Política de Segurança da Informação

Sumário

1. Objetivo

Estabelecer as diretrizes sobre segurança da informação formalizando os aspectos relevantes de controle e monitoramento, visando a proteção adequada dos ativos da informação com relação aos aspectos de integridade, disponibilidade e confidencialidade das informações contidas nos sistemas e demais recursos de TI.

2. Abrangência

Esta Política se aplica a todos os colaboradores, estagiários, trainees, temporários, fornecedores, cientes e terceiros vinculados à Regnier.

3. Definições

PSI: Política de Segurança da Informação

ACESSO REMOTO: Recurso que permite ao usuário acessar o ambiente de TI (redes, sistemas etc.) estando ausente da empresa, a partir de qualquer local, utilizando softwares/serviços específicos.

COLABORADORES (ES): Executivos, empregados, trainees, aprendizes e temporários que possuem relação com a Regnier.

CONFIDENCIALIDADE: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

DISPONIBILIDADE: Garantia de que os usuários autorizados tenham acesso à informação sempre que necessário.

INFORMAÇÃO: Dados que, após processados ou organizados, produzem fatos que tenham um significado compreensível. É um ativo e, como qualquer outro ativo importante para os negócios, tem um valor para a organização.

INTEGRIDADE: Garantia da exatidão e completude da informação e dos métodos de processamento.

RECURSOS COMPUTACIONAIS: Computadores, Notebooks, Tablets, Smartphones, Impressoras, Sistemas de informação, Drives de rede, SGBD, E-Mail (Correio eletrônico), Internet, Intranet e afins.

SGBD: Sistemas de gerenciamento de Banco de Dados.

SOFTWARE SHAREWARE: Versão concisa ou com prazo de validade limitado de um programa destinado à venda, dando ao cliente a opção de experimenta-lo antes da aquisição.

SOFTWARE FREEWARE: Programa gratuito, que permite ao usuário utilizá-lo desde que não o comercialize.

TI: Tecnologia de Informação.

USUÁRIOS: Todos aqueles que utilizam os recursos de tecnologia da informação, sendo, portanto, responsáveis pelo conhecimento e aplicação desta PSI, abrangendo os Colaboradores da Regnier, incluindo todos os prestadores de serviço terceirizados que precisem acessar os Recursos Computacionais da Regnier.

Usuário Normativo: Usuário responsável pelas funcionalidades, dados e informações de um ou mais sistemas da Regnier, a quem cabe a aprovação previa de melhorias a serem efetuadas no sistema de sua responsabilidade, bem como pela classificação, definição do perfil de usuário e do tipo de acesso às informações.

Key User: usuário responsável pela gestão dos perfis de acessos da sua área de negócios ou processos internos que está inserido.

Nível de Suporte: Privilégio atribuído aos gestores, pela área de Recursos Humanos e reconhecido na organização que define os limites para efeitos de aprovação de atos administrativos relacionados á gestão de suas áreas

4. Responsabilidades

4.1. Gestor de TI

Autorizar a realização de testes com o propósito de averiguar o nível de segurança do ambiente Regnier.

4.2. Colaboradores

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da Regnier. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à Regnier e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

4.3. Colaboradores Temporários e ou Terceirizados

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

4.4. Gestores de Processos e Pessoas

Ter postura exemplar em relação à segurança da informação conforme definido nesta política, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Regnier. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Regnier. Antes de conceder acesso às informações da Regnier, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

4.5. Usuário Normativo ou Key User

- Autorizar a liberação de direitos de acesso compatíveis com as funções desempenhadas pelos usuários, através de perfis de acesso diferenciados;
- Revisar periodicamente os acessos liberados aos recursos que é responsável, podendo solicitar remoção e/ou readequações de perfis para os usuários, que já possuem acesso, bem como readequações das permissões do próprio perfil (sem necessidade de aprovação gerencial).

4.6. Usuário Normativo

Aprovar as melhorias, sua classificação, definir perfil do usuário e do tipo de acesso a essas informações dos sistemas sob sua responsabilidade.

