas sempre orientam a conformidade assumindo a responsabilidade pelos processos nos quais estão envolvidas. Todas as pessoas em sua organização devem ser mapeadas para um processo. Você pode conseguir isso usando o seu portal de RH. Todos os usuários devem ser capazes de ver a quais processos eles estão mapeados.
  - Se um funcionário não puder ser mapeado para um processo, ele deverá receber mais clareza sobre sua função na empresa.

- **Processos (1,1) Produtos:** Cada objeto em Processos deve ser mapeado para apenas um objeto em Produtos. Mais uma vez, embora seja verdade que mais de um processo pode ser envolvido na criação de um produto, o conceito de um produto é mais inclusivo quando se trata de conformidade:
  - Um produto significa qualquer valor criado fora de um processo. Isso inclui:
    - O produto ou serviço final pelo qual os clientes pagam.
    - Componentes como bibliotecas de software, inventário de ferramentas, registros de ativos e até mesmo planilhas cruciais. Eles também são produtos porque são consumidos pelos usuários dentro da sua organização.
  - Cada processo produz algum produto que é vendido aos clientes ou utilizado internamente em outro processo, levando eventualmente à criação do produto final pelo qual seus clientes pagam.
  - Se um processo não puder ser mapeado para um produto, em outras palavras, ele não produzirá nenhum valor, ele não deverá existir.

A lista de Pessoas, seu portal de RH, pode ser mapeada para a sua lista de processos, que é o seu registo de atividade. Além disso, sua lista de Produtos é o inventário de todo o valor que sua organização cria.

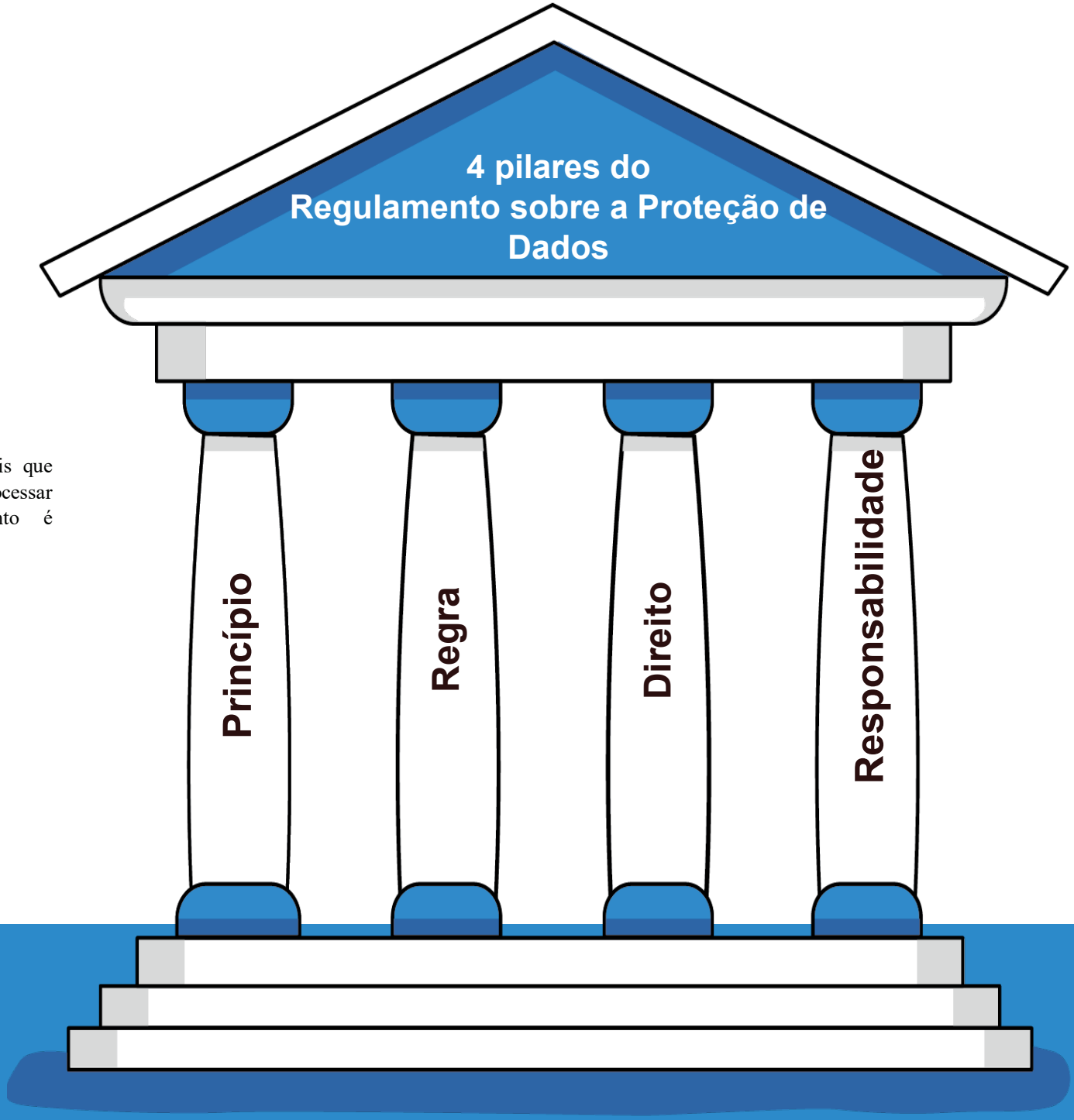
Ao consolidar controles de certificações como ISO 27001 ou uma regulamentação como HIPAA, você pode mapear facilmente qual controle corresponde a qual entidade. Essa clareza o ajudará a decidir quanto esforço você deve colocar em cada área para atingir o nível desejado de conformidade.

Pense nisso...

A conformidade com padrões e regulamentos não é a mesma. Os ***padrões*** *são desenvolvidos por organizações internacionais, como ISO e ITU. As organizações podem optar por adotar esses padrões para melhorar a qualidade de seus processos.* ***Regulamentos*** *são leis que devem ser obedecidas se uma organização precisar fazer negócios na jurisdição.*

Lei

O GDPR, o HIPAA e o CCPA são leis que determinam como as empresas devem processar dados pessoais. Qualquer regulamento é sustentado por quatro pilares:



Princípios: Estes são os valores que os órgãos reguladores querem que você tenha em mente e aplique em todos os seus processos. No GDPR, o capítulo 2 (Art. 5-11) é totalmente dedicado aos princípios que devem ser seguidos durante o processamento de dados pessoais.

- **Legalidade, justiça e transparência:** O GDPR fornece seis bases legais, e qualquer processamento (coleta, uso, divulgação e armazenamento) deve estar de acordo com uma dessas leis.
- **Limitação do propósito:** Você deve coletar e usar os dados somente para a finalidade declarada e coletar dados somente pelo tempo necessário para concluir essa finalidade.
- **Minimização dos dados:** Você deve garantir que os dados pessoais processados sejam adequados e relevantes para o que for necessário em relação à sua finalidade de processamento.
- **Exatidão:** Você deve tomar todas as medidas razoáveis para atualizar ou remover dados imprecisos ou incompletos.
- **Limitação do armazenamento:** Você deve excluir dados pessoais quando não precisar mais deles.
- **Integridade e confidencialidade:** Você deve manter os dados pessoais seguros e protegidos contra processamento não autorizado ou ilegal, bem como perda acidental, destruição ou danos, usando medidas técnicas ou organizacionais apropriadas.

Da mesma forma, a Lei Geral de Proteção de Dados (LGPD) do Brasil lista 10 princípios que devem ser levados em conta no processamento de dados pessoais, como limitação de finalidade, necessidade, transparência, segurança, não discriminação, e responsabilidade.

Os princípios entram em ação quando foram esboçadas políticas para reger seus processos.

Regras: Estas geralmente descrevem o que acontece quando você não está em conformidade com a lei ou são as instruções permanentes quando você a cumpre. Por exemplo, o artigo 83 do GDPR descreve o quanto as organizações serão multadas com base no tipo e na gravidade da violação que enfrentam. As regras também descrevem as ações que você precisa tomar para garantir que os princípios sejam implementados.

Da mesma forma, a Seção 1798.155(a) do Título 1.81.5 do CCPA descreve a penalidade por violar o ato. Outras regras descrevem como responder a violações e como informar os titulares dos dados.

As regras entram em jogo quando procedimentos foram esboçados e padronizados para seus processos.

Direitos e responsabilidades: O Capítulo 3 do GDPR estabelece os direitos que os titulares dos dados têm e o Capítulo 4 descreve as responsabilidades que as organizações têm quando assumem a função de controlador ou processador.

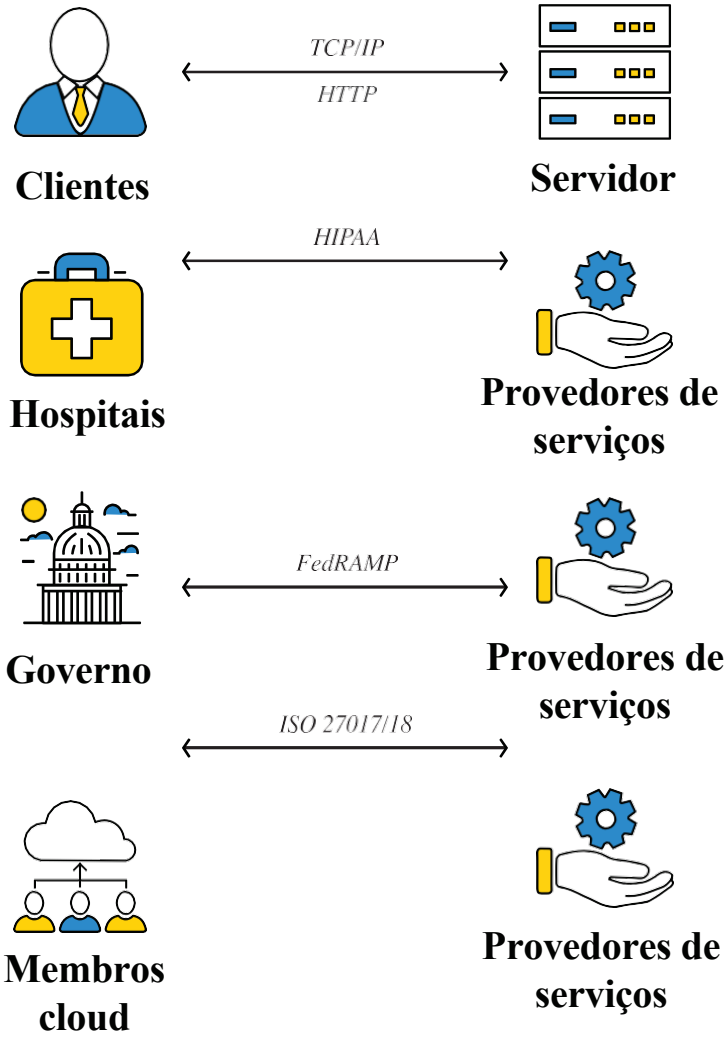
Os direitos e as responsabilidades afetam as atividades de processamento da sua organização.

Por exemplo, o "direito de ser esquecido" no GDPR mudará a forma como você processa os dados. Você perceberá que não é mais possível enviar vários e-mails de suporte distribuídos em várias caixas de entrada. Um sistema de suporte técnico consolidado pode garantir que todos os dados correspondentes a um ticket de suporte estejam em um local, de modo que, quando o direito de ser esquecido for invocado, tudo o que você precisa fazer será concentrar-se no suporte técnico em vez de em várias caixas de entrada individuais.

Padrões

Os padrões são o que ajuda um cliente nos EUA a comprar um medidor de tecido de um fornecedor na Ásia. Graças a um desses padrões, o Sistema Internacional de Unidades, pessoas em todo o mundo podem entender as expectativas uns dos outros sem complicações.

Toda comunicação precisa de um padrão para ser eficaz. Um servidor entende um cliente por meio do Protocolo de Controle de Transferência (TCP, Transfer Control Protocol). Da mesma forma, o governo dos EUA entende os provedores de serviços por meio do FedRAMP. Quando um provedor de serviços é certificado com padrões, os usuários saberão o que esperar dele e não terão que testar pessoalmente os processos do provedor para garantir a consistência.



Os padrões têm um conjunto de definições, controles e requisitos que precisam ser atendidos para que a consistência seja estabelecida entre todas as partes.

A conformidade com os padrões é uma questão de compreender as definições e mapear os controles de um padrão para seus processos. *Os controles, aqui, são medidas ou certas atividades que os padrões esperam que você execute.* Há dois casos:

- Se o padrão exigir um controle que não faz parte do seu processo, você pode tentar incluí-lo no seu processo ou dar a justificativa de que a ausência de tal controle não afeta as expectativas dos clientes.
- Se o padrão exigir um controle que faça parte do seu processo, você deverá coletar evidências suficientes de que o controle é executado de forma eficaz e eficiente.

Auditorias

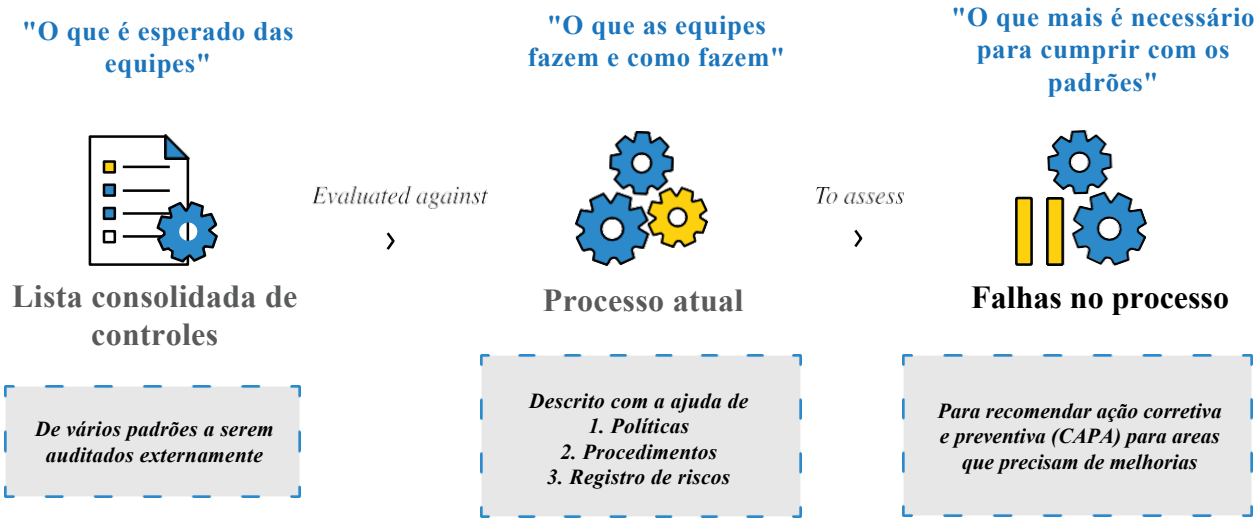
As auditorias determinam o que te falta em relação a um determinado padrão. Nesse sentido, as auditorias internas e externas são as mesmas. No entanto, a necessidade de se concentrar mais nas auditorias internas surge do problema da escala. Considere um exemplo:

A Zylker, depois de grandes esforços, obtém sua primeira certificação ISO 27001. No entanto, quer expandir ainda mais para SOC, PCI e outros padrões ISO, como 27017 e 27018. As auditorias externas estarão ocorrendo durante todo o ano se a Zylker for receber essas muitas certificações.

É prático que a Zylker realize auditorias internas para cada padrão com que escolha estar em conformidade com o que vai acontecer? Cada time de produto e operações deve dedicar muitas horas de trabalho para auditorias internas e externas, e isso pode se tornar um obstáculo à produtividade, o que derruba todo o ponto de controle do processo. Então, qual é a solução?

Consolide os requisitos de auditoria em uma lista de controles. Liste todas as expectativas que você tem dos times com relação a esses padrões e crie uma lista consolidada de controles.

