Regras, Procedimentos e Descrição dos Controles Internos

EMPIRICUS GESTÃO DE RECURSOS LTDA.

Setembro 2024

Índice

1. Política de Treinamento

1. Objetivos

1.1.1. Objetivos Gerais

Estabelecer uma Política diretiva para estruturar um programa de Treinamento e Desenvolvimento de Pessoal na EMPIRICUS GESTÃO DE RECURSOS LTDA. (“Empiricus”), visando, desta forma, detectar necessidades de formação, motivar, aprimorar e melhorar o desempenho dos profissionais. Tal programa compreende tanto atividades de desenvolvimento de habilidades técnicas, intrínsecas de cada área como atividades de desenvolvimento comportamental.

Hoje, investir no desenvolvimento e retenção de seu time de funcionários já não é uma opção administrativa, mas sim fundamento básico de gestão dos seus recursos humanos, no sentido de formar a equipe dentro dos princípios da cultura empresarial. Mais do que um simples complemento da formação escolar, as atividades de treinamento e desenvolvimento permitem disseminar a cultura empresarial e acelerar o crescimento profissional, incrementando a performance.

1.1.2. Objetivos Específicos

- Estabelecer programas de treinamento com ênfase no Desenvolvimento Organizacional, visando provocar mudanças comportamentais duradouras, no que se refere à atitudes, valores, estrutura organizacional e práticas administrativas.
- Trabalhar as relações interpessoais e intergrupais através de uma perspectiva sistêmica focada nas relações de interdependência entre os diversos componentes da organização.
- Estabelecer e viabilizar programas de treinamentos técnicos e/ou específicos de cada área, no sentido de capacitar o indivíduo ou o grupo a novas habilidades necessárias.

2. Princípios Básicos

- Contribuir para o desenvolvimento de profissionais,
- Garantir adequação às regras e normas do setor,
- Melhorar a performance empresarial.

3. Levantamento de Necessidades de Treinamento

No Levantamento de Necessidades de Treinamento, deve-se partir sempre de um diagnóstico com base na visão de futuro da empresa. Antes de olharmos para onde estamos, devemos ver onde queremos chegar, trabalhando então, na construção de uma visão de futuro favorável e promissor, considerando o momento presente.

É importante estabelecer padrões claros, concisos e específicos sobre como fazer o trabalho para obter os resultados esperados, abrir canais de comunicação e criar confiança nos relacionamentos.

Observando estes princípios o RH efetuará, juntamente com o responsável de cada área, o Levantamento de Necessidades de Treinamento.

4. Classificação dos Programas de Treinamentos

Os programas de treinamento podem se classificar como:

Cursos Internos: São cursos realizados com recursos da Empiricus, dentro ou fora da empresa, elaborados por colaboradores internos.

Cursos externos: São cursos realizados através de recursos externos, dentro ou fora da empresa, ministrados por instrutores de entidades ou de centros de formação.

Certificações obrigatórias: Algumas funções requerem certificações obrigatórias para o exercício de suas atividades. Todos funcionários requeridos devem obter as certificações necessárias em tempo hábil para não interromper o funcionamento do setor. Tais atividades e certificações podem ser identificadas em conjunto com os reguladores da atividade em questão e as áreas de Compliance e RH.

5. Ações de treinamento

- "Repasse" (onde um funcionário retransmite aos seus colegas, os conhecimentos obtidos em um curso do qual ele participou);
- Reciclagem;
- Implantações;
- Rodízio de Funções;
- Programa de Desenvolvimento Gerencial;
- Programa de Idiomas;
- Programa de Graduação e Pós-Graduação;
- Seminários;
- Cursos de Atualização;
- Cursos técnicos;
- Cursos de habilidade comportamental;
- Visita técnica.

2. Política de Privacidade

Nós, da Empiricus, estamos comprometidos em resguardar sua privacidade e proteger seus dados pessoais. Queremos explicar para você um pouco mais de como tratamos os dados pessoais.

Canal de contato - privacidade@empiricus.com.br

Para acessar a Política de Privacidade completa da Empiricus, favor clicar aqui.

3. Política de Segurança da Informação

Estabelecer a base para o Programa de Segurança da Informação, cuja essência é a de aplicar medidas economicamente eficientes que protejam os ativos da Empiricus e seus Clientes com um nível aceitável de risco residual. Esta Política fornece uma base para o planejamento, implementação, exequibilidade e manutenção da segurança da informação.

Aplica-se a todas os Colaboradores, estagiários, contratadas e outras pessoas e organizações – que estiverem envolvidos de qualquer forma com os ativos de informação da Empiricus. Ela cobre todos os modos e formas de salvaguardar as informações em todos os ambientes e mídias, incluindo, mas não limitados a mídias eletrônicas, impressas e em filme.

