Protegendo seus dados

Nossa abordagem para proteção de dados e segurança da informação

Building a better working world

A EY acredita que uma reputação comercial sólida depende de um programa robusto de proteção de dados e segurança da informação.

Nós vemos a proteção de dados e a segurança da informação como componentes fundamentais para fazer negócios. Temos o compromisso de proteger os ativos da informação, dados pessoais e informações do cliente. Acreditamos que programas sólidos de proteção de dados e segurança da informação são os componentes essenciais nas melhores organizações de serviços profissionais. O objetivo deste documento é apresentar um resumo de nossa abordagem para proteção de dados e segurança da informação. Traz uma visão geral de como protegemos as informações do cliente e de nossos sistemas de informação que servem de suporte. As particularidades dessas medidas podem variar dependendo dos serviços executados e dos requisitos regulamentares aplicáveis do país. Nossos programas e práticas de proteção de dados e segurança da informação se concentram no compartilhamento de informações de maneira apropriada e legal, enquanto preservam a confidencialidade, integridade e disponibilidade.

Uma estratégia de segurança e proteção de dados bem articulada

A capacidade da equipe EY de prestar ao cliente um serviço contínuo, consistente e de alta qualidade em todo o mundo é apoiada por uma estratégia bem articulada de proteção de dados e segurança da informação. Protegemos ativos da informação, dados pessoais e informações de clientes sempre e onde quer que sejam criados, tratados, transmitidos ou armazenados. Mantemos uma governança efetiva e conformidade contínua com as normas regulatórias nacionais e internacionais aplicáveis.

A implementação de nossos programas e práticas de proteção de dados e segurança da informação é gerenciada por dois grupos distintos, porém alinhados: a rede de Proteção de Dados Globais (*Global Data Protection*) e a organização de Segurança da Informação Global (*Global Information Security*). Sua missão é proteger os ativos da informação de nossa organização e de clientes da EY contra coleta, retenção, uso, divulgação, modificação ou destruição não autorizados. Isso se dá por meio de políticas, normas, procedimentos, diretrizes, controles tecnológicos e administrativos apropriados e esforços contínuos de treinamento e conscientização.

As equipes de Proteção de Dados Globais da EY e a organização de Segurança da Informação Global estão alinhadas em relação à prioridades globais implementadas em todo o mundo dentro da organização da EY. Isso fornece uma visão única e coesa em torno da proteção de nossos ativos da informação, dados pessoais e informações de clientes.

Nossa estrutura de proteção de dados

Nossa estrutura de proteção de dados baseia-se nos princípios do Regulamento Geral de Proteção de Dados da União Europeia (EU) (GDPR). Aborda os problemas levantados por ferramentas e sistemas modernos de gerenciamento de dados. Aplicamos um conjunto comum de princípios de gerenciamento de dados pessoais a todas as firmas-membro da EY, fornecendo uma estrutura para o tratamento de dados pessoais em conformidade com o GDPR, leis de privacidade locais e normas profissionais, bem como suas próprias políticas internas. Nossa estrutura de proteção de dados tem como base os seguintes princípios:

- Protegemos os dados pessoais usando medidas de segurança físicas, técnicas e organizacionais apropriadas. Essas medidas de segurança são desenvolvidas para facilitar a conformidade com os requisitos de proteção de dados por *design* e por padrão.
- Tratamos, armazenamos e divulgamos dados pessoais apenas para fins comerciais legítimos.
- Nossos contratos com operadores terceirizados contêm termos que confirmam que os dados são gerenciados de acordo com os mesmos padrões que implementamos em toda a empresa.
- Damos atenção e cuidado adicionais a dados pessoais sensíveis.
- Identificamos as medidas adequadas para manter os dados pessoais precisos, completos, atuais, adequados e confiáveis.
- Apenas retemos os dados pessoais de uma forma que permita a identificação pelo tempo que for necessário.
- Quando for o caso, notificamos os indivíduos com os quais as firmas-membro da EY se envolvem, informando-os sobre a finalidade para a qual tratamos seus dados pessoais.
- Mantemos um registro das atividades de tratamento realizadas. As atividades de tratamento que possam resultar em um risco elevado para os direitos e liberdades das pessoas naturais serão objeto de uma avaliação do impacto na proteção de dados.