Em seguida, você pode agendar duas ou três auditorias internas por ano para avaliar o processo atual dos times em relação ao conjunto desejado de controles, da seguinte maneira:



A auditoria interna prossegue então para a coleta de evidências para as avaliações de lacunas e a implementação da CAPA. Tais evidências devem abranger tudo, inclusive comunicações por e-mail, capturas de tela de processos e registros de auditoria, para comprovar a conformidade do processo real com os controles padrão.

ZOHO E AUDITORIAS

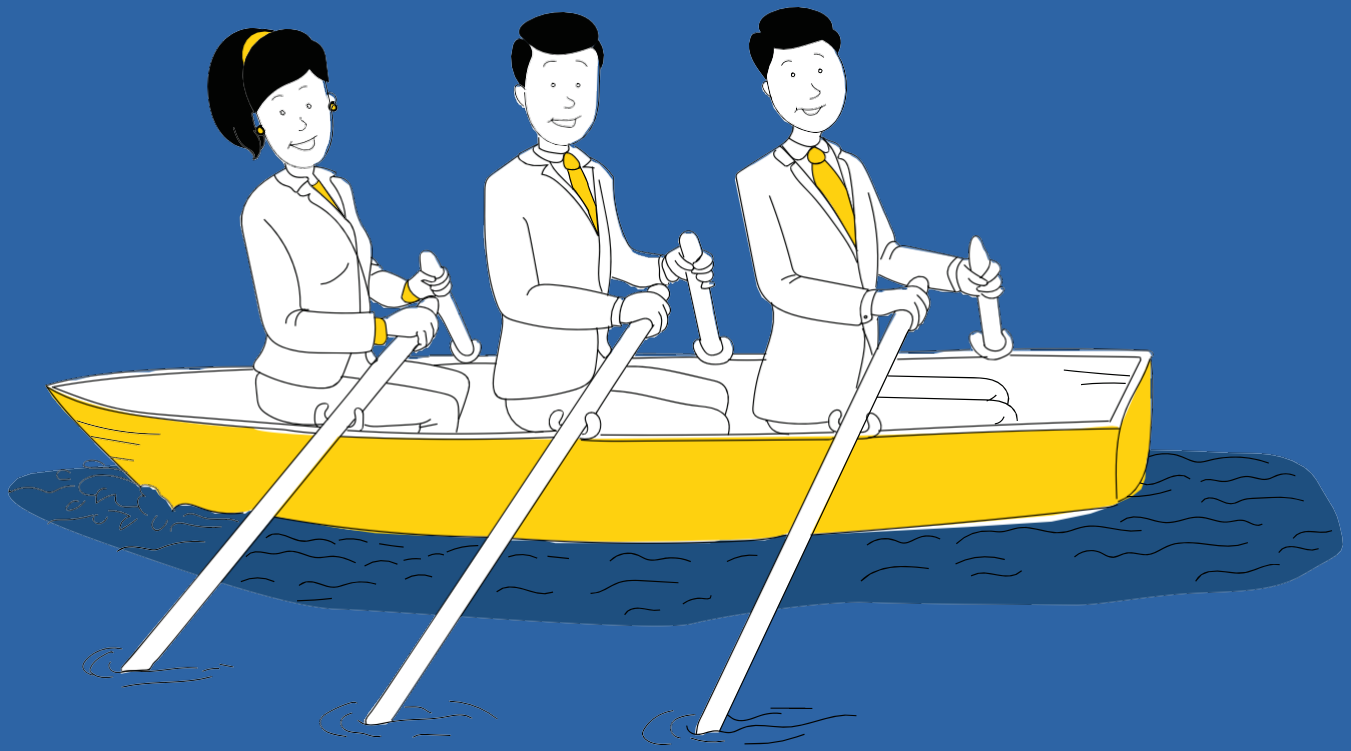
À medida que expandimos nosso portfólio de conformidade, sempre há outra auditoria por vir. Embora as auditorias iniciais fossem desafiadoras, pudemos incluir uma seção de "prontidão da auditoria" nos processos dos times para mantê-las no circuito e configurá-las para auditorias externas.

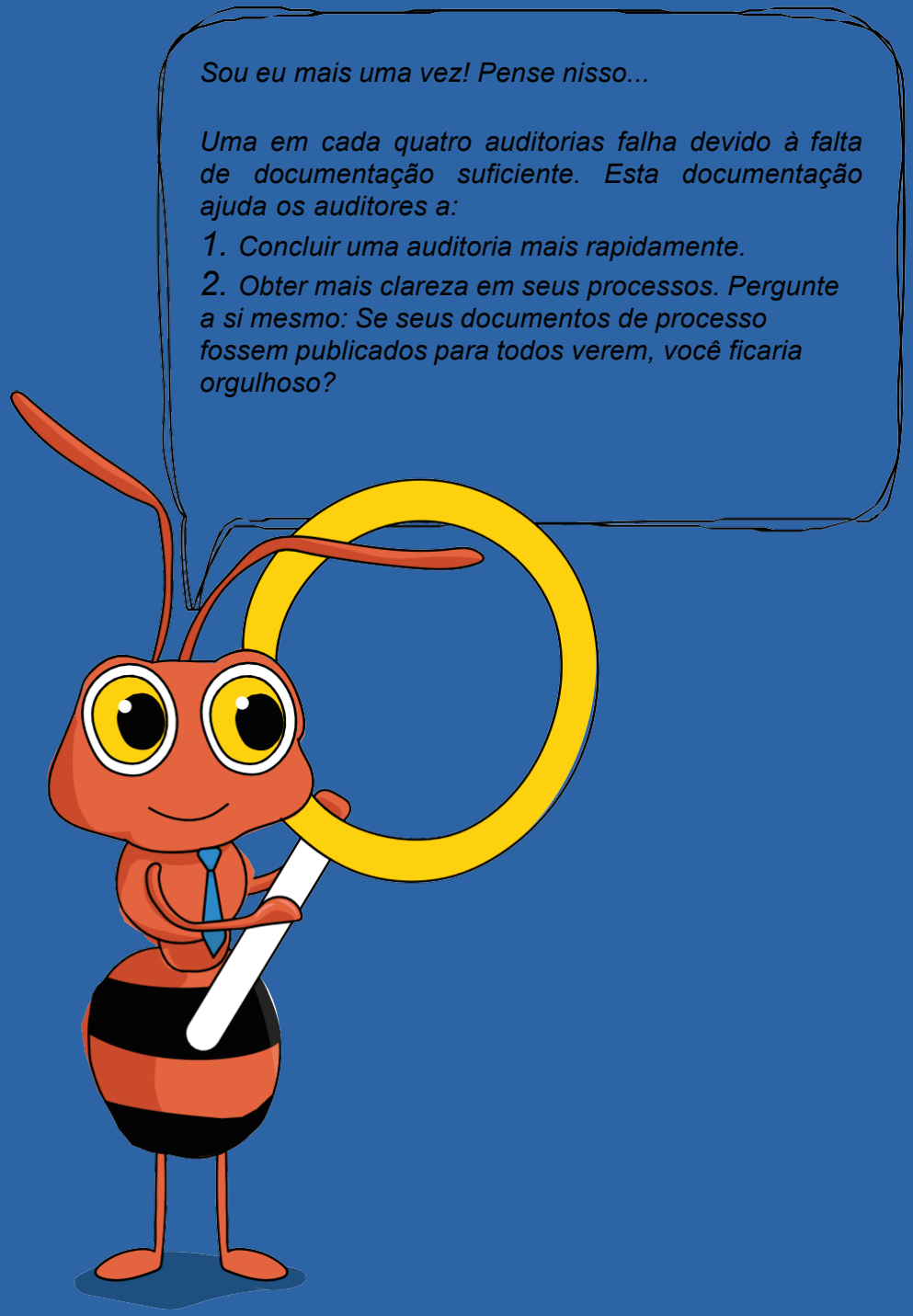
As dificuldades iniciais também nos ajudaram a ensinar como cada padrão é diferente. As auditorias ISO, como a ISO 27001, concentram-se fortemente no sistema de gerenciamento de segurança das informações (ISMS) da organização, enquanto o SOC 2 concentra-se em controles no nível do sistema com atenção especial à proteção de dados. De uma perspectiva de auditoria, esses padrões parecem estar a quilômetros de distância mas, de uma perspectiva de processo, é possível consolidá-los em um sistema de controles. Na verdade, se o controle de processo de uma organização for eficiente e eficaz, a conformidade com qualquer padrão poderá se tornar apenas uma questão de extrapolação sobre os processos existentes.

Para enfrentar várias auditorias externas ao longo do ano, a estrutura de auditoria interna de uma organização precisa ser robusta. É por isso que uma abordagem baseada em estrutura é a melhor maneira de manter a conformidade.

36

6 GERANDO RESPONSABILIDADE





Você já se perguntou como a responsabilidade pode ser útil da perspectiva da conformidade e da produtividade?

Sua organização é composta por milhares de atividades executadas por vários times. Portanto, sua organização se torna compatível quando cada atividade se torna compatível. No entanto, pode haver não conformidades (NCs) nas atividades. E cada vez que você fixa uma NC, você fica mais em conformidade. Como você garante que, quando uma NC é corrigida em uma atividade, atividades semelhantes em sua empresa não cometem o mesmo erro?

Por exemplo, a Zylker considera a codificação como uma "atividade" na empresa. Há 25 times realizando esta atividade, com centenas de desenvolvedores de software. Um desenvolvedor de um time escreveu algum código contendo uma configuração incorreta de segurança que resultou em um bug. Esse problema, uma NC em OWASP, foi resolvido posteriormente. Esse time em particular aprendeu a lição de ter cuidado com as configurações incorretas de segurança sempre que codificam, mas e os outros 25 times e seus códigos?

Há uma boa chance de:

Nº de vezes que uma NC pode ocorrer = Nº de atividades relevantes para essa NC

Como você pode garantir que o número de NCs diminua? Como você garante que cada desenvolvedor seja cauteloso com essa NC e não cometa o mesmo erro em seu código?

A resposta está na responsabilidade. Se a pessoa responsável por cada atividade for conhecida e registrada, ela será obrigada a garantir que a atividade esteja em conformidade.

Assim que a NC é identificada, o time SPA da Zylker envia um e-mail para todas as pessoas responsáveis, informando-as sobre esta NC, incluindo os passos que devem dar para garantir que esta NC não se repita em suas atividades.

Esta é a primeira etapa da estrutura 3P, na qual você mapeia Pessoas e Processos juntos.

Como você faz isso?

Você invoca uma das ferramentas mais poderosas para a conformidade: documentos.

Documentos: Seus principais instrumentos

Qual é a forma mais simples e lógica de começar a colocar a abordagem 3P em funcionamento? Colocá-la no papel. Mas primeiro, lembre-se de que muitos funcionários têm essas noções preconcebidas sobre documentação:

- "É um trabalho adicional, algo que reduzirá minha produtividade."
- "Não serve para nenhum propósito real, pois estou apenas repetindo o que sei."

No entanto, documentar é o primeiro passo em direção à clareza. Tudo o que você sabe sobre o seu trabalho está apenas na sua cabeça. Somente quando ele vai para o papel você realmente sabe o que sabe e o que não sabe.

Até que você documente com confiança o que faz, é quase impossível determinar as áreas nas quais você pode fazer melhor.

Uma instituição sem a documentação adequada não é vista com bons olhos por reguladores e agências de aplicação da lei.

O princípio de responsabilidade do GDPR, que indiretamente sugere uma documentação abrangente, é tão importante quanto sua agenda jurídica. O artigo 30 do GDPR enfatiza a necessidade de criar um "registro de atividades de processamento" e considera que as organizações precisam demonstrar "proteção de dados por projeto e por padrão", o que implica que você deve identificar e corrigir problemas na fase inicial de processamento.

Mostraremos como você pode documentar o seguinte:

- Suas atividades que fazem parte do trabalho (registro de atividade, matriz RACI)
- Detalhes dos produtos, serviços ou produtos finais (registro de ativos de informações)
- Os perigos potenciais associados a esses processos e como você lidaria com eles (avaliação de riscos)

O exposto acima é literalmente o que todo padrão internacional espera de você. Ter esse tipo de documentação simplifica a obtenção de certificações como ISO e SOC, pois seus documentos são a principal e mais confiável fonte de comunicação com auditores externos.

Registro de atividades

Um registro de atividades é a adaptação mais direta do Art. 30 do GDPR. Basta listar todas as atividades da sua empresa. Mesmo que não seja usado para conformidade, um registro de atividade é algo bom de se ter.

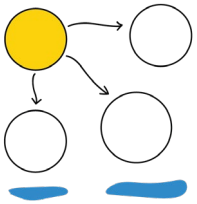
Cada atividade é um componente básico da sua organização. Sua empresa terá uma estrutura de conformidade sólida e inviolável somente quando cada bloco for responsável, compatível e robusto.

Para levar a responsabilidade às atividades da sua organização, você também precisa mencionar quem é responsável por essa atividade - em outras palavras, quem será questionado se a atividade sair do controle.

Há várias maneiras de fazer isso:

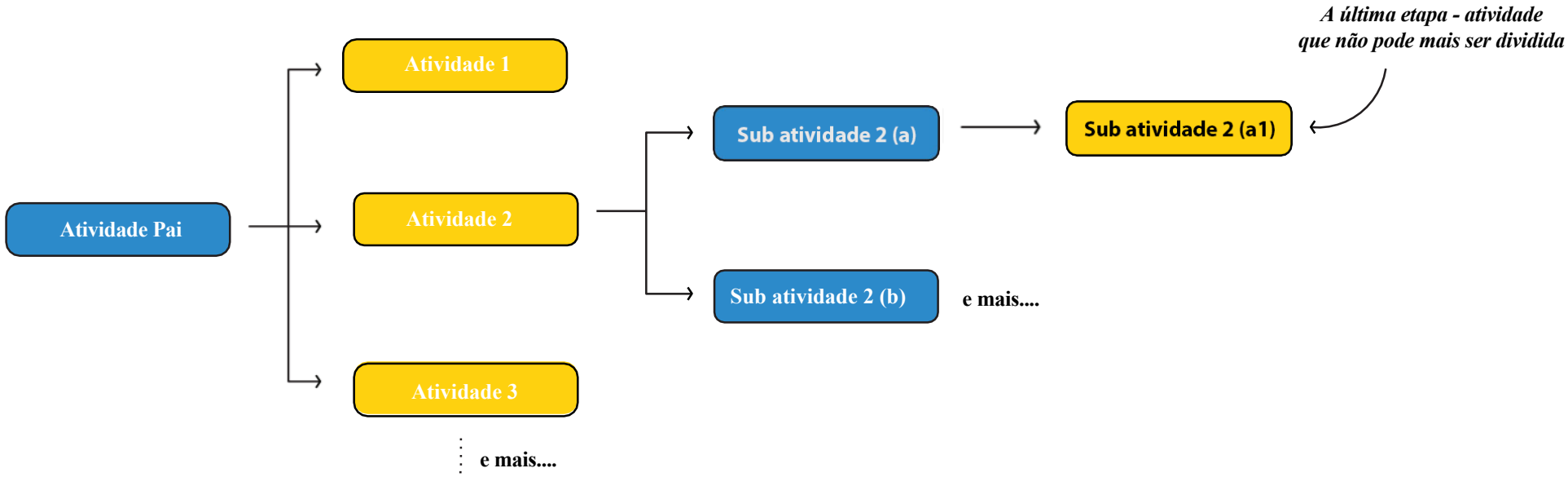
- Método 1: Peça a cada pessoa da sua empresa que registre o que eles fazem como parte de seu trabalho. → Reúna todas essas atividades e faça um registro. → Para cada atividade, identifique a pessoa responsável.
- Método 2: Atribua gerentes para este projeto. → Peça que eles listem cada atividade de seu time. → Peça aos gerentes para marcar uma pessoa responsável em seu time para cada atividade.
- Método 3: Peça ao time SPA para criar uma lista de atividades para a empresa com base em funções. → Peça aos gerentes para usarem essa lista como base e fazerem modificações para se adequar aos seus times. → Peça aos gerentes para marcar as pessoas responsáveis por cada atividade. → Exija que as pessoas responsáveis verifiquem a lista.