4.7. Analista de TI

Aprovar o envio de cópia de sistema (programas, telas, fontes etc.) em atendimento a qualquer demanda necessária, exceto para fins de auditoria externa das demonstrações financeiras;

Autorizar e garantir o registro de intervenções feitas pela TI nos seguintes processos, através de perfis de acesso específicos:

- No controle do fluxo de documentos fiscais eletrônicos (NFe, CTe, MDFe etc.) entre os sistemas da Regnier e as diferentes Secretarias de Fazenda estaduais e vice-versa, garantindo que o fluxo de troca de informações aconteça entre os diferentes ambientes;
- Nas mensagens trocadas entre os sistemas o que inclui mas não se limita a ERP's e/ou Sistemas de automação, garantindo que o fluxo de troca de informações aconteça entre os ambientes;
- Execução de processos de archiving (remoção de dados das bases produtivas e levando-as para outra plataforma Integrada ao ERP):
- Manutenção de registros em tabelas de configuração de sistemas.

5. Diretrizes Gerais

5.1. Princípios e Definições Gerais

- A Segurança da Informação é responsabilidade de todos. Da mesma forma, deve refletir em hábitos, posturas, responsabilidades e cuidados constantes nos momentos de uso, solicitação e aprovação de recursos;
- A área de TI é responsável por manter e fomentar a implementação desta Política, bem como orientar os usuários quanto aos preceitos de segurança da informação a serem observados por todos, colaboradores, com maior ou menor integração com o restante da organização;
- A utilização das informações e dos recursos computacionais deve ser sempre compatível com a ética; confidencialidade e a finalidade das atividades desempenhadas polo usuário, seguindo padrões e procedimentos definidos pela Regnier, para garantir a disponibilidade e desempenho das aplicações;
- A conexão de equipamentos de terceiros na rede da Regnier somente será permitida se não apresentar risco ao ambiente corporativo e estiver de acordo com as políticas da Empresa aplicáveis aos demais equipamentos;
- A utilização indevida dos recursos computacionais pode provocar suspensão dos acessos, deve ser notificada à área de Segurança da informação e, se necessário, à equipe de investigação interna poderá iniciar investigação referente a esta não conformidade;
- Qualquer violação a qualquer uma das diretrizes e orientações expressas nesta política poder resultar em medidas disciplinares apropriadas, bem como em investigações internas, e sujeitará o usuário às penalidades administrativas e àquelas previstas nas legislações cível, trabalhista e penal.

5.2. Gestão da Segurança da Informação

- Todos os colaboradores são responsáveis pela segurança das informações da Companhia;
- Cada gestor da Regnier é o Usuários Normativos das informações pertencentes ao domínio da sua autoridade, e podem delegar as funções de concessão de direitos de acesso/homologação de alterações nos sistemas e demais recursos de TI. Para tanto, devem formalizar estas delegações através de solicitação ao Gestor de TI.

5.3. Segurança Física dentro das instalações da Regnier

- Para as movimentações de equipamentos de estrutura básica do ambiente computacional da empresa (servidores, roteadores, switches, hubs, controladoras, impressoras, meios óticos e magnéticos para backup, etc) é obrigatória a solicitação de autorização do gestor do colaborador solicitante ao gestor de TI.
- Os Centros de Processamento de Dados (CPD) devem ter dispositivos contra riscos, tais como, controle de acesso físico, controle de incêndio, controle de fumaça dentre outros. Cabe ao Gestor de TI a definição de tais dispositivos de proteção, considerando características regionais, a criticidade das informações e os recursos tecnológicos envolvidos.

5.4. Segurança Lógica

- Cabe à Diretoria de TI exigir que todos os ambientes lógicos (sistemas operacionais, SGBD's e sistemas de informação) tenham o seu acesso restrito por senhas, estando em conformidade com as diretrizes descritas nesta Política, salvo em situações nas quais existem restrições técnicas impeditivas;
- Todo programa ou transação desenvolvido ou adquirido para execução no ambiente da Regnier deve conter os requisitos de segurança definidos no documento de padrão de desenvolvimento. Os casos de exceção deverão ser tratados em conjunto pelas áreas de TI e a Diretoria da Regnier;
- Nenhuma senha pessoal pode ser gravada no código-fonte de programas, tampouco em arquivos ou tabelas destinadas a outros fins. No caso de tabelas/arquivos especificas para armazenamento de senhas, deve-se utilizar de forma segura utilizando criptografia;

