Política Empresarial

Tecnologia e Segurança da Informação

1 OBJETIVO

A Política sobre Tecnologia e Segurança da Informação estabelece conceitos e orientações para a gestão do ambiente tecnológico da FORESEA, compreendendo infraestrutura, sistemas, aplicativos, ativos e segurança dos dados manipulados em meio digital ou físico, pelos integrantes ou parceiros no desenvolvimento de suas atividades, visando assegurar a proteção das informações, bem como suportar os objetivos estratégicos da FORESEA.

São objetivos desta Política:

- Estabelecer e/ou orientar os integrantes e parceiros da FORESEA sobre:
  - a importância da segurança da informação para prevenção e redução de riscos e a garantia da integridade, o sigilo e a disponibilidade das informações;
  - padrões de criação, recepção, retenção e destruição de dados, registros e informações produzidas no curso das atividades empresariais;
  - como agir para garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e rastreabilidade da informação necessária para a sustentabilidade da FORESEA;
- Apoiar a FORESEA em seus objetivos de negócio e estar em conformidade com os requisitos legais e regulamentares;
- Servir de referência para qualquer iniciativa ou processo relacionado à informação ou aos ativos de processamento de informação;
- Definir as responsabilidades na gestão da segurança da informação.

2 APLICAÇÃO

Esta Política é aplicável à FORESEA, inclusive suas empresas controladas que não tenham Conselho de Administração, a todos os integrantes, Diretores e membros do Conselho da Administração, em qualquer jurisdição.

Adicionalmente, esta Política serve de orientação para os membros dos conselhos de administração indicados pela FORESEA, em controladas ou coligadas, para que, em alinhamento com os demais conselheiros, aprovem e implementem uma política sobre segurança e tecnologia da informação que contenha os princípios, conceitos e demais orientações definidos e explicitados nessa política, sem deixar, contudo, de promover os complementos e outras orientações necessárias para adequação às características de seus respectivos negócios e às contribuições dos demais conselheiros.

3 SIGLAS E DEFINIÇÕES

Autenticidade: é a propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física ou por um determinado sistema, órgão ou entidade.

CA-FORESEA: Conselho de Administração da FORESEA. Órgão colegiado executivo, deliberativo, responsável por aprovar o direcionamento estratégico e acompanhar o desempenho da empresa, deliberar sobre as demais matérias de sua competência e exercer as funções de controle que lhes são pertinentes.

COMEX: Comitê Executivo.

Confidencialidade: implica em impedir o acesso não autorizado, acidental ou intencional, garantindo que apenas pessoas, sistemas, órgãos ou entidades devidamente autorizados e credenciados tenham acesso à informação.

Disponibilidade: garantia de que a informação estará acessível às pessoas, processos automatizados, órgãos ou entidades no momento em que for requerida. Logo, a disponibilidade está relacionada à prestação continuada de um serviço, sem interrupções no fornecimento de informações.

Firewalls: dispositivo de rede de computadores, na forma de um programa ou de equipamento físico, que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP.

Gerenciamento de dados e backup: processo que tem o propósito de garantir a integridade, autenticidade e legalidade das informações registradas pelos usuários da FORESEA.

Incidentes de segurança da informação: um incidente de segurança da informação é um ou uma série de eventos não desejados ou não esperados, com uma probabilidade significante de comprometer as operações dos negócios e ameaçar a segurança da informação (ISO/IEC 27000 2.36).

Informação: propriedade da FORESEA, consiste em toda Informação produzida, transmitida ou armazenada no âmbito dos negócios, que pode ser de caráter de engenharia, comercial, financeira, administrativa, estratégica, mercadológica, legal ou de qualquer outra natureza, bem como todas as informações adquiridas por contrato, associação, aquisição ou fusão, como também aquelas relativas a clientes ou parceiros, entre outras (protegidas ou não por confidencialidade), independentemente de sua forma (verbal e escrita) e suporte (físico ou digital).