Dependendo do tamanho da sua organização, da natureza e da experiência do seu time SPA e da cultura da sua organização, você pode escolher o método mais adequado para você.



Árvore de atividades

Uma árvore de atividades resolve os problemas gerenciais que ocorrem quando você adiciona suas atividades em uma planilha e elas se acumulam em centenas de linhas, dificultando a pesquisa e extração de dados. Para classificar isso, você pode usar uma árvore de atividades:



Dessa forma, você pode escolher em qual nível da árvore de atividades está interessado.

Quando se trata de listar atividades, é comum ficar preso em algumas perguntas:

- **Que tipo de atividades não deve ser mencionadas no registro?**

Para atividades operacionais como recrutamento e suporte, não é necessário mencionar exemplos de atividades. Vamos supor que a Zylker recruta novos recém-formados todos os anos. Recrutar graduandos universitários é uma atividade liderada por John Taylor, do RH da Zylker, e deve constar no caixa. No entanto, contratar de uma faculdade específica para o ano de 2020 para um time específico é um exemplo de recrutamento, por isso não deve ser mencionado, uma vez que John repete essa atividade muitas vezes. John lida com essas instâncias usando ferramentas de gerenciamento de projetos, como o Zoho Projects.

- **Qual o nível de especificidade que você precisa ter ao listar as atividades?** Depende da pessoa responsável. Se não conseguir encontrar uma pessoa que seja por si só responsável subatividade 2(a1) nailustração acima, esta deve ser interrompida.

Por exemplo, o time administrador de sistemas da Zylker, liderado por Graham Peterson, é estruturado de forma tal, que faz com que Michael Smith lide com todas as atividades de integração para novos funcionários, enquanto o processo de saída é realizado por Brendon Drake. Michael lida com todas as atividades de integração, como atribuição de *notebooks*, criação de contas, garantia de criptografia e fornecimento de gadgets e software. Brendon recupera todos os *gadgets* e atualiza o registro de ativos durante o processo de saída, mas é tarefa de Martin Groove remover pseudônimos de e-mail e desligar o acesso a ambientes críticos, como data centers.

Aqui, a árvore de atividades para em "Integração", enquanto o "Processo de saída" se ramifica para "Recuperação de gadgets e atualização do registro de ativos" e "Remoção de pseudônimos de e-mail e desligamento do acesso a ambientes críticos".

- **Devem ser mencionadas ações corriqueiras, como fazer login em uma conta ou acessar um servidor?** Esse nível de detalhe não é necessário, pois essas informações podem ser adicionadas como o procedimento para a subatividade que não admite maiores ramificações.

- **Como as atividades de desenvolvimento/produção devem ser mencionadas?**

Os desenvolvedores geralmente são responsáveis por um recurso ou módulo no produto ou serviço no qual estão trabalhando. O desenvolvimento em si pode ser uma atividade com subatividades, mas o recurso ou módulo em que um desenvolvedor está trabalhando deve ser listado junto com o nome do desenvolvedor no registro de atividades.

Por exemplo, a Zylker está desenvolvendo uma plataforma educacional, Think, para que as empresas ajudem a educar e avaliar o conhecimento de seus usuários em relação a qualquer assunto. Este projeto é liderado por Dwayne Charles. Nesta plataforma, Julie Ann está desenvolvendo o módulo de conteúdo para armazenar e distribuir materiais educacionais, enquanto Lisa Bingel é responsável pelo módulo de avaliação que faz perguntas aos usuários. Embora ambas estejam realizando a mesma atividade, desenvolvimento, faz mais sentido incluir os módulos que estão desenvolvendo no registro de atividade para melhor responsabilidade.

- **Qual é a função real de uma pessoa responsável?**

Uma pessoa responsável garantirá que sua atividade esteja em conformidade. Elas receberão ferramentas e educação por meio do time SPA.

Atividade pai	Atividade	Responsável
Operações Zylker	Sysadmin	Graham Peterson
Sysadmin	Integração	Michael Smith
Sysadmin	Processo de saída	Brendon Drake
Processo de saída	Recuperação de gadgets e atualização do registro de ativos	Brendon Drake
Processo de saída	Remoção de apelidos de email e terminação de ambientes com acesso crítico	Brendon Drake
Zylker - Think	Desenvolvimento	Dwayne Charles
Desenvolvimento - Think	Módulo de conteúdo	Julie Ann
Desenvolvimento - Think	Módulo de avaliação	Lisa Bingel

A magia do RACI

Uma atividade envolve mais do que apenas a pessoa responsável por ela.

Por exemplo, a unidade de recrutamento no campus da 2020 em Zylker envolve mais do que apenas John. Dwayne, gerente do projeto Think, decide quantos desenvolvedores ela precisa. Lisa avalia os candidatos e dá a opinião apropriada ao time de RH. John pede então que seu time conduza a entrevista final. Graham, o administrador de sistemas, deve saber sobre a unidade de recrutamento, pois ele deve levantar a solicitação de ativos e obtê-los antes que os recrutas se juntem. Da mesma forma, os times de finanças e administração também devem ser notificados sobre o evento de contratação.

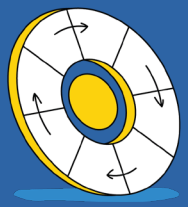
Embora John esteja designado como responsável pela atividade, envolve também outras funções.

Estas são as quatro funções cruciais:

- **Responsável principal:** Aquele que assume o comando da atividade e, em última análise, responde por isso. Deve ser um indivíduo, uma vez que ter mais de uma pessoa responsável leva a conflitos de interesse e confusão. No exemplo acima, apenas John é o responsável principal.
- **Responsáveis:** As pessoas que realmente realizam a atividade. Pode ser uma pessoa, um time ou um grupo *ad hoc*. Eles respondem ao responsável principal. Em nosso exemplo anterior, o time de recrutamento de cinco pessoas sob supervisão de John será designado como responsável.
- **Consultados:** As pessoas que oferecem opiniões. Geralmente, são especialistas no assunto que devem ser consultados antes que uma decisão seja tomada. Esta situação poderá ser concretizada por um indivíduo ou um time. Em termos de orientação de recrutamento da Zylker, o time de projetos Zylker - pensada por Dwayne, que avalia a capacidade técnica dos candidatos, será consultado antes de serem tomadas quaisquer decisões de contratação.
- **Informados:** As pessoas que devem ser mantidas constantemente informadas sobre como a atividade está progredindo. Pode ser uma pessoa, um time ou um grupo de indivíduos. Em nosso exemplo acima, Graham do time administrador de sistemas, juntamente com os times de finanças e administração, será mantido informado sobre essa atividade.

Para cada atividade listada no registro de atividade, identifique quatro grupos que são responsáveis principais, responsáveis, consultados e informados (em resumo, RACI). Depois de fazer isso, sua atividade estará realizada apropriadamente. E por que chamamos isso de mágica anteriormente? Porque ele resolve problemas reais que você nem sabia que estavam lá:

- Incerteza sobre quem toma decisões
- Criação e envolvimento em trabalho não essencial para preencher o tempo
- Perguntas sobre quem faz o quê
- Um ambiente de trabalho reativo em vez de um ambiente proativo como uma atitude "não tenho tanta certeza, portanto não faço nada"
- Culpar os outros por não fazer o trabalho



A primeira etapa de sua estrutura de conformidade

Eis como seria o registo de atividade da Zylker após o toque de RACI:

Atividade pai	Sub atividade	Responsável	Encarregado	Consultado	Informado
RH	Recrutamento	john.taylor	Equipe de recrutamento (D)	Zylker - Think (D)	graham.peterson, finance (D), admin (D)
Operações Zylker	Administração do sistema	graham.peterson	michael.smith, brendon.drake	-	Alta gerencia
Sysadmin	Integração	michael.smith	michael.smith	-	Dono do projeto
Sysadmin	Processo de saída	brendon.drake	Brendon.drake, martin.groove	-	Dono do projeto
Processo de saída	Recuperação de gadgets e atualização de registro de ativos	brendon.drake	Brendon.drake	Gerente	-
Processo de saída	Remoção de apelidos de email e terminação de acesso a ambientes críticos	martin.groove	martin.groove	Gerente	Dono do projeto

Agora você sabe o que faz e quem faz exatamente isso.

Sugestões úteis:

- *É preferível indicar pessoas com IDs exclusivos para eliminar confusão. Isso pode ser seu endereço de e-mail (micheal.smith@zylker.com) ou ID de funcionário (Zylker-1234). No exemplo acima, listamos o endereço de e-mail de cada funcionário, mas deixamos o nome de domínio.*
    - *Isso também facilita vincular o registro de atividade ao seu portal de colaboradores.*
- *Também é aconselhável adicionar uma marca ao lado de departamentos ou times [como "(D)" em nosso exemplo] para que eles possam ser localizados e vinculados ao portal do funcionário.*
- *As colunas consultadas e informadas nem sempre precisam ser preenchidas. Para as atividades principais, como a administração do sistema, esse pode ser o caso.*
- *O responsável principal também será frequentemente responsável pela execução da tarefa. O proprietário e o gerente do projeto mudarão com os projetos. Então, em vez de mencionar tantos nomes nas colunas, "dono do projeto" será suficiente.*

O toque SPA: O time SPA deve criar um ambiente em que toda a organização possa ser aberta sobre as funções de qualquer indivíduo. Veja como isso pode acontecer:

- Eles devem criar um repositório central onde todas essas listas de atividades, com detalhes do RACI, são mantidas. Pode ser tão simples quanto uma planilha.
- Eles devem tornar a planilha acessível a toda a organização e dar aos respectivos gerentes a opção de editá-la sempre que necessário.
- As alterações a este repositório RACI devem ser regidas pelo time SPA. Qualquer alteração numa atividade deve ser partilhada com as partes nas colunas Consultado e Informado para que sejam preparadas.
- Se você tiver um módulo ou portal para gerenciar sua força de trabalho, onde cada funcionário tem um perfil, você poderá integrar este módulo à matriz RACI. Sempre que alguém se conectar, poderá encontrar a lista de atividades pelas quais é responsável ou simplesmente consultado e informado. Recursos para pesquisar funcionários, atividades e times responsáveis também podem ser incluídos.

ZOHO E A MÁGICA DO RACI

Com centenas de times de produtos, o uso de uma matriz RACI foi, de longe, a solução óbvia para obter o máximo de clareza sobre nossa organização. Olhar para o RACI mudou a forma como olhamos para os processos.

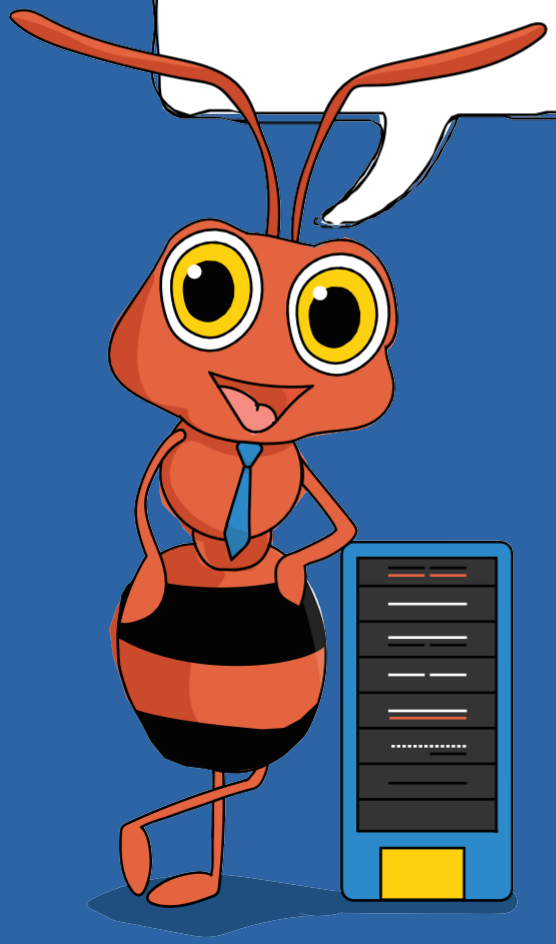
→ As pessoas têm um melhor senso de propriedade sobre o que estão fazendo. Uma vez que criamos e implementamos uma matriz RACI, o número de desculpas para não fazer as coisas começaram a diminuir.
→ Determinar o RACI para cada atividade nos ajudou a nos comunicar muito melhor. Os bate-papos em grupo são menos ativos, pois as pessoas sabem exatamente com quem se comunicar.
→ Reuniões para pequenos incidentes, auditorias de recursos internos etc. exigem menos pessoas, pois sabemos quem é responsável por quê.
→ As auditorias externas são mais suaves, pois os auditores são capazes de destacar facilmente a pessoa responsável que desejam questionar.

A conformidade realmente se torna uma responsabilidade compartilhada somente quando você criou uma matriz RACI para os processos da sua organização.

7 LIDAR COM ATIVOS DA MANEIRA CERTA

Pense nisso...

É 2020 e o universo digital está próximo de 44 trilhões de GB. Mas apenas quatro por cento das organizações podem extrair o valor total das informações que detêm. As violações de dados expuseram 4,1 bilhões de registros no primeiro semestre de 2019. Um hacker ataca a cada 39 segundos, com média de 2.244 vezes por dia. Portanto, os dados são o ativo mais crucial, e o acesso a eles tem um preço.



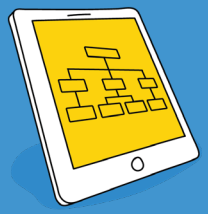
Qualquer coisa que seja de valor para você é um ativo. Tudo o que você gostaria de proteger é um ativo.

Essa definição é crucial, pois ajudará você a reconhecer os ativos de forma que possa ajustá-los à sua estrutura 3P. Então, quais são alguns dos ativos que você conhece?