Elementos de nossa estrutura de proteção de dados

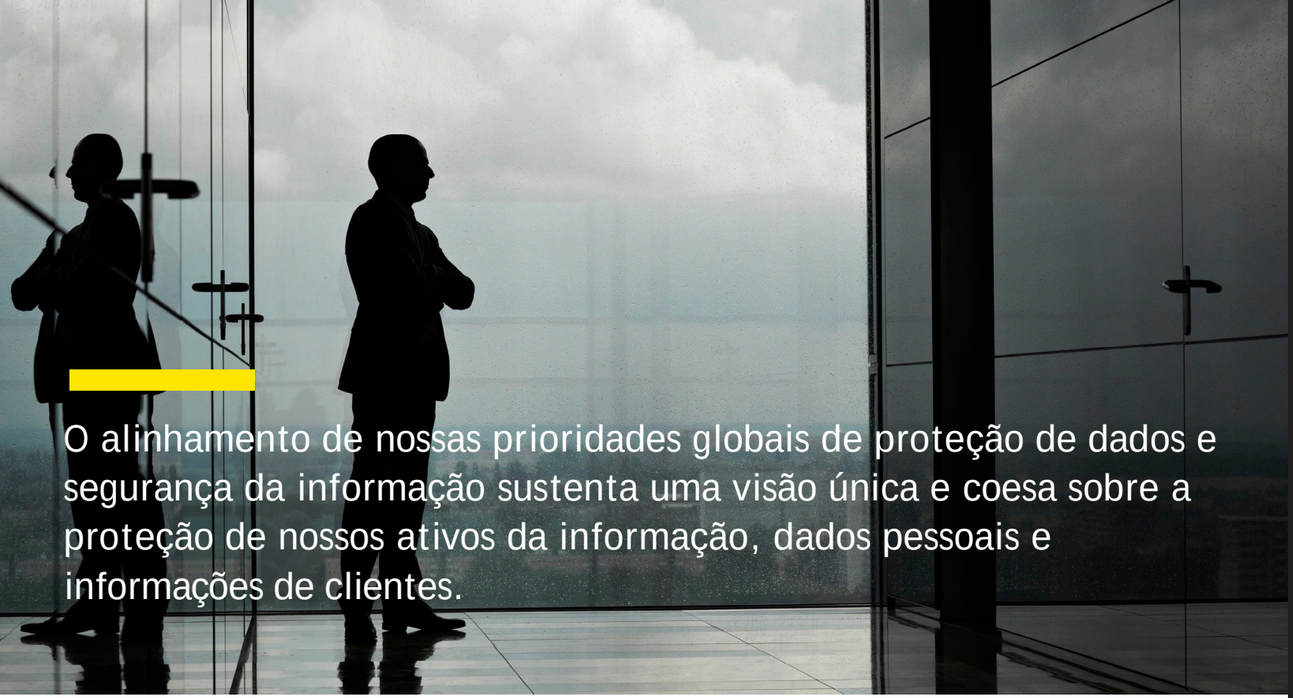
Transferências internacionais de dados

A transferência internacional de dados pessoais é estritamente regulamentada pelo GDPR. Os países fora do Espaço Econômico Europeu (EEE) sem uma abordagem legislativa abrangente em relação à proteção de dados não são considerados pela UE como países que oferecem um nível adequado de proteção para os direitos de privacidade de dados dos indivíduos. O GDPR, portanto, proíbe a transferência de dados pessoais para esses países, a menos que a organização que transfere as informações tenha implementado as garantias jurídicas apropriadas.