3.1 Fundamentos da segurança da informação

- **Mantenedor e titular do ativo de informação:** cada ativo de informação deverá possuir um mantenedor, que será responsável por tal ativo. A responsabilidade, neste contexto, se refere à responsabilidade pela implementação e manutenção das medidas de segurança necessárias para a proteção apropriada do ativo da informação. Os requerimentos que determinam quais medidas de segurança devem ser adotadas são definidos pelo titular do ativo da informação.

- **Confidencialidade, Integridade e Disponibilidade:** todos os ativos de informação deverão ser categorizados por sua necessidade de confidencialidade, integridade e disponibilidade, em conformidade com as necessidades comerciais e quaisquer restrições e requerimentos legais, contratuais ou regulatórias. Um determinado ativo de informação deverá receber um nível de segurança por todo o banco.

- **Segregação de Deveres:** as transações envolvendo ativos de informação de alto valor não deverão permanecer sob o exclusivo controle de uma única pessoa. Por exemplo, uma transação financeira não deverá ser incluída e confirmada pela mesma pessoa, e o software não deverá ser desenvolvido e então utilizado na produção pela mesma pessoa.

- **"Necessidade de saber" e "Necessidade de fazer":** as pessoas devem apenas ter acesso às informações ou funcionalidade que forem necessárias para a devida execução de seus deveres. O acesso aos ativos de informações deverá estar explicitamente autorizado, sendo que o padrão é não se ter acesso.

- **Medidas apropriadas de segurança:** as medidas de segurança da informação deverão ser selecionadas com base em requerimentos comerciais e contratuais, por meio de avaliações de risco, eficiência econômica e restrições legais. Devido ao fato de que nenhum sistema de informação é absolutamente seguro, os riscos residuais após a implementações de salvaguardas deverão ser avaliados, documentados pelo mantenedor do ativo e levados à atenção do titular do ativo.

- **Monitoramento da conformidade:** auditorias regulares e atividades de revisão deverão ser realizadas pelos titulares do ativo de informação ou por seus substitutos, assim como por funções independentes de controle e auditoria, para monitorar a conformidade geral com as políticas e diretrizes sobre segurança e para reportar deficiências suspeitas ou conhecidas na segurança.

- **Lidando com incidentes:** os mantenedores dos ativos de informação deverão monitorar os sistemas pelos quais eles são responsáveis, para detectar quaisquer violações ou anormalidades na segurança. Os processos deverão ser estabelecidos para reagir de forma sensível e efetiva, e também para que se aprenda com incidentes, para melhorar as salvaguardas.

3.2 Responsabilidades pela segurança da informação

- **Colaboradores, contratados e agentes bancários:** todos os Colaboradores, contratados e agentes bancários são responsáveis pela compreensão e manutenção da segurança da informação em sua própria área de trabalho e na empresa como um todo. Eles devem estar cientes da significância das informações a eles confiadas e deverão exercer a devida diligência em sua proteção. Eles deverão conhecer seus deveres com relação à segurança das informações e aceitar a obrigação de cumprir com as políticas, diretrizes e normas relevantes. Eles deverão utilizar as informações apenas dentro dos limites de sua autorização e para os propósitos para os quais as informações foram fornecidas.

- **Gerentes:** possuem a responsabilidade adicional de fornecer liderança na execução e na conformidade com as medidas de segurança da informação, enquanto mantêm um senso de proporção e equilíbrio. Os gerentes deverão auxiliar os Colaboradors na compreensão da importância da segurança da informação e sua observância nos regulamentos relevantes.

- **Chefes de negócios:** deverão gerenciar os riscos de informação relativos às suas atividades comerciais. Eles deverão designar os titulares dos ativos de informação para os vários ativos sob sua responsabilidade. Os titulares dos ativos de informação deverão aprovar a implementação de salvaguardas técnicas e procedimentais apropriadas, propostas pelos mantenedores do ativo de informação, uma vez que eles são os que possuem o conhecimento interno e aceitam o risco residual envolvido. Não obstante, por uma perspectiva externa (legal e regulatória), o responsável máximo por quaisquer riscos residuais é o chefe do negócio.

- **Titulares dos ativos de informação:** todos os ativos de informação deverão possuir um titular explícito, que será responsável pela classificação e definição apropriadas dos requerimentos para a proteção de todos os ativos de informação a eles confiados.

- **Mantenedores dos ativos de informação:** os mantenedores dos ativos de informação asseguram o uso das medidas apropriadas de segurança para proteger os ativos e deverão estabelecer procedimentos para lidar com incidentes.