- O edifício em que seu escritório está
- O computador que você usa
- O antivírus que seu administrador de sistema instala
- O software que você usa para gerenciar sua empresa
- O código que você desenvolve
- A impressora que você usa

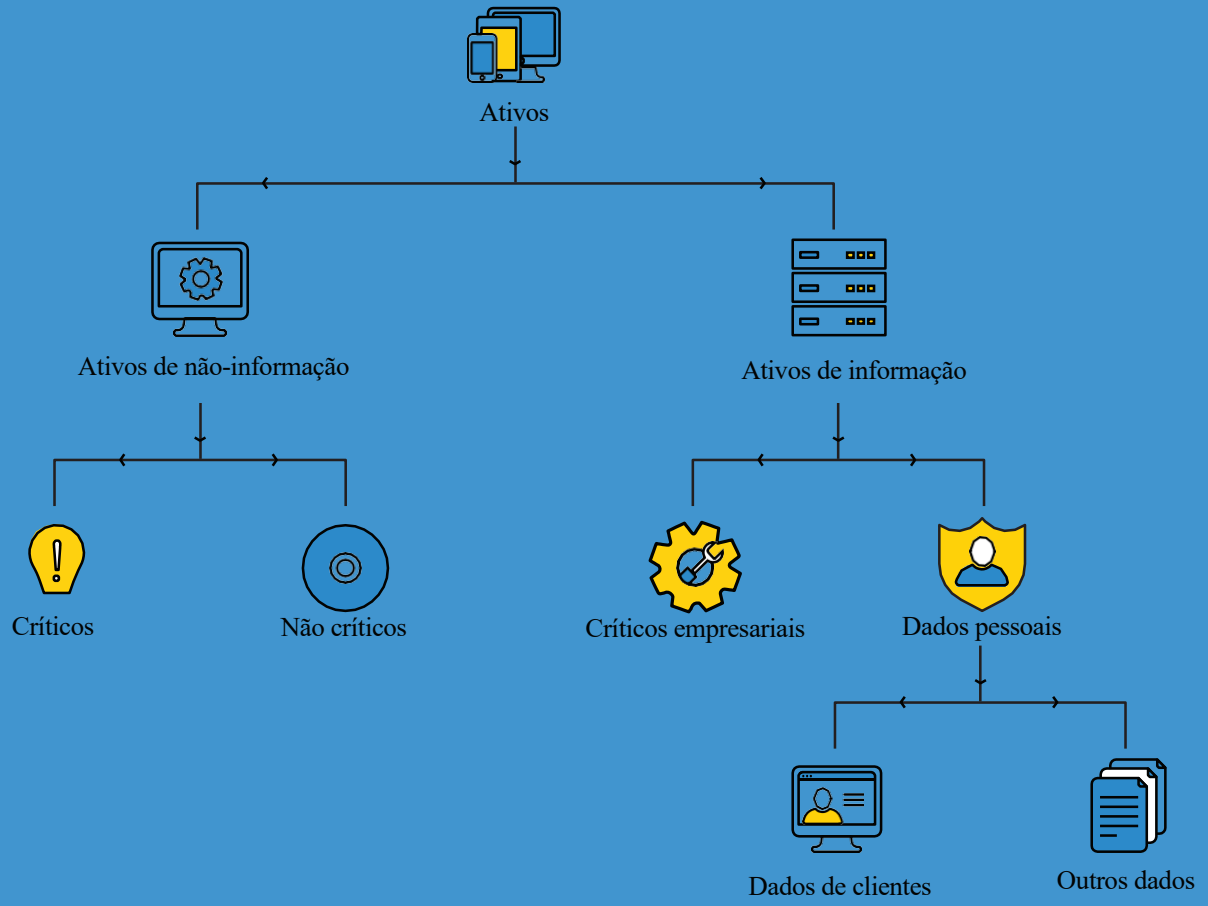
Se você quiser listar todos os ativos que gostaria de proteger, ela vai se tornar uma tarefa trabalhosa e complicada. Onde você começa e como procede a respeito disso? Duas coisas virão lhe socorrer:

- Classificação de ativos
- Sua relação com a estrutura 3P



Classificação de ativos

Não há uma maneira única e correta de classificar e gerenciar ativos, e isso depende da natureza da sua organização. No entanto, para auxiliar na conformidade, o método de classificação abaixo pode ser de muita valia:



As informações, sendo o ponto focal de sua classificação, ajudarão você a fazer algumas chamadas cruciais sobre quais ativos devem ser protegidos da melhor forma.

Todos os ativos que não sejam de informações podem ser protegidos física ou procedimentalmente, dependendo do nível de criticidade. No entanto, em termos de conformidade, os ativos de informações exigem uma abordagem mais elaborada. Mas, primeiro, devemos entender o que são dados pessoais.

Nota: Ao criar a lista de todos os ativos em sua empresa, os ativos podem ser marcados para indicar em qual categoria eles se enquadram. Isso pode ser feito com a ajuda de um símbolo exclusivo ou um código de cores que indica várias categorias de dados.

Dados pessoais

O artigo 4 do GDPR define os dados pessoais como "quaisquer informações relacionadas a uma pessoa natural identificada ou identificável".

O que consideramos dados pessoais depende de como analisamos essa definição.

- Pode ser subjetiva ou objetiva em sua natureza
- Pode consistir em informação sobre a vida privada ou uma atividade de um indivíduo
- O formato do dado pode indicar detalhes sobre um indivíduo

Qualquer informação **relacionada a**

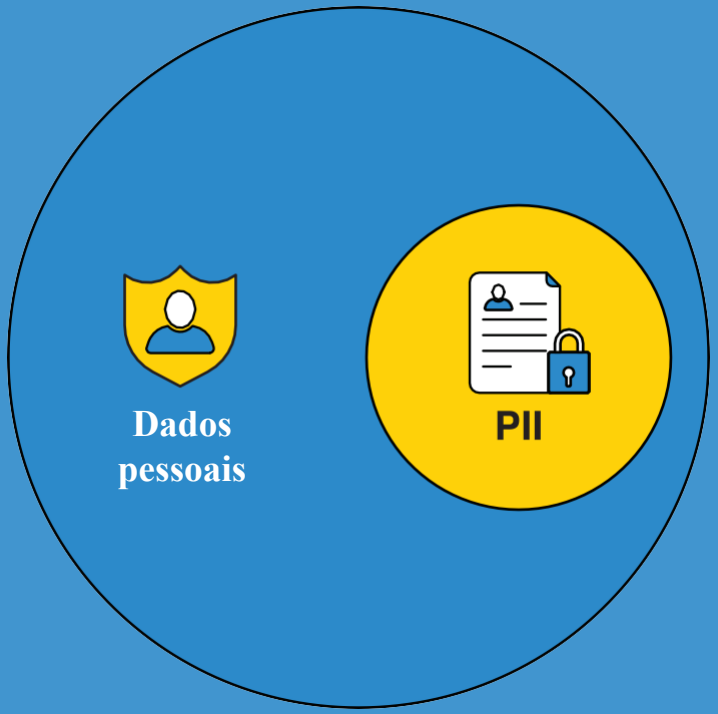
- Pode se referir diretamente a um indivíduo
- Pode avaliar, considerar ou analisar um indivíduo de uma certa maneira

uma pessoa natural identificável ou não identificável

Por exemplo, o valor monetário de uma casa é:

- Dados pessoais, se forem usados para fins fiscais.
- Dados não pessoais, se forem usados para fins imobiliários.

Como você pode ver, os dados podem ser pessoais dependendo da situação. Por segurança, é melhor tratar todos os dados com a mesma importância que os dados pessoais.



Informações pessoalmente identificáveis (PII): Qualquer informação sobre um indivíduo, mantida por uma pessoa ou organização, que pode ser usada para distinguir ou rastrear um indivíduo direta ou indiretamente.

PII é um subconjunto de dados pessoais e tem mais implicações se for violada, uma vez que pode ser usada para identificar diretamente um indivíduo e pode levar ao comprometimento dos direitos e da liberdade desse indivíduo. Aqui estão alguns exemplos:

- Nome, como nome completo, nome de solteira, nome de solteira da mãe ou apelido
- Número de identificação pessoal, como número de Seguro Social (SSN), número do Aadhaar, número do passaporte, número da carteira de motorista, número de identificação do contribuinte, número da conta financeira ou número do cartão de crédito
- Informações de endereço, como endereço físico ou e-mail
- Características pessoais, incluindo imagem fotográfica (especialmente do rosto ou outra característica de identificação), impressões digitais, escrita à mão ou outros dados biométricos (por exemplo, leitura de retina, assinatura de voz, geometria facial)
- Informações sobre um indivíduo vinculado ou vinculável a um dos exemplos acima

Registro de ativos de informações (IAR)

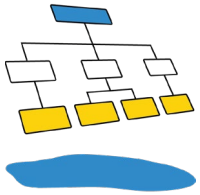
O registro e a manutenção sistemáticos de todos os ativos de informação são conhecidos como IAR. Este banco de dados é a única ferramenta mais eficaz para cumprir o princípio de responsabilidade do GDPR e simplificará muito sua conformidade com muitas outras leis e padrões.

Para cada atividade, o responsável principal deve ser encarregado de criar e manter o IAR.

São dois os componentes que formam o IAR: Registro

- de atividade e matriz RACI
- Diagramas de fluxo de dados

O registro de atividade e a matriz RACI formam a base do IAR, que é então construída com a ajuda dos diagramas de fluxo de dados.



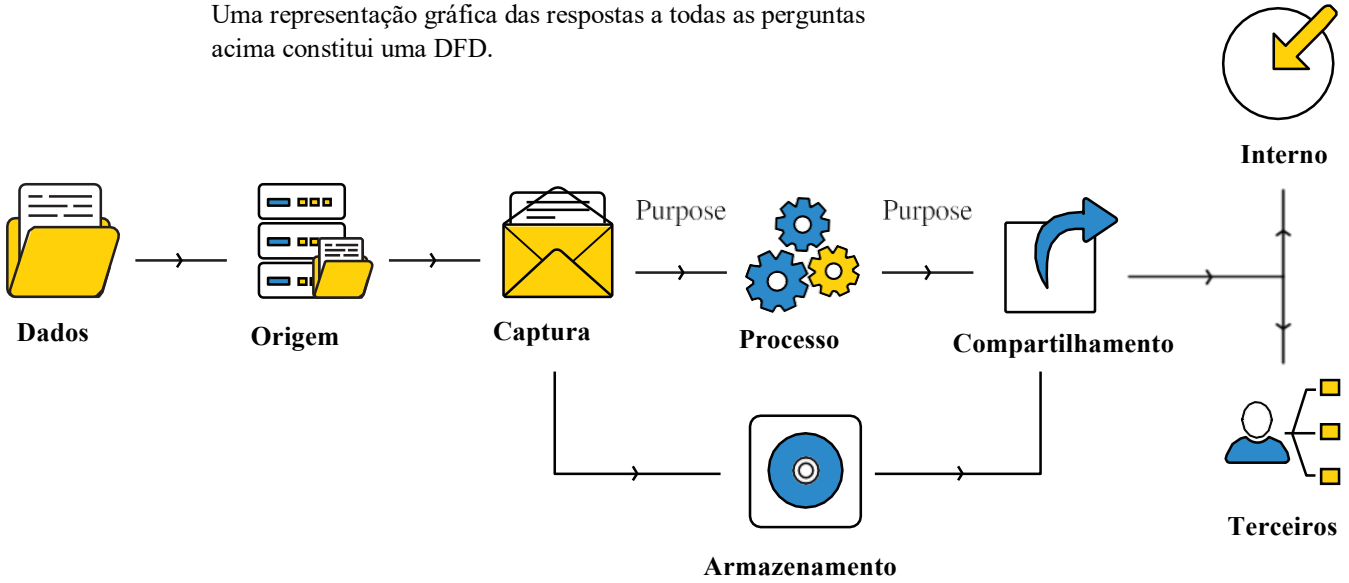
Diagramas de fluxo de dados (DFDs)

O registro de atividade e a matriz RACI devem fornecer a lista de todas as atividades.

Cada atividade dessa lista envolverá ativos de informações.

- Como o ativo de informações é tratado?
- Como ele é capturado?
- De onde ele se origina?
- Onde ele é armazenado?
- Como ele é processado?
- Com quem ele é compartilhado?

Uma representação gráfica das respostas a todas as perguntas acima constitui uma DFD.



Dados

Pode ser um ativo como um endereço de e-mail ou número de telefone, ou pode ser uma lista de ativos se todos eles receberem o mesmo tratamento.

Por exemplo, o time de marketing da Zylker realiza a atividade de coletar a lista de participantes de um evento corporativo. É esse o aspecto dos dados envolvidos:

Nome
Email
Nome da empresa
Tipo de negócio

Origem

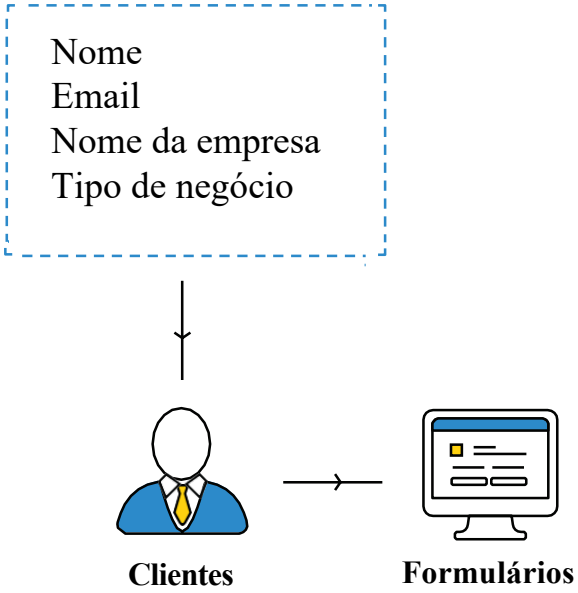
De onde esta atividade adquiriu os dados. Pode ser de um cliente, um banco de dados, outra organização ou fontes disponíveis publicamente. A Zylker coleta essas informações diretamente dos clientes.

Nome
Email
Nome da empresa
Tipo de negócio

Cliente

Captura

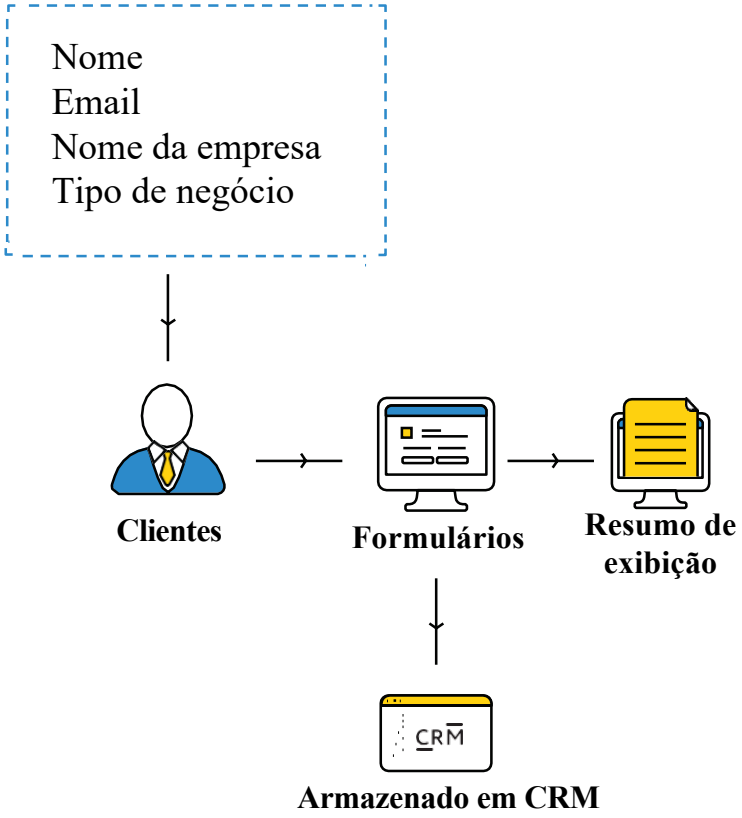
O meio pelo qual os dados foram adquiridos.



Os dados também podem ser capturados por e-mails, entrevistas, uma aplicação em nuvem ou qualquer outro meio.