Nossas equipes estabeleceram Normas Corporativas Globais (*Binding Corporate Rules* - BCRs) para atividades realizadas por controladores e operadores de dados pessoais como um mecanismo para permitir a transferência internacional de dados pessoais entre as firmas-membro da EY. As BCRs nos permitem transferir dados pessoais sem problemas entre as firmas-membro da EY, facilitando a formação de equipes entre linhas de serviço. Embora as obrigações legais em relação ao GDPR se apliquem apenas aos dados pessoais usados e coletados na UE, aplicamos essas BCRs em todo o mundo. Nossas BCRs encontram-se em ey.com/bcr.

Nossas equipes também utilizam Cláusulas Contratuais Padrão aprovadas pela UE em contratos com clientes e terceiros, quando apropriado.

Além disso, a firma-membro da EY nos EUA é certificada para a UE-EUA e Suíça-EUA Privacy Shield Frameworks. O Tribunal de Justiça da União Europeia (TJUE) invalidou a EU-US Privacy Shield framework como mecanismo de transferência de dados pessoais do EEE para os EUA. Além disso, o Comissário Federal de Proteção de Dados e Informações da Suíça concluiu, em um documento, que a Suíça-US Privacy Shield não fornece mais um nível adequado de proteção para a transferência de dados pessoais da Suíça para os EUA. No entanto, a firma-membro dos EUA está comprometida em cumprir os princípios da Privacy Shield framework, embora não dependa deles para legitimar as transferências de dados pessoais.



O alinhamento de nossas prioridades globais de proteção de dados e segurança da informação sustenta uma visão única e coesa sobre a proteção de nossos ativos da informação, dados pessoais e informações de clientes.

Treinamento e programas de conscientização

À medida que os métodos de ataque mudam, as informações, orientações e treinamentos que oferecemos aos empregados da EY também devem mudar. A conscientização sobre ameaças à privacidade de dados e à segurança da informação é um processo contínuo e dinâmico. É algo que levamos muito a sério e que se reflete não apenas em treinamentos obrigatórios atualizados regularmente para os profissionais de cada uma das linhas de serviço da EY, mas em inúmeras outras atividades realizadas para conscientizar toda a população global da EY.

Política Global de Segurança da Informação da EY

Nossa Política de Segurança da Informação e suas normas e controles de apoio são continuamente examinados pela alta administração para confirmar se o material continua oportuno e preciso e se ele se correlaciona com os requisitos legais e regulatórios aplicáveis a nós. As declarações de política obrigatórias e recomendadas abrangem quase uma dúzia de áreas de segurança da informação amplamente reconhecidas, incluindo, entre outras:

- Controle de acesso
- Gestão de ativos: classificação e controle
- Segurança de comunicações e operações
- Segurança de recursos humanos: pessoal
- Aquisição, desenvolvimento e manutenção de sistemas de informação
- Segurança física e ambiental
- Avaliação de risco

Controles técnicos de segurança

Nossa abordagem à segurança da informação não depende somente de uma política ou normas de segurança por escrito. Também mantemos a confidencialidade, a integridade e a disponibilidade das informações por meio da proteção de nossos recursos e ativos tecnológicos. As medidas incluem, entre outras:

- Criptografia de disco completo de desktop e laptop
- Ferramentas de criptografia de mídia removível
- Firewalls de desktop e laptop
- Software antivírus e antimalware
- Abordagens de autenticação multifator
- Patches automatizados e avaliações de vulnerabilidades de segurança
- Fortes controles físicos, ambientais, de rede e de perímetro
- Tecnologias de detecção e prevenção de intrusão
- Sistemas de monitoramento e detecção

Além disso, investimos tempo e recursos consideráveis em futuras tecnologias de segurança do estado. Alinhamos nossa estratégia de segurança da informação ao nosso roteiro de produtos de tecnologia e mantemos uma estreita associação com nossas ofertas de serviços de tecnologia. Com disso, conseguimos abordar questões de segurança que possam ameaçar a confidencialidade, a integridade ou a disponibilidade de nossos recursos de tecnologia.

Nossas equipes oferecem ferramentas desenvolvidas para nos ajudar a colaborar com os clientes da EY, além de transferir e armazenar dados de forma segura e confiável.