  Nota: *O acesso - mesmo o de simples consulta - aos arquivos ou tabelas de senhas não será permitido, em nenhuma circunstância, a nenhum colaborador. Tal restrição deverá ser provida por mecanismos de segurança (exemplo: criptografia, restrição de acesso ao banco de dados, etc.)*

- Toda conta de acesso sem uso há mais de 45 dias poderá ser desabilitada sem prévia autorização do proprietário ou de seu Gestor, de modo a liberar recursos físicos e/ou licenças de softwares alocados, a exceção a essa regra é para nível de gerência e/ou diretoria, que serão contatados antes do recurso ser desabilitado;
- A partir de 45 dias da data de desligamento os usuários poderão ter seus acessos excluídos, sem a necessidade de aprovação prévia;

- É proibida a desinstalação, nas estações usuárias, de softwares e/ou hardwares, que são utilizadas para realizar controle físico e lógico dos recursos disponíveis;
- Somente será permitido o uso de recursos homologados e autorizados pela empresa, desde que sejam identificados individualmente, inventariados, com documentação atualizada e atendendo a legislação pertinente em vigor. Portanto, qualquer usuário que exponha a empresa a sanções jurídicas por utilização de softwares não homologados, independentemente de sua classificação (shareware, freeware, demo, etc) sem respaldo das respectivas licenças, está sujeito as medidas disciplinares, bem como em investigações internas, e às sanções previstas em lei;
- No caso de contas de acesso standard e impossíveis de serem eliminadas ou alteradas, as senhas standard (que vem junto do produto) serão, obrigatoriamente, modificadas imediatamente após a disponibilização do sistema e/ou ambiente, sem que haja solicitação específica sobre isso;
- É obrigatória a existência de documentação de Segurança e de infraestrutura para implantação de sistemas de informação, conforme metodologia em vigor, sendo que não serão implementados se trouxerem fragilidades que comprometam o ambiente da Regnier;
- Somente os usuários devidamente autorizados e com justificativa poderão ser administradores das respectivas estações de trabalho.

5.5. Formação e Uso de Senhas

Todos os sistemas do ambiente da Regnier devem atender os requisitos abaixo, salvo os casos em que ocorrerem impedimentos técnicos (exemplo: Sistemas legados), devidamente justificado pelo analista de TI e/ou gestor responsável.

- Para a formação das senhas, serão adotados os seguintes critérios:
- Tamanho mínimo de 8 caracteres;
- Nunca podem ser nulas ou estar em branco;
- Nunca visíveis na tela onde são informadas para atualização;
- Mínimo de 2 dígitos numéricos;
- Mínimo de 2 caracteres alfabéticos;
- Vetar a reutilização de últimas 5 (ou mais) senhas utilizadas;
- Serem bloqueadas após 5 tentativas consecutivas e malsucedidas de acesso.
- Todas as senhas de uso individual expirarão no máximo a cada 90 dias. Além disso, todas as senhas iniciais serão criadas expiradas, devendo ser alteradas no primeiro acesso por cada usuário;
- As senhas pessoais podem ser trocadas pelo próprio usuário, independentemente de sua data de expiração. Porém, deverão ser impossibilitadas de serem trocadas mais de 1 vez no mesmo dia;
- Nenhum colaborador poderá usar de sua superioridade hierárquica ou funcional sobre outrem para determinar ou obrigar que este compartilhe sua senha individual de acesso com quem quer que seja.
- O compartilhamento de senhas individuais é proibido para todos os níveis da organização. Da mesma forma, abrir uma conexão autenticada para deixar que outra pessoa a utilize. Em hipótese alguma, um usuário poderá passar a sua senha individual de acesso para outrem. Tal ação, uma vez detectada será devidamente reportada à Diretoria da Regnier;
- Qualquer tentativa de *quebrar* (tentar descobrir) a senha individual de acesso de uma outra pessoa, ou mesmo de invadir ambientes ou sistemas cujo acesso lhe é negado, serão notificadas ao Comité de Ética e poderá resultar em medidas disciplinares apropriadas, conforme disposto no Código de Ética da Companhia, bem como em investigações internas;

- É dever de todos zelar pelo sigilo de suas senhas de autenticação, bem como escolher senhas fortes dificultando ser descoberta facilmente por outra pessoa;
- Exceções a esses requisitos mínimos de segurança devem ser aprovados e validados pela Área de TI em conjunto com a Diretoria.