- **Fornecedores de serviços de informação:** os fornecedores do serviço de informação são responsáveis pelo fornecimento de produtos e serviços confiáveis e seguros, que estejam em conformidade com as necessidades de segurança da informação do banco. Eles são responsáveis por assegurar que os produtos e serviços em uso sejam mantidos de forma apropriada, mantidos atualizados, com relação às ameaças que surgirem e compatíveis para uso entre as áreas de negócios.

- **Diretor de Segurança:** independente da TI, é responsável pela identificação e avaliação do risco associado com todo o uso de recursos de informação e por relatar à gestão avaliações de risco e outras informações relevantes ao risco.

- **Jurídicos e Compliance:** fornecem orientação, para assegurar a conformidade com todas as leis e regulamentos aplicáveis (incluindo atos de proteção aos dados), relativos à segurança das informações. Em cooperação com especialistas em segurança da informação e com o Diretor de Segurança, revisarão as ações sendo executadas e a adequabilidade da solução de segurança da informação de um ponto de vista jurídico.

- **Auditoria Interna:** a Auditoria Interna possui uma função independente na execução de revisões baseadas em risco da conformidade com as políticas, diretrizes e normas sobre segurança da informação. Eles também podem avaliar a eficácia de controles de segurança, examinar os controles de segurança planejados e participar do processo de análise de riscos.

A política de Segurança da Informação é organizada sob a forma de um framework, composto das seguintes políticas internas:

- Email e Mensagens Eletrônicas;
- Gerenciamento de Ativos de Software e Hardware;
- Proteção Contra Vírus & Malware;
- Framework de Risco de TI;
- Exceções às políticas e padrões de TI;
- Gerenciamento de incidentes e problemas;
- Gerenciamento de Vulnerabilidades;
- Controle de Acesso;
- Segurança de Aplicações;
- Segurança de Banco de Dados;
- Segurança de Sistemas Operacionais;
- Segurança no Desenvolvimento de Sistemas;
- Monitoramento e Registro de Transações;
- Armazenamento e Recuperação de dados;
- Gerência de Mudanças;
- Gerenciamento de Capacidade e Desempenho;
- Segurança em Conexões de Rede;
- Acesso Remoto;
- Uso da Internet.

4. Segurança, classificação e ciclo de vida de dados e Confidencialidade

Esta política estabelece diretrizes aplicáveis à segurança, classificação e ciclo de vida de dados, que se inicia quando as informações são concebidas e percorrem todo o ciclo até sua destruição ou exclusão, passando pelos estágios intermediários de classificar, transmitir / receber e salvar / arquivar. As responsabilidades das equipes em cada um dos estágios previamente mencionados do ciclo de vida dos dados também serão tratadas neste documento.

A presente política descreve o ciclo de vida dos dados por uma perspectiva de segurança. Ela detalha cada estágio pelos quais as informações podem passar, desde sua concepção inicial até sua destruição. Cada estágio requer que os colaboradores lidem com informações de forma apropriada para que os dados de clientes, funcionários e da Empiricus permaneçam seguros, o que implica no impedimento de divulgação

não autorizada. Portanto, o principal objetivo desta política é fornecer orientação
quanto à correta classificação das informações a fim de evitar exposição não autorizada de conteúdo sensível criado, processado ou compartilhado pelos colaboradores de forma diária.

Deve ser observado que a divulgação não autorizada de informações sensíveis poderá resultar em sérias consequências, como perdas financeiras, danos à reputação da Empiricus e infração a requerimentos estatutários (por exemplo, confidencialidade banco-cliente, confidencialidade do negócio, atos de proteção dos dados), que poderia resultar em processos criminais contra os colaborares e contra a Empiricus.

4.1. Princípios Fundamentais

A segurança dos dados está baseada na Tríade - Disponibilidade, Integridade e Confidencialidade, que são os princípios mais importantes desta Política.

A disponibilidade assegura o acesso de pessoas autorizadas aos dados em tempo oportuno. A integridade dos dados deve ser mantida em todo tempo, garantindo a precisão e confiabilidade das informações. A confidencialidade indica o nível necessário de sigilo com o qual a informação deve ser tratada.

5. Política de Prevenção à Lavagem de Dinheiro e Anticorrupção

Lavagem de dinheiro é crime e pode ser definida como o resultado de fazer com que o faturamento com atividades criminosas pareça ter vindo de atividades e negócios legítimos. Considera-se crime na maioria das jurisdições o ato de facilitar atividades de lavagem de dinheiro e/ou negligenciar/deliberadamente não detectar/reportar atividades suspeitas às autoridades competentes.