Código de conduta global

Mantemos nossos profissionais de acordo com as normas profissionais e técnicas aplicáveis e exigimos adesão ao Código de Conduta Global da EY.
Esses princípios estão disponíveis publicamente para visualização no site global da EY (https://www.ey.com/pt_br/global-code-of-conduct) e representam normas vinculantes que se aplicam a todas as firmas-membro globalmente. O Código de Conduta Global da EY baseia-se em uma estrutura comportamental e ética abrangente. Ele orienta as decisões diárias tomadas por todos os colaboradores da EY, independentemente de sua função individual, cargo ou firma-membro. Exige que os profissionais respeitem e protejam as informações pessoais e confidenciais obtidas ou relacionadas à organização EY, pessoas da EY, clientes da EY ou terceiros.

Proteção de dados

Continuidade de negócios e recuperação de desastres

Nosso compromisso contínuo com a proteção dos dados da organização e do cliente é demonstrado por meio de nossos recursos de recuperação de desastres e continuidade de negócios. Estamos comprometidos com a proteção das pessoas, instalações, infraestrutura, processos de negócios, aplicativos e dados da EY antes, durante e após um evento catastrófico. Os procedimentos de resposta a desastres e recuperação do sistema para nossos aplicativos de serviços críticos foram cuidadosamente planejados e testados. Nossas metodologias de recuperação de desastres e continuidade de negócios incluem o seguinte:

- Avaliações de impacto nos negócios
- Planos de recuperação de desastres de missão crítica baseados nas principais normas do setor
- Apoio de profissionais de planejamento certificados em recuperação de desastres e continuidade de negócios
- Testes regulares de planos de recuperação de desastres e continuidade de negócios para verificar a prontidão operacional

Programa de garantia de risco (*risk assurance*) do fornecedor

Nosso programa de garantia de risco de fornecedores está alinhado com nossos processos de *due diligence* de gestão de fornecedores a fim de abranger atividades de terceiros relacionadas à segurança da informação, compras, contratos, proteção de dados e independência, incluindo:

- Avaliação de fornecedores em potencial para conformidade com nossas políticas e controles globais alinhados à ISO 27001/2
- Revisões de *due diligence*, incluindo a preparação de classificações e identificação de riscos
- Mitigação dos riscos identificados
- Apoio na seleção de fornecedores e negociações de contratos

Usamos avaliações de segurança padrão do setor para avaliar riscos inerentes e residuais em segurança da informação, conformidade e outras categorias de risco, como classificação de dados, localização de dados, acesso e tipo de transmissão de dados.

Estratégia e *mindset* de segurança

Nosso programa de segurança multifacetado tem como base nossas políticas globais de segurança da informação e conduta pessoal. Foi desenvolvido com o intuito impulsionar e promover a confidencialidade, a integridade e a disponibilidade de nossos ativos da informação pessoais e de clientes. Esses esforços encontram apoio nas tecnologias de proteção de dados aplicadas de acordo com as leis de privacidade e requisitos regulatórios aplicáveis, bem como com os padrões ISO 27001/2 internacionalmente aceitos para gerenciamento de programas de segurança.

Nossa organização é proativa em proteger e gerenciar adequadamente informações confidenciais e pessoais por meio de nosso programa de segurança da informação baseado na ISO 27001/2, que inclui:

- Políticas, padrões, diretrizes e gerenciamento de programas apropriados
- Fortes controles técnicos de segurança
- Um programa de conformidade de segurança envolvendo revisões de segurança, certificações e auditorias
- Uma estratégia de segurança e um roteiro bem definidos que considerem o seguinte:
  - Proteção de dados: requisitos legais, regulamentares e processuais
  - Negócios: procedimentos e requisitos obrigatórios
  - Tecnologia: políticas, normas e procedimentos
  - Ameaças externas: mudanças no cenário de ameaças à segurança
- Um programa de gerenciamento de incidentes de segurança para controlar e remediar efetivamente incidentes relacionados à segurança, incluindo um programa de resposta a vulnerabilidades críticas de defesa cibernética

Conformidade e auditoria

Nossas equipes contam com programas globais de proteção de dados e segurança da informação. Mantemos uma área de governança eficaz e realizamos revisões de conformidade por meio de exercícios formais de auditoria. Gerenciamos a conformidade com as obrigações de proteção de dados e segurança da informação executando as seguintes revisões e programas.