Processos

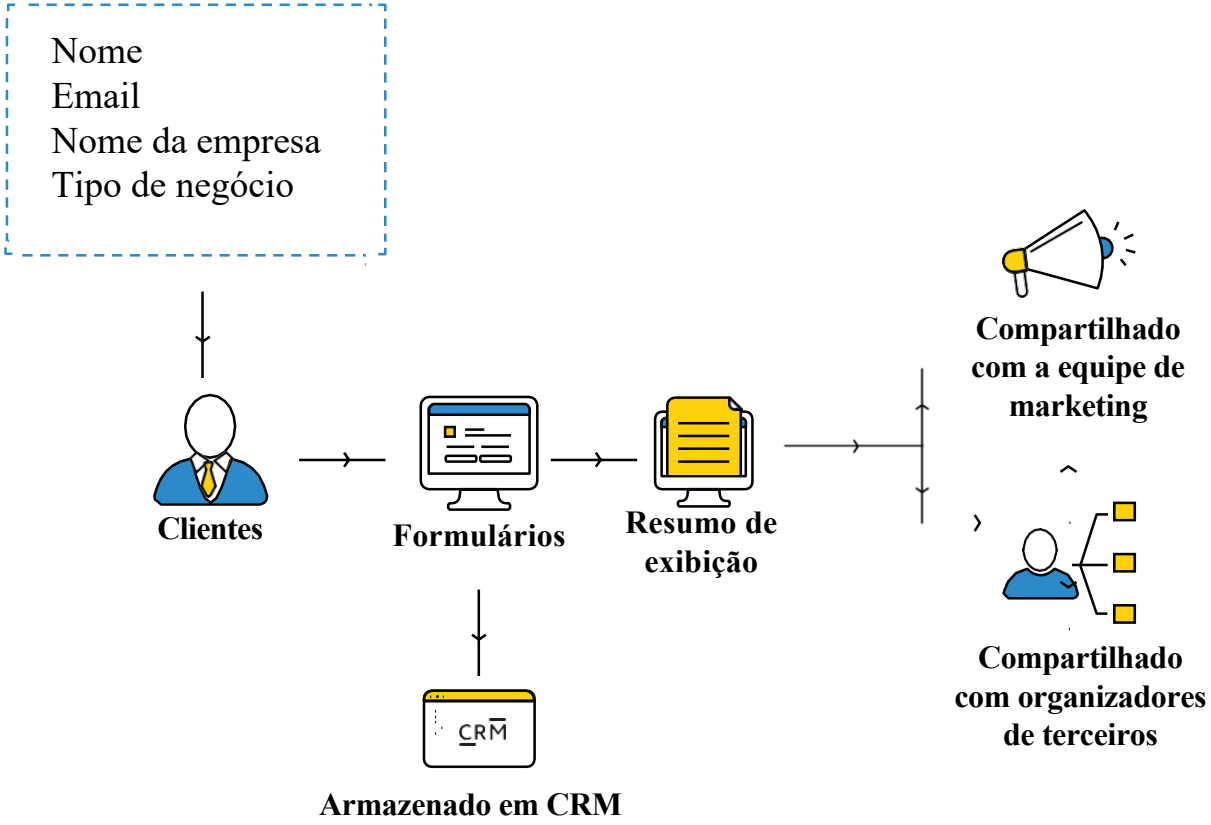
Como esses dados são utilizados na atividade.



Os dados podem ser enviados por e-mail, usados para executar um algoritmo de *machine learning* usados para análise ou para qualquer outro processo.

Compartilhar

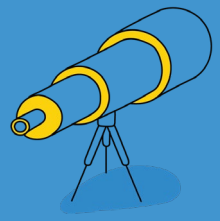
Compartilhar: Os dados podem ser compartilhados internamente com outros colaboradores ou times, ou com terceiros. Neste exemplo, os dados são compartilhados com uma empresa de gerenciamento de eventos.



Finalidade

Identificar a finalidade do processamento de dados é útil para cumprir a maioria dos padrões. No exemplo acima, o resumo dos dados coletados foi exibido. Qual é a finalidade disso? Da mesma forma, qual é a finalidade de compartilhar dados com terceiros ou outros grupos internos?

A finalidade pode fazer parte do DFD ou pode ser mencionada junto com a matriz RACI. A última opção é recomendada, pois facilita a compilação de todas as suas informações em um único documento que pode ser enviado às autoridades quando necessário.



Escopo de um IAR: Processo e produto

O Capítulo 4 do GDPR descreve claramente as obrigações dos controladores e processadores. Mais do que apenas listar as regras, esta parte do GDPR pode ajudá-lo a obter clareza sobre como deve ser o seu IAR. Há duas maneiras de criar DFDs para seus processos:

- DFD para o processo
- DFD para o produto

Ambos são igualmente importantes, pois são úteis em diferentes momentos em que você está no meio de uma auditoria.

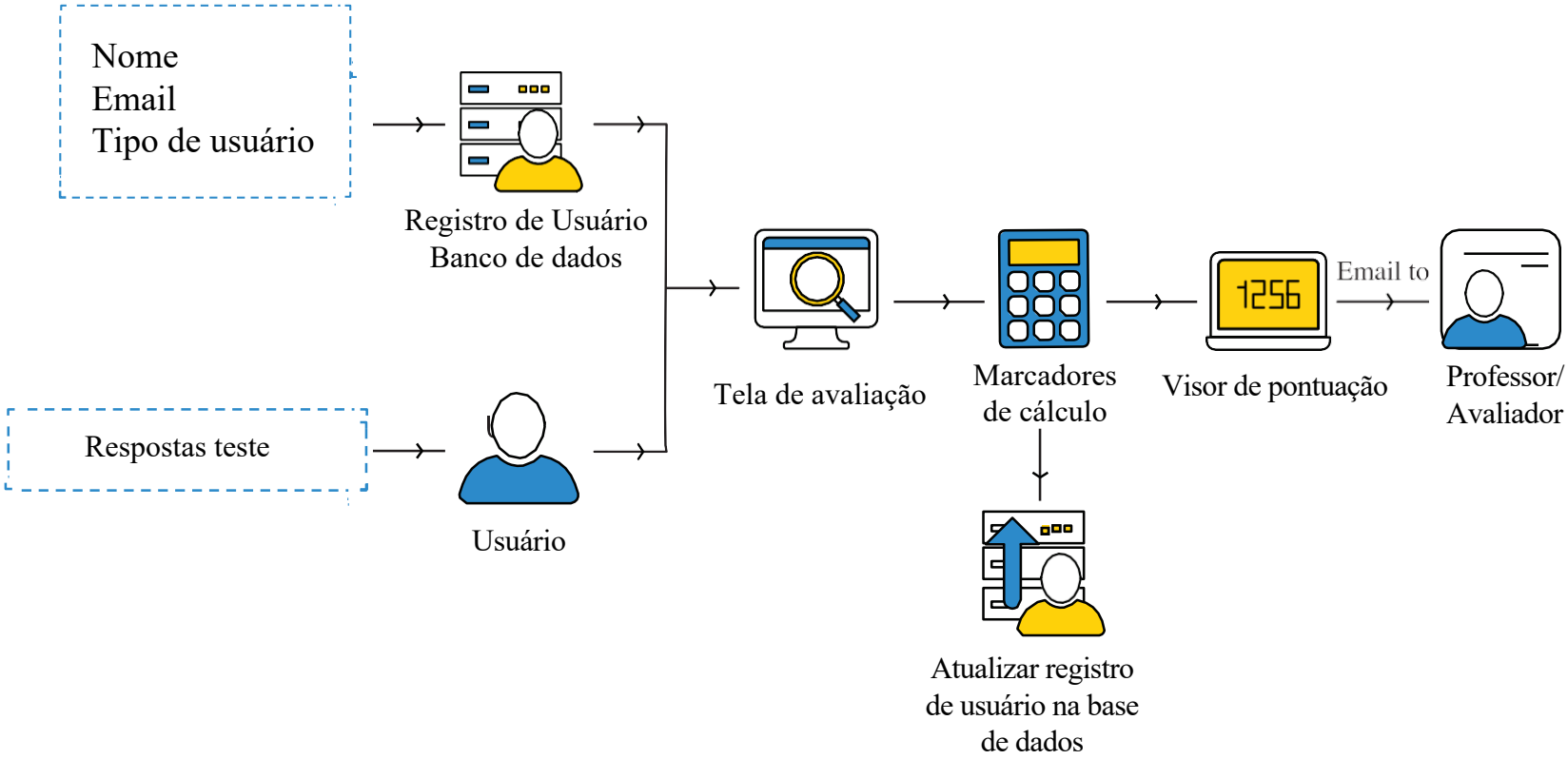
Os DFDs de processo são criados do ponto de vista das funções da sua empresa. É aqui que você é o controlador: você é o proprietário dos ativos de informações e pode decidir como eles são processados. O exemplo acima é típico para DFDs de processo.

Os DFDs de produto são criados do ponto de vista do seu produto. Aqui, os ativos de informações estão dentro do seu produto e pertencem a seus clientes e/ou usuários do produto. Você ainda pode encontrar esses ativos em seu *data center* ou em algum lugar que possa acessar, mas eles não pertencem a você.

Esse ponto se torna crítico quando você faz a análise de risco.

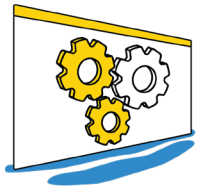
DFDs de produto

Se criarmos um DFD para a plataforma Think da Zylker, seria do universo da própria plataforma. Na verdade, cada recurso pode ter um DFD. O módulo de teste de Lisa Bingel terá o seguinte DFD:



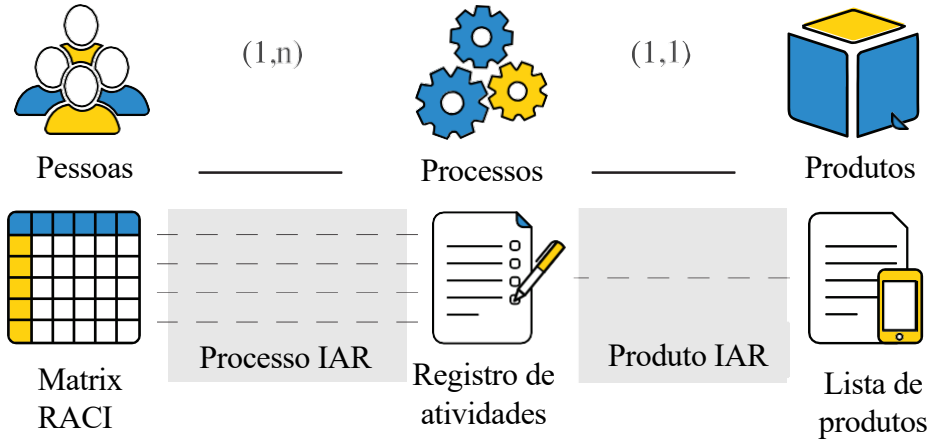
Cada recurso pelo qual uma pessoa é responsável deve ter um DFD. A coleta de todos esses DFDs será o do produto.

É preferível manter os IARs separados para seus processos e seus produtos.



Os IARs e a estrutura 3P

Em uma estrutura 3P, a entidade mais à direita é o produto. A lista de todas as instâncias desta entidade fornecerá a você a lista de produtos. A entidade no meio é o processo. Já enquadramos esta lista de atividades e, se você tiver seguido este guia, ela já vai estar mapeada para os colaboradores da sua organização.



Como resultado, agora você tem documentos que descreverão seu processo e seu produto. O desafio agora é manter esta documentação capturando quaisquer alterações.

Ativos de não informação

A maneira mais prática de lidar com esses ativos é a mesma de como você lida com ativos de informações: mapeá-los para a estrutura 3P.

Em algumas etapas simples, você pode obter a lista de todos os ativos em sua organização:

1. Os responsáveis principais na matriz RACI listam os ativos envolvidos nas atividades pelas quais são responsáveis. Eles podem fazer isso simplesmente adicionando uma coluna à matriz RACI.
2. Com a Ilustração 8 como referência, cada ativo é marcado.

Se você filtrar os elementos exclusivos da coluna Ativo, terá a lista de ativos de não informação.

A influência SPA

Quando os responsáveis por um processo precisam de ajuda, não há melhor time para oferecer assistência do que o time SPA. No entanto, o time deve oferecer mais do que apenas esclarecimentos sobre as dúvidas dos indivíduos responsáveis; deve também fornecer:

- Modelos para DFDs para diferentes tipos de atividades.
- Ferramentas para facilitar a criação do IAR.
- Um IAR abrangente para o time, para que todos possam usá-lo como exemplo. Acompanhamento e
- revisão constantes de IARs.

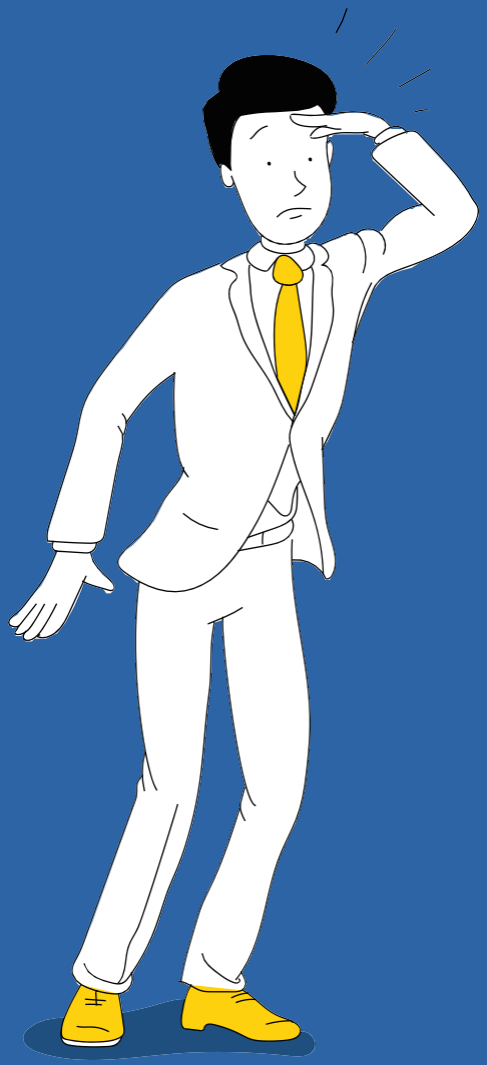
O IAR DA ZOHO

Com nosso processo distribuído por vários times operacionais e de produtos, um procedimento unificado para IARs foi uma ideia difícil de conceber. Cada time lida com diferentes ativos de dados de diferentes maneiras. Embora os DFDs sejam representações simples do ciclo de vida dos dados, eles podem ser interpretados de várias maneiras. Resolvemos esse problema com a técnica Dividir e Conquistar: Dividimos toda a jornada de criação do IAR em times de produtos, infraestrutura e operacionais e abordamos o IAR de cada perspectiva.

Por exemplo, o IAR de processo de um time de produto para desenvolvimento de software tecnicamente pode não envolver dados, porque eles apenas codificam. Portanto, a maioria de seus DFDs seria semelhante. No entanto, o IAR de seus produtos envolveria dados de clientes. Dentro do universo do produto, os desenvolvedores ainda lidam com os dados pessoais dos clientes, mesmo que eles pareçam nunca entrar em contato com os dados dos clientes. As operações, por outro lado, não têm tais complexidades. Por exemplo, recrutamento e integração são atividades que lidam diretamente com dados pessoais. Mas um pacote como o Zoho Finance lida com dados pessoais em todos os seus produtos.

Essas diferenças estão vinculadas à existência em qualquer organização. A chave para resolver esses problemas tem que vir do time SPA de uma organização. O SPA deve usar estas regras:

1. Categorizar as funções em operações e produtos, ou de qualquer forma lógica, dependendo de como elas funcionam e de quais os ativos por elas manejados.
2. Criar modelos personalizados para cada categoria.
3. Liderar pelo exemplo; pegar um time em cada categoria e criar um IAR para eles mesmos.



8 A PALAVRA "R" QUE IMPORTA

Você sabia?