Colaboradores não devem, conscientemente, iniciar ou participar de qualquer esquema de lavagem de dinheiro. Qualquer Colaborador será considerado participante de tal esquema se for evidente que ele/ela sabia ou deveria saber da atividade. Atividades suspeitas de lavagem de dinheiro devem ser relatadas internamente ao responsável pela Prevenção à Lavagem de Dinheiro (“PLD” ou “AML”, na sigla em inglês) do Compliance *(AML Compliance Officer*).

Colaboradores devem sempre empregar o princípio do “conheça seu Cliente” (“KYC”, na sigla em inglês). Você deve acompanhar os procedimentos de abertura de conta na sua área de negócios que exijam o fornecimento de informações para que o banco possa ter registros de com quem faz negócios. A identificação correta do Cliente deve ser feita antes de iniciar uma relação financeira. Colaboradores devem esclarecer o histórico econômico e propósito de qualquer transação onde a estruturação e/ou valor pareçam estranhos em relação ao Cliente, banco ou subsidiária em questão.

5.1 Para isso, Colaboradores devem:

- Categorizar o Cliente (i.e., governo, corporativo, regulado/não regulado, “private”, instituição de caridade, fundo, assessor de investimento etc.);
- Avaliar o risco e, quando necessário, realizar uma verificação aprofundada em Cliente que possam representar maiores riscos com base em: **geografia** (por exemplo, se o Cliente é relacionado a um país sensível); **tipo** (por exemplo, se o Cliente é uma entidade regulada ou não, se o Cliente é uma pessoa politicamente exposta – “PEP”, na sigla em inglês); **setor** (por exemplo, cassino, comerciante de armas, “doleiros” ou assemelhados, *shell bank* etc.); a **natureza do produto ou atividade de negócios** (por exemplo, metais preciosos, notas bancárias, negócios que lidam com altas somas de recursos em espécie etc.); ou **reputação** (por razões sociais, ambientais ou outras);
- Levantar informações comerciais e sobre a fonte de renda (quando exigido pelo tipo de Cliente ou risco);
- Quando necessário, definir a estrutura societária e identificar pessoas relacionadas ao Cliente; e
- Levantar informações e dados necessários para verificar a identidade do Cliente e pessoas relacionadas (quando relevante).

Colaboradores e *Business Sponsors* devem também avaliar continuamente o relacionamento e as atividades de seus Cliente, pelos quais sãoresponsáveis, e informar o AML Compliance sobre qualquer

mudança material, tais como mudanças na situação do Cliente, informações de *status* ou propriedade de tomem ciência ao longo da relação de negócios.

Entender as transações normais e esperadas para determinado Cliente nem sempre é algo que pode ser feito ao início do relacionamento. Frequentemente, apenas após estudar as suas atividades por certo período de tempo é que se pode determinar os padrões de normalidade para as transações do Cliente. Você deve monitorar as transações de seus Cliente e entender/determinar o que está dentro dos parâmetros considerados normais, legítimos e esperados para cada um deles.

Tal monitoramento irá depender do tipo de Cliente, conta e classificação de risco identificados no processo de abertura de conta e *KYC*, e se houve qualquer mudança neste perfil de risco. O tamanho da conta, bem como o número e o tamanho das transações conduzidas através desta, o risco de atividade ilícita associado ao tipo de Cliente e as transações conduzidas por meio de tal conta, devem ser levados em consideração.

Se for determinado que um Cliente prospectivo representa risco inaceitável de lavagem de dinheiro, financiamento de terrorismo ou crime financeiro, ou não for possível afirmar com razoável certeza a verdadeira identidade de um Cliente por meio dos processos de identificação e verificação estabelecidos no Programa de Identificação (“Client Identification Program – CIP”), a conta não poderá ser aberta.

Se o Colaborador tomar conhecimento de informações que levantem dúvidas quanto à identidade de um Cliente ou se perceber atividades não usuais que sejam suspeitas, deve procurar o AML Compliance que irá decidir se é necessário notificar os órgãos reguladores.

5.2 Terrorismo

A Empiricus é totalmente comprometido com as legislações antiterrorismo de vários países no mundo. Nenhum Colaborador deve lidar, direta ou indiretamente, com qualquer pessoa ou grupo envolvido, ou suspeito de envolvimento, com atividades ou financiamento de terrorismo de qualquer tipo. Atividades suspeitas devem ser comunicadas ao *AML Compliance Officer*.

5.3 Suborno e Tratamento Especial

Colaboradores e terceiros são proibidos de oferecer/receber qualquer tipo de suborno, estímulo, tratamento preferencial ou outra consideração similar a agentes governamentais ou privados em troca da realização, ou promessa de realização, de atos ilícitos ou inapropriados para atrair negócios ou por qualquer outro motivo.