Processo de certificação de segurança

Antes de implementados, todos os aplicativos e sistemas são submetidos ao nosso processo de certificação de segurança a fim de confirmar que foram desenvolvidos de acordo com nossas políticas de segurança da informação e com padrões de desenvolvimento de aplicativos seguros.

O processo de certificação de segurança inclui uma avaliação de risco, revisões de documentação e avaliações de vulnerabilidade. É aplicado a qualquer aplicativo ou sistema usado na criação, armazenamento ou gerenciamento de informações em nosso nome. Esse processo nos ajuda a manter a confidencialidade, a integridade e a disponibilidade de nossas informações e das dos clientes da EY.

Avaliações de impacto de privacidade e confidencialidade

Conduzimos avaliações de impacto de privacidade e confidencialidade (PIAs) de aplicativos e iniciativas de negócios que lidam com informações pessoais ou de clientes. Cada PIA analisa o aplicativo ou a iniciativa em relação aos padrões globais e, quando necessário, fornece conselhos para mitigar os riscos de privacidade e confidencialidade dos dados.

Depois da PIA, prepara-se uma lista de recomendações de privacidade e confidencialidade de dados, com orientações detalhadas, para todos os usuários e administradores daquele sistema. Essa avaliação detalhada inclui uma análise de quaisquer transferências de dados transfronteiriças para confirmar que cumprem os requisitos da UE.

Nossas organizações têm um vasto conjunto de políticas e diretrizes que nos ajudam a implantar aplicativos de acordo com os padrões e requisitos de proteção de dados aplicáveis.

Avaliações de eficácia de controle

Para verificar se os controles foram implementados e estão operando de forma eficaz, realizamos diversas avaliações de eficácia do controle, incluindo:

- Avaliações de vulnerabilidades de rede e aplicativos, que se concentram nos aspectos técnicos da Política Global de Segurança da Informação, como gerenciamento de *patches*, segurança de aplicativos e segurança de infraestrutura
- Avaliações de eficácia operacional, que revisam os controles técnicos e criam processos de componentes como sistemas operacionais, bancos de dados e infraestrutura
- Monitoramento operacional contínuo da eficácia do controle a fim de validar se os controles de segurança foram implementados e estão configurados adequadamente

Auditorias de segurança da informação

Para que tenhamos uma visão mais completa de nossa conformidade com a segurança da informação, nossos produtos, serviços e data centers globais de tecnologia são submetidos a auditorias. Realizamos diversas formas de auditoria:

- Auditorias independentes de conformidade de terceiros em relação à ISO 27001:2013 para certificar o Sistema de Gerenciamento de Segurança da Informação empregado em nossos três data centers globais nos EUA, Alemanha e Cingapura e salas de dados locais
- Atestação anual SOC 2, Tipo 2 conduzida por um auditor terceirizado independente, que abrange os princípios de segurança, confidencialidade e disponibilidade e abrange nossos três data centers globais nos EUA, Alemanha e Cingapura e a Plataforma Terceirizada de Tecnologia do Cliente EY baseada em nuvem
- Atestação anual ISAE 3402/SOC 1, Tipo 2 de nossos três data centers globais nos EUA, Alemanha e Cingapura e a Plataforma Terceirizada de Tecnologia do Cliente EY baseada em nuvem, por meio da qual nossos controles de segurança são testados e verificados por um auditor independente
- Varreduras na rede em busca de vulnerabilidade, que se concentram nos aspectos técnicos de nossa Política Global de Segurança da Informação, como gerenciamento de *patches*, segurança de aplicativos e segurança de infraestrutura
- Auditorias de fundação, que revisam os controles técnicos e criam processos de componentes como sistemas operacionais, bancos de dados e infraestrutura
- Auditorias de campo presenciais, que incluem entrevistas com o pessoal-chave da administração, visitas detalhadas ao local, revisões de documentação e varreduras de vulnerabilidades de rede - a forma mais significativa e detalhada de auditoria, que avalia a conformidade com todos os aspectos de nossa Política Global de Segurança da Informação

As constatações da auditoria de conformidade de segurança da informação são compiladas e avaliadas pela alta administração. Os planos de ação corretiva são determinados e aceitos, caso sejam necessários.