5.6. Segurança de Acessos

- A conta de acesso e a senha de cada pessoa são únicas, individuais e intransferíveis, sendo reconhecidas como equivalentes à sua assinatura e representam nível de delegação concedida para o desempenho de suas funções;
- Os acessos externos a recursos da empresa (acesso remoto de colaboradores, terceiros, fornecedores, clientes e outros casos que vierem a surgir) somente serão concedidos mediante autorização prévia por intermédio de soluções técnicas corporativas e homologadas pela Regnier;
- O acesso à Internet e permitido somente por intermédio do sistema de segurança corporativo. É proibido o acesso direto à Internet por intermédio de provedores externos estando conectado à rede corporativa;
- Eventuais interligações entre redes (de forma física e/ou lógica) envolvendo processos de automação e/ou informação, só deverão ocorrer utilizando soluções corporativas definidas pela área de TI, de forma a garantir a disponibilidade, a integridade e a confidencialidade dos ambientes.

5.7. Controle de Acesso

- A área de TI deve assegurar que nenhum colaborador ou prestador de serviço obtenha direitos de acesso sem as devidas aprovações;
- A área de Recursos Humanos definirá em conjunto com a área de TI um padrão de identificação de usuários. Essa identificação será utilizada para associar, de maneira única, cada direito de acesso à pessoa que o detém;
- Serão concedidos direitos de acesso compatíveis com as funções desempenhadas pelos usuários, através de perfis de acesso diferenciados. Tais perfis objetivam restringir os dados e operações disponíveis, e sua definição será realizada em conjunto com Usuários Normativos.

5.8. Segregação de Ambiente e Funções

A Area de TI deve assegurar que todos os sistemas de informação sejam aderentes às diretrizes a seguir:

- Os ambientes de processamento de TI deverão manter o ambiente de produção segregado dos demais;
- No ambiente de Produção os usuários da Area de TI e prestadores de serviços que realizam atividades de suporte, só podem ter acesso de consulta, salvo as exceções que devem ser autorizadas diretamente entre a gerência envolvida, a Área de TI e a Diretoria;
- O acesso de alteração às bases de dados dos ambientes de produção será feito, unicamente, através dos sistemas de informação. É totalmente vetado qualquer tipo de acesso direto. Os casos extremos de necessidade de liberação serão aprovados pelo Gestor do Solicitante Gestor de TI e a Diretoria em Conjunto, sendo que esta última possui poder de veto.

- As alterações no ambiente computacional de produção da Regnier, deverão ser realizados conforme os processos de gestão de mudanças aprovados pelos respectivos responsáveis.

5.9. Propriedade Intelectual

Todos os sistemas, projetos de TI e/ou configurações desenvolvidos para atender as necessidades e aos interesses da empresa, são de propriedade única e exclusiva da Regnier, e somente poderão ser cedidos ou comercializados mediante aprovação da Area de TI e da área responsável pelo sistema.

5.10. Auditoria e Investigação

- Todos os usuários devem estar cientes que as informações armazenadas nos recursos tecnológicos da Regnier, pertencem à mesma, podendo a qualquer momento, serem monitoradas sem aviso prévio;
- A Auditoria Interna e Investigação poderão ter acesso, a qualquer informação que esteja armazenada no ambiente lógico (sistemas operacionais, SGBD's e sistemas de Informação). Havendo suspeita de qualquer atividade que possa comprometer a segurança do ambiente de TI, a Diretoria poderá solicitar procedimento de Auditoria e Investigação, podendo investigar e monitorar sob demanda as atividades de qualquer usuário além de inspecionar seus arquivos e registros de acesso, sempre que julgar necessário;
- Os sistemas devem ser desenvolvidos ou adquiridos visando a existência de recursos de trilhas de auditoria, sendo que as mesmas devem ser protegidas contra acessos indevidos a devem conter no mínimo as seguintes informações: Identificador do usuário, data e hora da operação, operação, dados alterados.

6. Referências

Política de Privacidade

7. Aprovação

Jérémy Matioszek

Diretor Geral - Brasil