Os eventos de risco podem afetar seus negócios em muitos níveis. As organizações que enfrentaram um evento de risco crítico observaram os impactos mais significativos em:

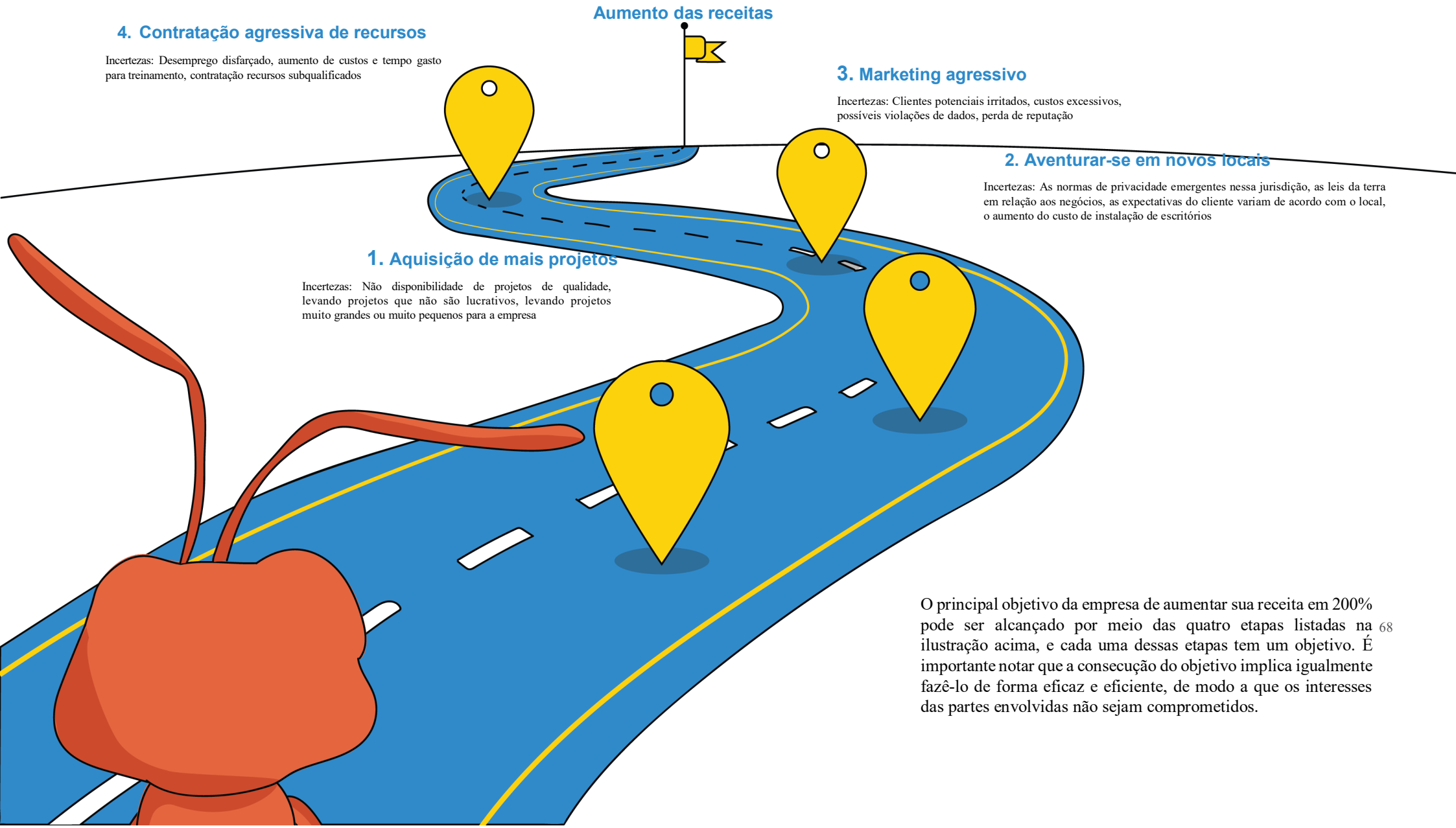
--> Produtividade do colaborador (62%)
--> Eficiência operacional (sistemas desestabilizados, processos, etc.) (59%)
--> Segurança do colaborador (29%)
--> Diferenciação competitiva (29%)
-> Marca e reputação (28%)

Risco

Tudo o que abordamos até agora, desde a responsabilidade até os IARs, leva-nos naturalmente à palavra "R" mais importante quando se trata de conformidade: risco. Existem vários padrões, métodos e modelos para realizar uma avaliação de riscos. Sugerir qual método ou estrutura você deve usar está fora do escopo deste livro. Mas colocaremos todos os elementos da análise de risco em prática para lhe dar clareza suficiente para começar com qualquer método que lhe seja mais adequado. O objetivo é tornar a análise de risco sustentável, prática e fácil para todos. Para isso, vamos começar com uma definição simples:

Risco é a incerteza de não atingir um objetivo.

Por exemplo, a Zylker quer aumentar sua receita em 200% em 2020.



O principal objetivo da empresa de aumentar sua receita em 200% pode ser alcançado por meio das quatro etapas listadas na ilustração acima, e cada uma dessas etapas tem um objetivo. É importante notar que a consecução do objetivo implica igualmente fazê-lo de forma eficaz e eficiente, de modo a que os interesses das partes envolvidas não sejam comprometidos.

Eis o que sabemos sobre cenários de risco:

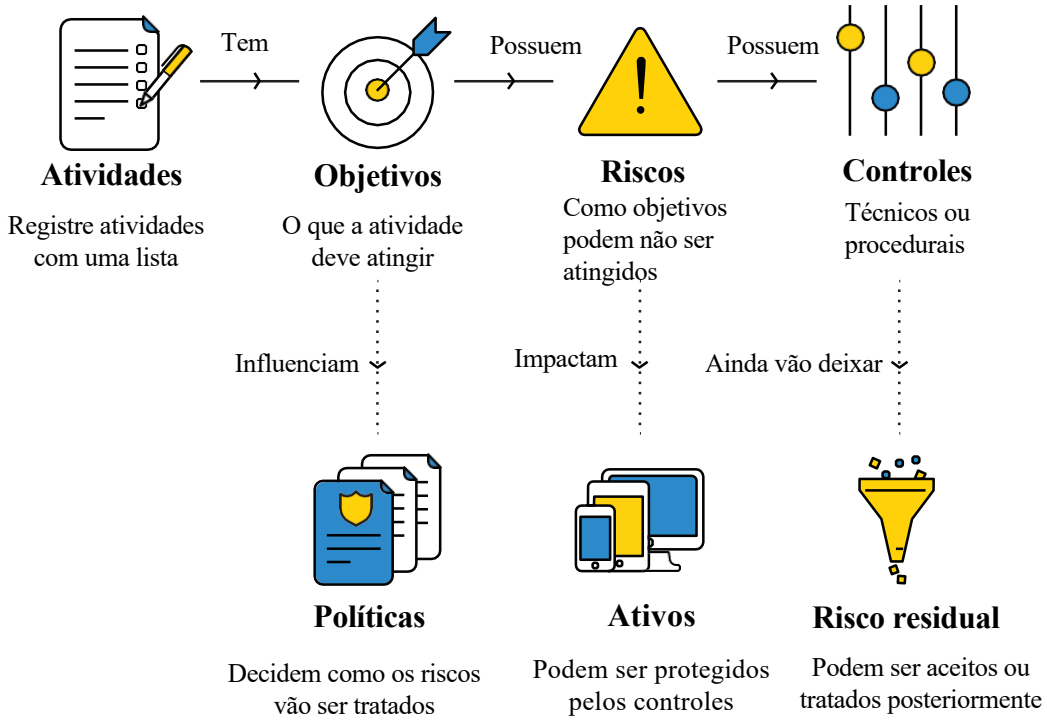
- O risco nunca pode ser eliminado, mas apenas minimizado. A pergunta é: quanto você precisa para minimizar o risco?
- O risco depende do seu objetivo.

Pergunte-se, *quais cenários nos faria não cumprir nosso objetivo?*

- Todas as respostas possíveis à pergunta acima são seus riscos e eles precisam ser controlados.
- Cada cenário de risco precisa de pelo menos um controle.
- Mesmo depois de aplicar o controle, haverá risco. É o risco residual, e é o seu pior cenário.
- Os cenários de risco sempre serão associados ao impacto. O impacto será direta ou indiretamente sobre o ativo associado à atividade.

Análise de risco na estrutura 3P

A única unidade exclusiva da estrutura 3P é uma atividade. A forma que o risco se origina de cada atividade é melhor representada por esta estrutura:



A ilustração acima mostra como cada atividade leva a riscos e determina controles. Os controles, em última análise, decidem como a sua organização faz para cumprir os padrões, pois estes geralmente têm um sistema de controles que você espera empregar. A análise de risco, com atividades como ponto de origem, garantirá que esses controles façam sentido para sua organização.

A declaração de aplicabilidade é a linguagem através da qual sua empresa e os auditores externos conversam. O sistema de controles que você derivou por meio da análise de risco desempenhará um papel importante na chegada à declaração de aplicabilidade.

Tornando a análise de risco escalonável: Riscos globais e locais

Claramente, quando há uma atividade, há um objetivo e haverá risco. Para uma organização com centenas de atividades, haverá ainda mais riscos. Com centenas de pessoas responsáveis pensando em ainda mais riscos, esse processo pode ser realmente escalável?

Ainda que a análise de risco seja altamente necessária, não é prático pressupor que cada responsável principal em sua organização fará isso de forma eficaz. Deve haver um sistema que possa ajudá-los.

Esse sistema deve ser construído para esclarecer a análise de riscos e fornecê-la prontamente para qualquer um que queira realizá-la. Um **registro de risco** centralizado com um sistema de codificação e categorização de riscos é um bom ponto de partida.

A influência SPA

Não há um time melhor do que o time SPA para criar um registro adequado para toda a organização. O time de SPA deve manter um registro de risco que capture:

Riscos globais: Riscos que afetam toda a organização.

Por exemplo, um desastre natural, como um terremoto, sabotaria todas as operações da Zylker. Da mesma forma, uma falha da parte do provedor de serviços de Internet pode fazer com que os servidores da Zylker sejam desligados indefinidamente. Esses tipos de riscos podem afetar a Zylker como um todo e se aplicam a todas aos times e indivíduos.

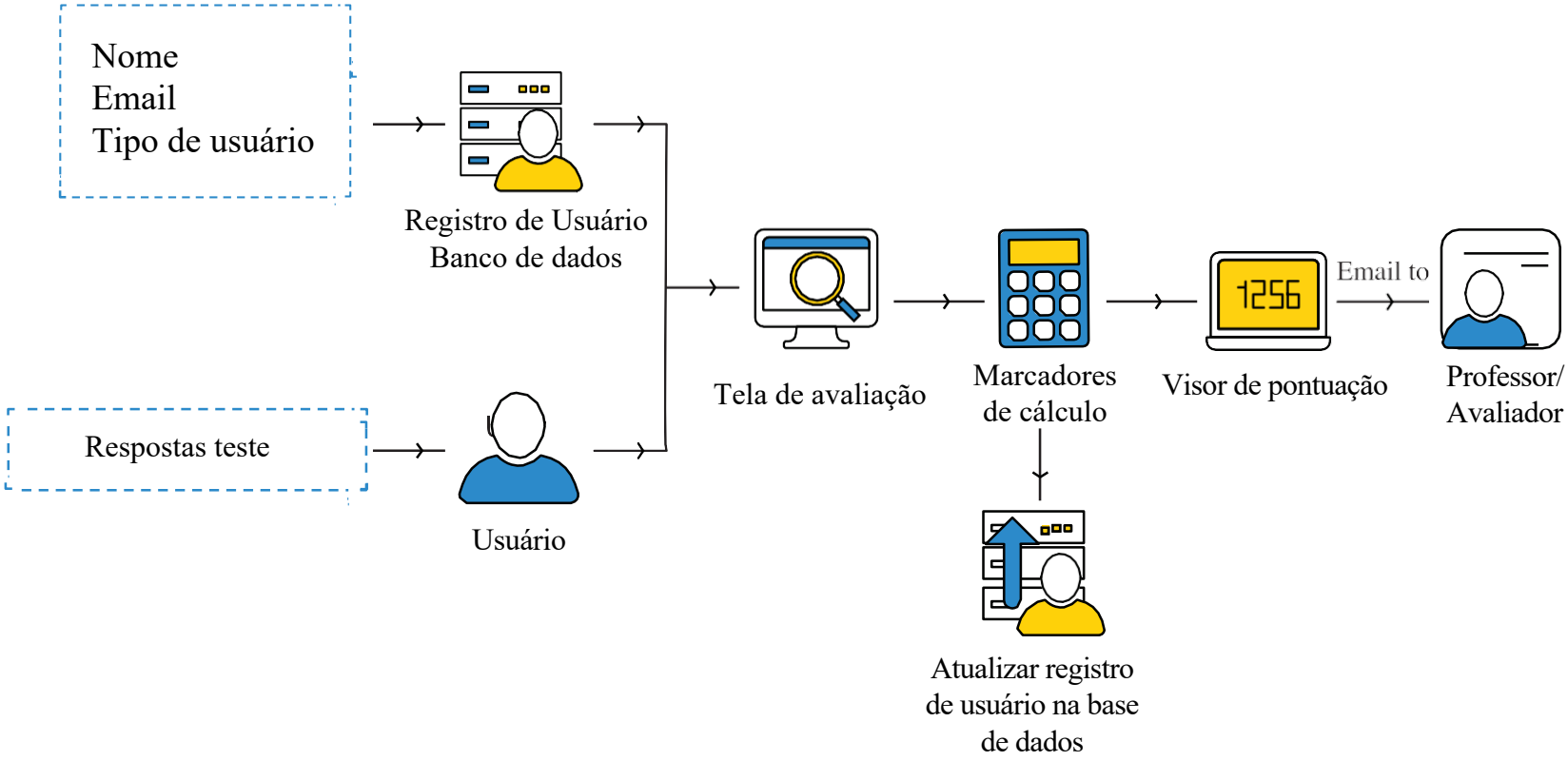
Quando Dwayne está realizando a análise de risco para a Zylker - pense, faz sentido que ele analise todos esses riscos globais? Na verdade, não. É por isso que o time SPA deve colaborar com outros times centrais e times de operações para formar uma lista abrangente de riscos e controles globais. Esses controles devem ser aplicados em todos os times.

Dwayne agora pode simplesmente consultar o registro de risco global do time de SPA e mencionar esses riscos. Ele pode se concentrar apenas nos riscos específicos da Zylker - Think, que são chamados de riscos locais.

Riscos locais: Riscos específicos às atividades e identificados pelos responsáveis principais.

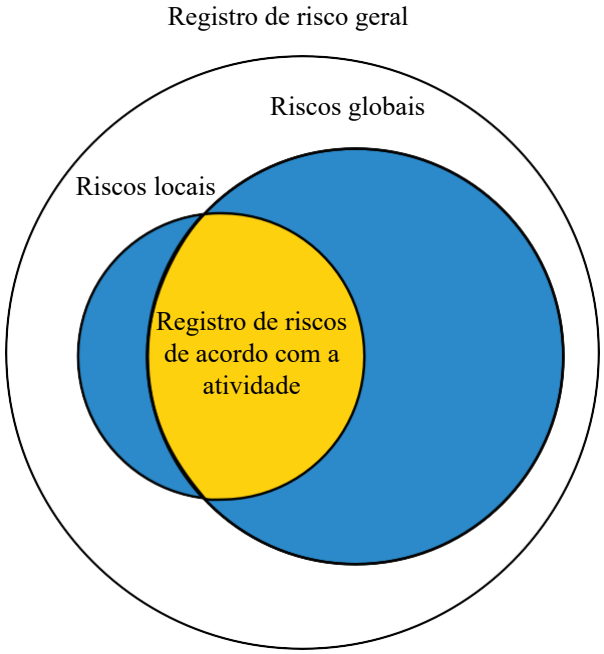
Uma boa maneira de abordar os riscos locais é através dos três princípios de segurança: confidencialidade, integridade e disponibilidade (a tríade CIA). Para analisar os riscos locais relacionados ao módulo de avaliação Zylker - Think, veja uma abordagem:

Nota: É preferível usar um DFD para análise de risco, pois ele serve como uma lista de verificação para todos os cenários que precisam ser considerados.



- Devido a um erro de programação, o registro de um usuário pode ser mapeado para o ID de outro usuário. Isso pode afetar as operações e a privacidade (confidencialidade). A Zylker mitiga isso fazendo com que o time de SPA crie uma lista de verificação (controle) que os desenvolvedores devem seguir.
- Um registro de usuário pode ficar indisponível (disponibilidade) ou danificado (integridade) devido a uma atualização de construção incorreta. A Zylker faz *backups* (controle) de seus dados de usuário para garantir que isso não afete o usuário.
- Se o método de avaliação ou os critérios de pontuação forem alterados, isso poderá levar a dados obsoletos, pois os resultados de dados antigos não serão mais relevantes (integridade). A Zylker migra dados antigos (controle) para evitar isso.