Exceções relacionadas à segurança da informação

Se um problema não puder ser gerenciado por meio de um plano de ação corretivo, utiliza-se um processo de exceção para revisar os riscos associados ao problema e explorar alternativas. O processo de exceção inclui um processo formal de aprovação, revisões regulares de cada exceção e uma avaliação de segurança com a atribuição de uma classificação de risco. Os controles de compensação normalmente acompanham as exceções aprovadas a fim de ajudar a mitigar adequadamente os riscos que podem surgir devido à modificação. Esse processo de exceção confirma que as exceções e quaisquer ações corretivas subsequentes estão devidamente documentadas, são gerenciadas, e serão revisitadas em uma data futura.

Resumo

Protegemos os ativos de informação dos clientes da EY por meio da adesão à estratégia integrada de proteção de dados e segurança da informação:

- Submetemos os aplicativos e sistemas globais a avaliações de impacto de privacidade de dados e revisões de certificação de segurança, que sustentam uma abordagem robusta e consistente na implantação e operação.
- Protegemos os dados pessoais dentro de nossa rede usando medidas de segurança físicas, técnicas e organizacionais apropriadas.
- Confirmamos que nossos contratos com operadores terceirizados contêm disposições equivalentes às nossas próprias políticas, práticas e controles a fim de confirmar que seus dados são gerenciados de forma adequada e segura, de acordo com os requisitos legais e regulamentares.

Clientes e pessoas exigem responsabilidade de qualquer organização que manipule seus dados pessoais e confidenciais e estão certos ao fazê-lo.

Entendemos a importância de realizar as ações adequadas com o intuito de proteger os ativos da informação e estamos comprometidos em proteger as informações relacionadas aos clientes e aos colaboradores da EY.

Caso tenha alguma dúvida ou precise de mais informações sobre como protegemos você e sua empresa, entre em contato com seu representante EY.

EY | Construindo um mundo de negócios melhor

A EY existe para construir um mundo de negócios melhor, ajudando a criar valor de longo prazo para clientes, pessoas e sociedade e criar confiança no mercado de capitais.

Possibilitadas por dados e pela tecnologia, diversas equipes EY, em mais de 150 países, oferecem confiança por meio de auditoria e ajudam no crescimento, transformação e atuação dos clientes.

Trabalhando em auditoria, consultoria, direito, estratégia, tributos e transações corporativas, as equipes da EY fazem perguntas melhores a fim de encontrar novas respostas para os problemas complexos que nosso mundo enfrenta hoje.

EY refere-se à organização global e pode se referir a uma ou mais das firmas-membro da Ernst & Young Global Limited, cada uma das quais é uma entidade legal separada. A Ernst & Young Global Limited, uma empresa do Reino Unido limitada por garantia, não presta serviços aos clientes. Informações sobre como a EY coleta e usa dados pessoais e uma descrição dos direitos que as pessoas têm em relação à legislação de proteção de dados estão disponíveis em ey.com/privacy. As firmas-membro da EY não presta serviços advocatícios onde proibido pelas leis locais. Para obter mais informações sobre nossa organização, acesse ey.com.

© 2021 EYGM Limited.
Todos os direitos
reservados.

EYG no. 000907-21Gbl
CSG no. 2011-3646208

ED None

Este material foi preparado somente para fins informativos gerais e não se destina a ser utilizado como aconselhamento contábil, fiscal, jurídico ou outra forma de aconselhamento profissional. Entre em contato com seus consultores para obter aconselhamentos específicos.

ey.com