Se você puder ver como o fluxo de dados (DFDs) pode estar sujeito aos riscos do CIA, poucos riscos passarão desapercebidos.



ID do risco: Um sistema de codificação com IDs exclusivos para riscos facilitará para os responsáveis principais a identificação e inclusão de riscos que se aplicam às suas atividades.

Veja o que precisa ser feito:

- O time SPA cria um registro de risco, atribuindo um ID separado de risco e uma marca para identificar riscos como locais e globais.
- O time SPA colabora com vários times para identificar riscos globais.
- Cada responsável principal refere-se ao registro de risco e identifica os riscos globais aplicáveis às suas atividades.
- Cada responsável principal regista então os riscos locais aplicáveis apenas às suas atividades. Eles também receberão um ID de risco e serão marcados.
- O time SPA aprova os riscos locais após a realização de uma revisão.

Este registro permitirá que você filtre os riscos específicos de uma atividade, um conjunto de atividades, uma função de negócios ou um time. Isso torna a análise de risco um processo escalável.

Personalização da análise de risco para auditorias: Para fazer o melhor uso de sua avaliação de risco, você pode classificar os riscos ainda mais conforme a sua organização.

O time SPA da Zylker decide categorizar os riscos como sendo de negócios e de conformidade. Os riscos de negócios são os eventos que podem causar danos a aspectos da produtividade empresarial, receita e sentimento do cliente. Os riscos de conformidade são quando um risco específico falha no controle de um padrão. Essa diferenciação ajuda a Zylker durante as auditorias, pois a organização pode filtrar os riscos de conformidade e tratá-los separadamente.

Da mesma forma, a Zylker tem dois tipos de controles: controles locais e controles padrão. Os controles locais podem ser alterados para se adequar às operações da Zylker, enquanto os controles padrão são mapeados para padrões e não podem ser alterados sem a aprovação da gerência e da consulta com auditores externos.

Onde tudo começa: Políticas

Claramente, os riscos são derivados dos objetivos. Na Ilustração, se você montar a parte "Objetivo" de todas as atividades, terá a lista de coisas que sua empresa deseja alcançar.

Esta lista é a base das políticas.

Políticas são os valores que sua empresa representa.

Cada objetivo dessa lista é o que sua empresa deseja alcançar, e a lista ajuda a decidir o que sua empresa representa para atingir seus objetivos.

Vamos supor que a Zylker queira expandir seus negócios, e a alta gerência da organização percebe que os times de vendas e marketing precisam avançar para esse desafio. A organização lista o que espera que seus times de vendas e marketing façam:

- Todas as comunicações da Zylker com clientes em potencial e clientes atuais só serão feitas através de um dos seguintes canais: Site da Zylker, mídia social (Facebook, Twitter, blogs, LinkedIn), boletins, *webinars*, folhetos, brindes, reuniões anuais, conferências Zylker, *roadshows*, reuniões contratuais, e-mail e chamadas telefônicas.
- Todos os meios de comunicação externos – impressos, eletrônicos, verbais, etc. – devem ser baseados em uma das seis bases legais do GDPR. A base legal adequada deve ser registada no registro das atividades de processamento.
- Um dos membros da alta administração garantirá que o site da Zylker seja consistente em sua marca e mensagens. Todas as alterações necessárias para corresponder às tendências do setor devem ser discutidas e acomodadas.
- Quando apresentadas a clientes em potencial, as informações sobre os serviços da Zylker serão sempre verdadeiras. Os fatores relevantes suscetíveis de afetar as decisões das perspectivas serão comunicados de tal forma e num momento em que as perspectivas os possam ter em conta.
- O preço dos serviços está sujeito a alterações no que diz respeito às condições do mercado e deve ser feito com base nas diretrizes de preços da Zylker.
- As reuniões presenciais, incluindo as realizadas durante eventos e conferências, devem ser realizadas de maneira consciente e diligente, de modo que o nome da marca e a reputação da Zylker não sejam comprometidos.

Acima está uma lista não exaustiva do que cada colaborador deve saber ao realizar atividades de vendas e marketing para a Zylker. Da mesma forma, o desenvolvimento de produtos, a administração, os recursos humanos e outras funções de negócios podem ter suas próprias políticas, que são publicadas e compartilhadas com cada funcionário da empresa depois de aprovadas.

As atividades estarem ocorrendo de acordo com suas políticas é uma consideração crucial durante qualquer auditoria.

76

Você pode adotar duas abordagens quando quiser estruturar políticas:

De cima para baixo: A alta gerência decide sua postura em relação a várias funções, como vendas, produção e operações. Os objetivos das atividades serão decididos pelos responsáveis principais.

De baixo para cima: As políticas são derivadas da lista de objetivos. Os objetivos comuns são agrupados, e a política criada será uma representação de todos esses objetivos.

Cenários e controles de risco

O risco é como as coisas podem dar errado, e um controle é uma maneira de tentar minimizar a probabilidade (minimizar o impacto e/ou a probabilidade) de dar errado.

Como as coisas podem dar errado **- Cenários de risco**	Como você pode responder **- Controles**
• Atividades criminais por usuários autorizados • Ataques intencionais • Reorganização • Hackers • Funcionários desapontados • Erro de usuários • Desastres naturais • Dano físico • Mal uso de dados, recursos ou serviços • Mudanças em políticas da organização • Intrusões ou restrições governamentais, políticas ou militares • Erros de processamento • Erros procedurais • Abuse de privilégio pessoal • Picos ou perdas de energia • Falência ou interrupção da atividade de negócios • Intrusos • Mudanças de ambiente • Falhas de infraestrutura • Engenharia social	**Controles dissuasor** - Cercas para impedir invasões **Controles preventivos** - Sistemas de detecção de intrusão ou antivirus para impedir atividades indesejadas **Controles detectivos** - Cameras ou monitoramento de log para detectar atividade indesejada **Controles corretivos** - Reinicialização para modificar um ambiente para condições normais **Controles de recuperação** - Espelhar ou agrupar para voltar as condições originais

78

Mas se um controle é necessário ou não depende de como você responde ao risco. Você pode decidir não empregar um controle quando:

- O risco não causa nenhum dano a um ativo.
- É improvável que o risco ocorra.
- O impacto do risco é tão grande que qualquer controle que você possa implementar não o protegerá contra ele.
- O esforço necessário para proteger seus ativos contra o risco é desproporcional ao valor desses ativos para a empresa.
- As consequências do risco não afetarão seus objetivos de maneira substancial.
- Sua organização está disposta a aceitar as consequências.

A decisão de empregar controles deve ser tomada pelo responsável principal e deve ser periodicamente revisada pelo time SPA.

Avaliação do impacto à privacidade de dados (DPIA)

O Information Commissioner's Office (ICO) deu uma explicação elaborada para a execução de um DPIA, juntamente com um modelo que você pode usar imediatamente. No entanto, vamos analisar onde um DPIA se encaixa em sua estrutura geral de conformidade.

Um DPIA é uma ferramenta que o ajuda a identificar e atenuar riscos, mesmo antes de começar a processar dados pessoais, para que possa cumprir o artigo 25 do GDPR, que determina a proteção de dados por essência e definição. É semelhante à análise de risco, mas foca mais ainda nas leis de privacidade e proteção de dados.

O Artigo 35(3) do GDPR estabeleceu cenários em que o DPIA é obrigatório: definição de perfis, processamento de dados biométricos e genéticos, monitorização, negação de serviço, IA e aprendizagem automática, processamento invisível e marketing direto.

No entanto, do ponto de vista da conformidade, é seguro dizer que um DPIA é sempre aconselhável e é uma parte lógica do processo de ***gerenciamento de mudanças****.*

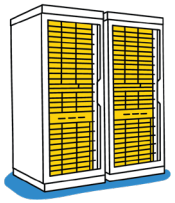
Aqui estão algumas alterações importantes que sua organização pode enfrentar:

- Apresentação de uma nova tecnologia, como *machine learning*, conduzindo novas operações
- Lançamento de novos recursos em produtos que exploram novas táticas de marketing
- Realização de negócios em uma nova área geográfica
- Parceria com uma nova empresa

Todas essas alterações acima envolvem uma modificação na forma como os dados pessoais são processados. Uma alteração como a liberação de um novo recurso pode não envolver diretamente dados pessoais, mas se você olhar mais de perto, verá que o próprio recurso pode ter contato com dados pessoais quando os clientes o usarem.

Portanto, é preferível seguir a primeira etapa para todas as alterações: Identificar a necessidade de um DPIA.

80



DPIAs e IARs

A conexão entre DPIAs e IARs é a conexão mais lógica entre um DPIA e a estrutura 3P, pois envolve diretamente o fluxo de dados pessoais.

Se a alteração tiver a ver com uma operação em sua empresa, um IAR de processo entra em cena. Se a alteração tiver que ser feita com um novo recurso ou produto, um IAR de produto será mais apropriado. De qualquer forma, seu IAR, que se concentra no fluxo de dados pessoais, é onde você pode iniciar seu DPIA.

Veja o exemplo da Ilustração 16. Tecnicamente, cada seta que indica um fluxo de dados e cada caixa que indica que um processo deve ser analisado quanto a riscos. Cada unidade do DFD pode ser interpretada a partir das seguintes perspectivas:

- **A finalidade do processamento:** Por que o sistema coleta os dados que coleta.
- **Armazenamento:** Onde os dados são armazenados (*data center*), quanto são protegidos no armazenamento, quanto tempo são armazenados e quem decide como e por quanto tempo devem ser armazenados.
- **Controle de acesso:** Quem tem acesso, como e por quem o acesso é monitorado e revisado, quanto acesso é fornecido a qual parte e em que base, e quanto acesso é necessário para processos como suporte e depuração.
- **Segurança:** A segurança dos dados em repouso e em trânsito, quais recursos são fornecidos, como o sistema pode ser abusado e mal utilizado e quais controles estão em vigor para evitar abuso e uso indevido.
- **Classificação dos dados:** Que nível de dados pessoais e confidenciais está envolvido, quais assuntos de dados estão envolvidos, quais são os riscos se esses dados forem comprometidos e como o sistema pode detectar e evitar comprometimento.
- **Backup e recuperação:** Como o sistema lida com perda ou dano de dados sem precedentes.
- **Conformidade regulamentar:** Quais direitos os titulares dos dados podem exercer sobre seus dados com base nas leis aplicáveis e como o sistema fornece tais direitos.

HISTÓRIA DA ZOHO

As avaliações de risco são atendidas por questões práticas que exigem paciência para resolver. Embora nosso time SPA tenha educado os times na avaliação de riscos, sempre havia dúvidas. Isso ocorre porque o risco é um conceito abstrato que pode ser interpretado de várias maneiras. É aqui que uma estrutura para orientar os times na realização de uma avaliação de risco é útil.

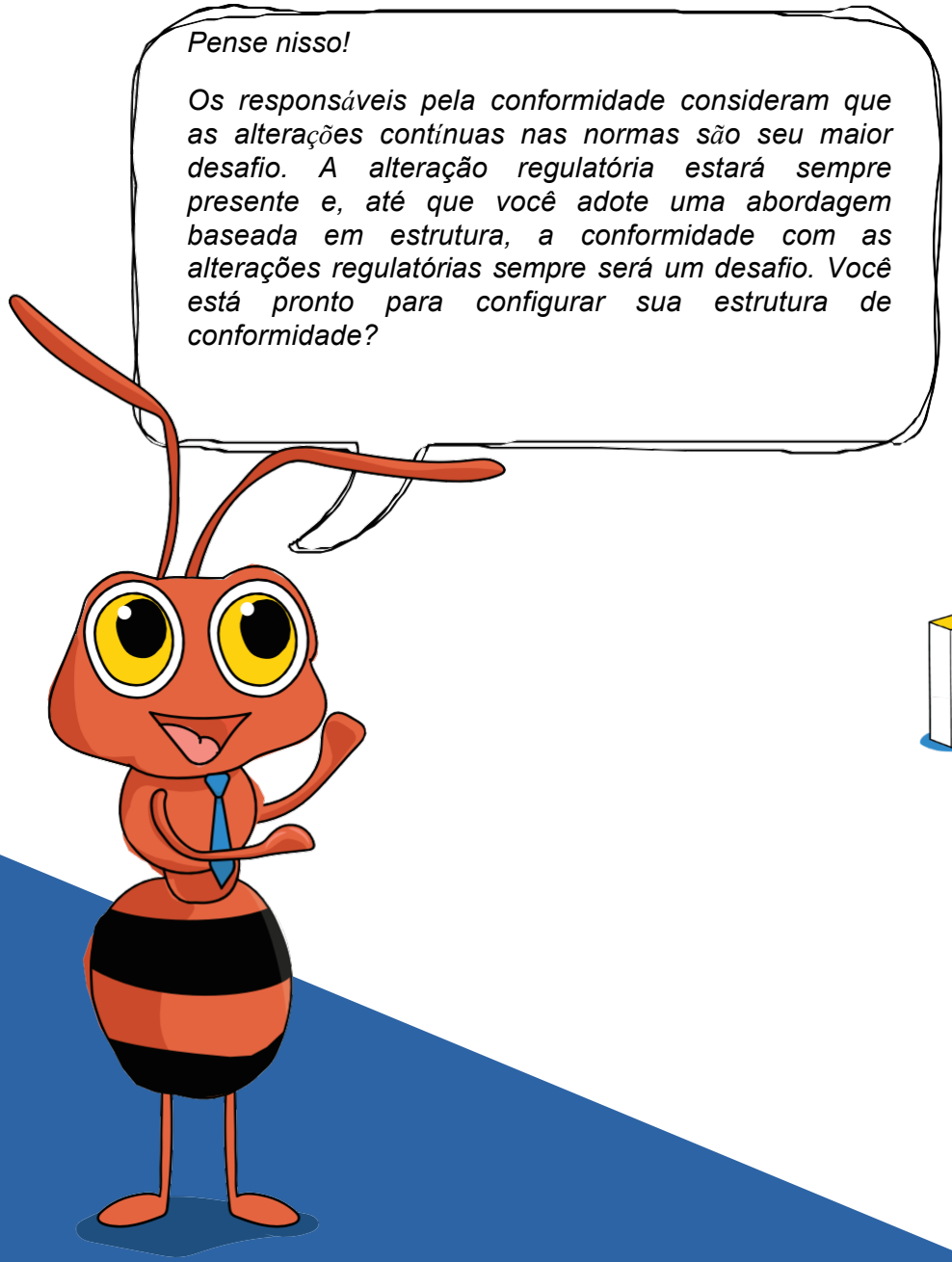
Por exemplo, um time de produto deve considerar os riscos principalmente relacionados ao seu produto. No entanto, eles também enfrentam riscos como uma queda de energia em massa, um servidor inteiro sendo hackeado ou um desastre natural. Embora todos esses riscos sejam importantes, não faz sentido que um time de produtos aloque seus recursos para lidar com esses riscos.

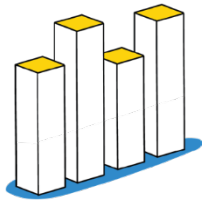
Inicialmente, tivemos muitos times que analisaram os riscos em excesso e incluíram todos os tipos de riscos de negócios generalizados. Embora isso não esteja errado, não foi útil para uma metodologia consistente de análise de riscos que possa ser mantida e dimensionada. Então, criamos um registro de risco onde os riscos gerais relativos à empresa foram listados. Os times de produtos agora usam nossa estrutura de conformidade para identificar os riscos de segurança, privacidade e regulamentação que realmente terão implicações em seus produtos.

Um DPIA é um aspecto crucial do nosso ciclo de vida de desenvolvimento de software (SDLC). Na verdade, um DPIA acontece mesmo antes do início do SDLC. O fluxo de trabalho do time de privacidade para o DPIA é onde ele começa e termina quando todos os riscos de proteção de dados são analisados. A chave para sustentar esse fluxo de trabalho para todos os times de produtos é usar modelos padronizados. Este modelo deve conter perguntas, referências e ponteiros para que o time de privacidade possa obter todos os dados necessários em uma única captura. Isso também reduz as discussões e diminui o tempo gasto para processar um DPIA.

82

9 E AGORA ESTAMOS EM CONFORMIDADE...





Até agora, discutimos vários instrumentos, métodos e abordagens que podem ajudar sua organização a estar mais em conformidade. No entanto, a forma ideal de alcançar a conformidade é através da normalização, que reunirá todos estes instrumentos de forma coerente, que pode ser utilizada por qualquer pessoa a qualquer momento, sem qualquer incerteza.

Padronize: Abordagem do funcionamento da empresa

Como o Zylker - Think, a empresa também oferece o Zylker - Health e o Zylker - Media, que criam plataformas para fins de saúde e criação de conteúdo, respectivamente. Essas plataformas têm a mesma estrutura que o Zylker - Think, com os times de desenvolvimento, marketing e suporte trabalhando juntos.

O mesmo conjunto de atividades é feito por vários times e todos eles se esforçam para manter a conformidade. No entanto, sempre haverá variações. Se o mesmo processo for repetido, não faz sentido que ele seja repetido de maneira consistente em todos os times?

Isso não só tornará a conformidade mais fácil, como também facilitará os processos para seus funcionários. Eles podem, com convicção, concentrar-se em realizar bem seus processos se souberem que estão fazendo o certo.

O mesmo conjunto de atividades repetidas em diferentes times pode ser agrupado em funções de negócios e padronizado para atingir um conjunto de atividades. O conjunto de atividades que os times realizam todos os dias agora será simplesmente outra instância dessas funções de negócios.

As funções comerciais típicas de qualquer organização incluem:

1. Gerenciamento de produtos
2. Engenharia/produção
3. Infraestrutura
4. Vendas e marketing
5. Governança, regulamentos e controle
6. Recursos humanos
7. Finanças
8. Pesquisa e desenvolvimento

Isso não é, de modo algum, o único método de definição de funções de negócios. Dependendo da natureza da sua organização, você pode ter mais:

- Uma empresa de software pode optar por dividir a infraestrutura em funções comerciais separadas, como operações de TI e de rede.
- Uma empresa automotiva pode optar por dividir a produção em fabricação e montagem.
- Uma empresa de mídia pode optar por lidar com relações públicas e sentimentos como uma função de negócios separada.
- Uma organização de saúde pode optar por ter governança e consultoria jurídica como funções de negócios separadas.

No entanto, o conceito de padronização permanece o mesmo:

Agrupar atividades semelhantes, padronizá-las e tornar cada processo de sua empresa uma instância desse padrão.

A Zylker decide tornar o desenvolvimento uma função de negócios com o seguinte conjunto de atividades padrão:

1. Entender os requisitos de recursos dos times de gerenciamento e vendas de produtos
2. Definir componentes de software e hardware, e interfaces entre eles, com base em:
    a. Requisitos da plataforma
    b. Segurança: Integridade, confidencialidade e disponibilidade
    c. Privacidade: Limitação de finalidade, minimização de dados e limitação de armazenamento
3. Compreensão dos riscos de componentes e interfaces, incluindo os de serviços e bibliotecas de software de terceiros, e implementar controles apropriados (modelagem de ameaças)
4. Definição de entidades e relacionamentos e criação de um diagrama de relacionamento de entidade (ER)
5. Definição de tabelas e relacionamentos em um dicionário de dados
6. Definição do fluxo de dados entre os componentes (IAR do produto)
7. Codificação com a utilização do ambiente de desenvolvimento
    a. Compreensão das vulnerabilidades e aplicação dos controles apropriados
    b. Check-in do código no repositório
        i. Compreensão e correção de avisos e erros de check-in
8. Análise do código em relação aos requisitos funcionais e não funcionais
9. Definição de casos de teste (teste de unidade)
    a. Teste de funcionalidades
    b. Teste de casos de uso indevido e abuso
    c. Teste do desempenho e teste de escalabilidade
10. Análise da cobertura do caso de teste e validação das funcionalidades (QA)

11. Implantação da compilação na preparação local
    a. Solicitação e obtenção das máquinas dos times de infraestrutura
    b. Registro do produto em local pré-definido
    c. Arquitetura de implantação
    d. Realização de migrações de dados, se necessário
    e. Realização de testes de integração
    f. Obtenção de validação de QA e confirmação de que nenhuma funcionalidade existente foi comprometida
12. Correção das ameaças de segurança e de código e resolução das vulnerabilidades de registro, validação de dados, gerenciamento de sessão e criptografia
13. Arquitetura de implantação
    a. Solicitação e obtenção das máquinas dos times de infraestrutura
    b. Modificação das configurações de acordo com o ambiente de produção
    c. Realização de migrações de dados, se necessário
    d. Implantação da configuração de pré-produção
        i. Teste das funcionalidades principais
    e. Implantação da compilação na produção
    f. Realização de testes de integração
    g. Obtenção de validação de QA e confirmação de que nenhuma funcionalidade existente foi comprometida
14. Informação dos times de suporte, vendas e marketing, bem como outras partes interessadas
15. Monitoramento e melhoria dos recursos do produto com base no uso, no desempenho e nos erros, e geração de solicitações de alteração

Todos os três times da Zylker – Think, Health e Media – seguirão o mesmo conjunto de atividades para desenvolvimento, mas com diferentes instâncias. Cada instância de atividade padrão (no Health e no Media) terá seu próprio RACI. Cada atividade padrão será apoiada por uma estrutura robusta que fornece o impulso necessário para a conformidade.

Atividades padrão em funções de negócios, repetidas em toda a empresa como instâncias, levarão à conformidade.

Orientação e avaliação

A maior vantagem da padronização é a facilidade com a qual a orientação pode acontecer mais tarde. Quando todas as instâncias de uma atividade adotam um procedimento unificado e seguem um sistema consistente de métricas para avaliação, fica mais fácil para o time SPA facilitar a jornada de conformidade da empresa.

A orientação e a avaliação serão baseadas em uma pergunta:

Onde a árvore de atividades interrompe a ramificação?

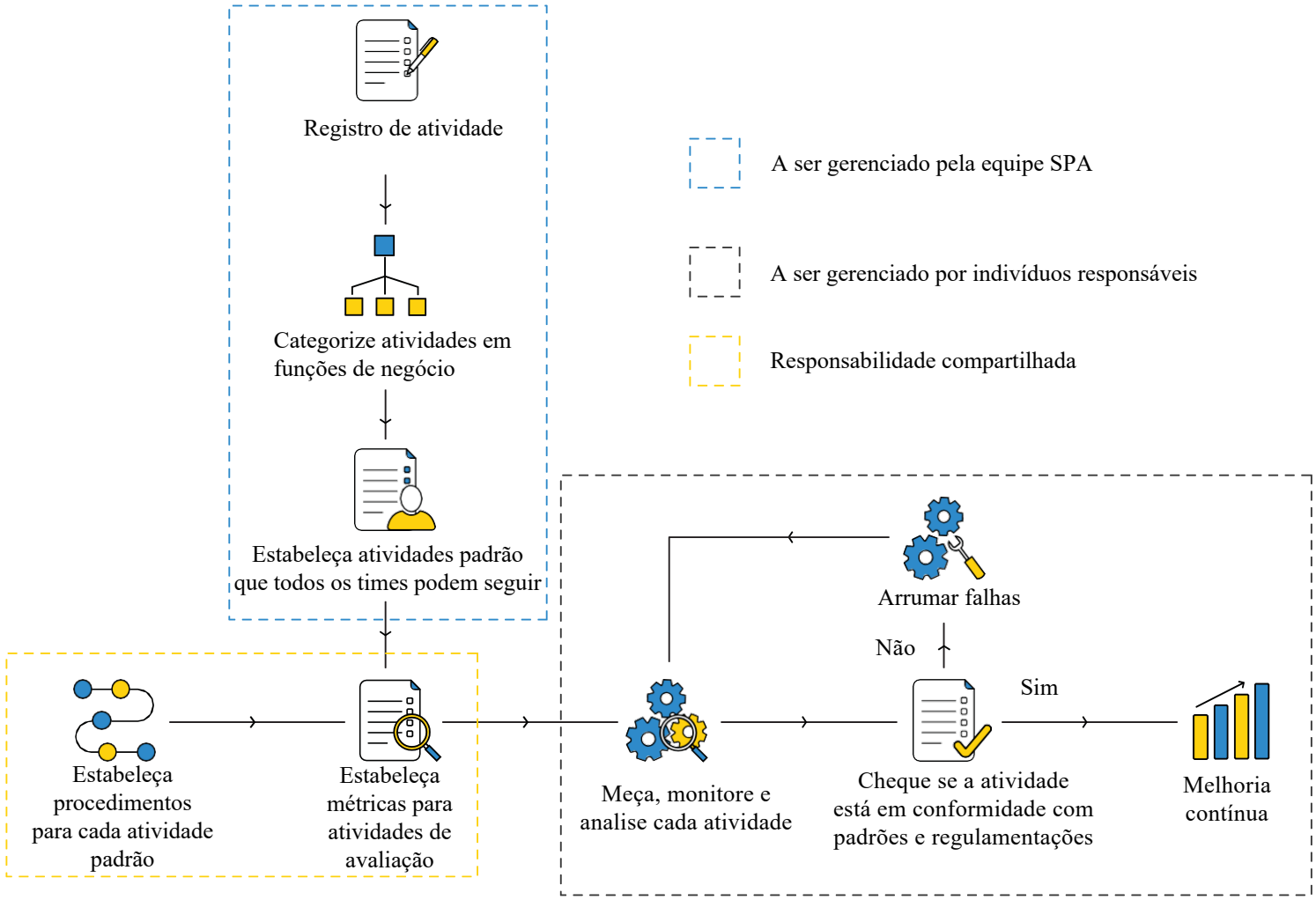
Em outras palavras, para as atividades que não podem ser divididas em subatividades, deve haver um **procedimento** para orientar a atividade e um sistema de indicadores para **avaliar** as atividades.

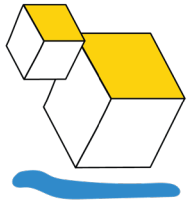
Um procedimento deve conter:

- Controles de revisão, aprovação e revisão.
- Uma sequência de etapas a serem seguidas, descrita em linguagem simples para que qualquer pessoa possa entender.
- Funções e responsabilidades para essas etapas, uma vez que o RACI não pode ir além dessa atividade.
- Pré-requisitos, como documentos ou listas de verificação.
- Exceções que podem ocorrer e instruções sobre como lidar com elas. Capturas de tela para simplificar a compreensão.
- Referências e links relevantes.

Indicadores para monitoramento e medição devem ser baseados em:

- O que será verificado para garantir que o processo seja seguido?
- Quais parâmetros serão considerados para garantir que o progresso constante seja visto a partir do procedimento que está sendo seguido?





Uma estrutura para você

A estrutura 3P oferece uma visão de alto nível da conformidade. Ainda é a melhor e mais prática maneira de criar sua própria estrutura de conformidade. Entretanto, para fazer sentido de todos os instrumentos e ideias falados neste livro, você pode precisar de uma estrutura mais elaborada.

Uma estrutura, para todas as suas variadas definições eloquentes, é simplesmente uma tabela glorificada. Aderindo a esta versão simplista, considere o diagrama abaixo, onde cada bloco é uma coluna, e cada linha será uma atividade (preferencialmente, uma atividade padronizada).

Atividades / Sub atividades	Objetivos	Entregáveis	RACI	Ativos envolvidos	IAR	Riscos	Controles	Declaração de política	Procedimentos	Métricas	Código de padrão de controle aplicável	Regulação aplicável, código da seção

Usando a estrutura

Cada produto que sua empresa cria, todos os serviços que fornece, e cada operação que ela realiza será uma instância dessa estrutura. Essa estrutura garante que cada projeto que sua organização empreende esteja em conformidade, pois uma estrutura em conformidade conduz as atividades nesse projeto.

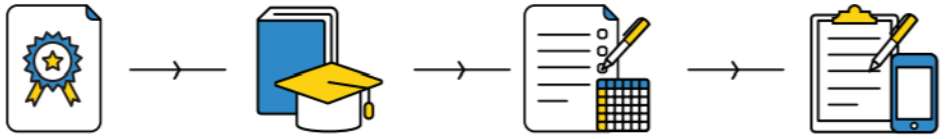
Essa estrutura também formará a base de seus principais requisitos de conformidade. Veja como você pode usar essa estrutura:

- Uma lista de atividades consolidadas vai te ajudar a enquadrar os registros de atividades de processamento de sua organização, que é um requisito crucial do GDPR.
- Uma lista de materiais de entrega o ajudará a formar o registro do produto. Isso vai te ajudar durante as auditorias ISO, nas quais você pode consolidar e preparar evidências com base no produto que está sendo auditado.
- O mapeamento do seu ativo com a matriz RACI ajudará você no gerenciamento e na propriedade de ativos.
- O mapeamento de produtos finais com o IAR formará uma parte crucial de seus documentos de processo durante qualquer auditoria.
- Um mapa de risco vs. controle formará seu registro de risco. Isso também pode ajudá-lo a tratar os riscos de acordo com seu peso com base em qualquer padrão (por exemplo, NIST).
- Uma lista de padrões e códigos de controle aplicáveis ajudará você a formar a declaração de aplicabilidade necessária para qualquer auditoria.
- Uma lista de declarações de política vai te ajudar a criar políticas para sua empresa e publicá-las no seu portal.

E isso é apenas um uso limitado para a estrutura. Com base na natureza de sua organização, essa estrutura pode ser usada de várias maneiras benéficas.

Escopo: *Essa estrutura também pode ser aplicada a qualquer organização, não-TI, de uma empresa de marketing digital a uma empresa de fabricação que produz caixas de câmbio para automóveis. Os conceitos de responsabilidade, gerenciamento de ativos, avaliação de riscos e uma abordagem baseada em estrutura permanecerão os mesmos.*

Revisão



Por que conformidade?
Crie um time SPA, com geração de conscientização

Educação
Eduque-se com marketing sutil

Registro de atividades com RACI
Forme uma lista de atividades de propriedade alocada

IAR
DFDs de produto e processo

A ser realizado pelo time SPA

A ser realizado pelos outros times

Avaliação de riscos
Riscos globais e locais

1.Funções de negócios
2. Procedimento e indicadores
3.Estrutura

Controles e regulamentos mapeados com atividades

Conclusão – mas é verdade?

A conformidade não é o que você faz, mas como você faz. É a maneira mais confiável de afirmar que suas ações em relação às suas metas estão funcionando. Sem essa afirmação, a eficácia e a eficiência de seus processos podem muito bem ser consideradas fantasia.

Você pode perguntar: "Se eu criar essa estrutura e mantê-la, estou em conformidade para sempre?"

A resposta é um sonoro “Não”! No entanto, essa estrutura garantirá que você esteja na posição perfeita para tornar-se compatível com qualquer regulamento ou padrão. Esses métodos, ao mesmo tempo em que ajudam você a melhorar seu processo, criarão uma plataforma que garantirá que a conformidade com qualquer coisa nunca mais será um fardo em sua organização.

HISTÓRIA DA ZOHO

Criar uma estrutura para a conformidade é como aprender a aprender. A conformidade nunca poderá ser considerada como alcançada, pois há sempre novos desafios à medida que os negócios crescem. Um novo ramo em que se investir, um novo país para iniciar negócios, e uma nova certificação para aumentar a confiança dos clientes estarão sempre lá. Mas o aspecto crucial desta jornada é que sabemos que podemos cumprir qualquer coisa porque nossos processos são orientados dessa forma, pois a conformidade é apenas um subproduto do controle de processos bem definido. Qualquer empresa que se concentre em seus processos navegará pelos requisitos de conformidade e é isso que fazemos aqui na Zoho.

94