Infraestrutura de Tecnologia da Informação: patrimônio que engloba todos os recursos de Tecnologia da Informação, proprietário ou de terceiros, tais como, mas não se limitando a, servidores, data centers, desktops, notebooks, tablets, smartphones, placas de dados, telefones celulares, telefones com protocolo de Internet, impressoras, links de Internet, linhas telefônicas, dispositivos de IoT, entre outros recursos que venham a ser utilizados no futuro em virtude da inovação tecnológica.

Integridade da informação: está relacionada à sua fidedignidade. Assegurar a integridade da informação, portanto, significa garantir que a informação não foi modificada ou destruída de maneira não autorizada, quer de forma acidental ou intencional.

Legalidade: garante que o uso das informações segue as legislações vigentes dos países, regulamentos, licenças e contra.

LGPD: Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parceiro: prestadores de serviço, parceiros de negócio e todos que não sejam classificados como integrantes e que interagem com as informações da FORESEA.

Programa de Ação (PA): documento que explicita as responsabilidades do integrante em um determinado período, cujo foco são os resultados esperados do trabalho de cada um e não as tarefas que deve realizar. Nele estão também a delegação que recebe, os compromissos que assume e a recompensa a que terá direito.

Proprietário da Informação: integrante ou parceiro responsável pela elaboração da informação ou receptor de informação externa.

Rastreabilidade: é a propriedade de configuração dos sistemas e de acesso às informações que possibilita o rastreamento de atividades físicas e lógicas.

Responsável pela gestão da Informação: responsável pela gestão de dados da FORESEA, exercendo também o papel de Encarregado de Dados ("Data Protection Officer" - DPO), em cumprimento à LGPD.

Segurança da Informação: conjunto de medidas de proteção da Informação adotadas pela FORESEA, para que esta seja conhecida somente por aqueles que devem conhecê-la para o desenvolvimento dos seus PAs, evitando o seu uso indevido, inadequado ou ilegal.

TI: Tecnologia da Informação.

4 DESCRIÇÃO

4.1 Grupo de Trabalho em Segurança da Informação

O Grupo de Trabalho em Segurança da Informação tem caráter permanente e conduz a gestão da Segurança da Informação no âmbito da FORESEA. Tem natureza multidisciplinar e é composto pelo Responsável por Tecnologia da Informação, Responsável pela Gestão da Informação, representante da equipe de Pessoas, representante da equipe Jurídica e representante da equipe de Conformidade.

4.2 Classificação da Informação

A Informação dever ser classificada por seu proprietário de acordo com as regras e padrões definidos em documento normativo elaborado pelo Grupo de Trabalho em Segurança da Informação, sendo a informação identificada de acordo com o grau de sigilo, sua importância e criticidade para o desenvolvimento dos negócios e em alinhamento com a legislação aplicável.

4.3 Controle de Acesso às Informações

Cabe ao Responsável por Tecnologia da Informação da FORESEA disponibilizar e gerir os sistemas de gerenciamento de identidade e de controles de acessos lógicos aos sistemas e à rede para minimizar riscos de acesso não autorizado a informações.

O proprietário do ativo da informação normalmente é a pessoa que opera o *ativo* e quem assegura que a *informação* relacionada a este *ativo* está protegida. Cabe ao proprietário do ativo da informação aprovar toda solicitação de acesso, revogação e o monitoramento da informação, Infraestrutura de Tecnologia da Informação e Sistemas de Informação para integrantes e parceiros, em função das necessidades de desempenho de seus Programas de Ação.

O acesso a informações, Infraestrutura de Tecnologia da Informação e Sistemas de Informação deve ser realizado por um usuário (login) pessoal e intransferível, visando garantir a rastreabilidade das ações.

A concessão de acesso a sistemas e à rede corporativa da FORESEA, a partir do ambiente corporativo ou do ambiente externo via acesso remoto, é realizada somente após a aprovação do líder imediato do integrante (ou gestor do contrato do parceiro) e/ou do proprietário do ativo da informação. Todos os privilégios são restritamente alinhados ao desempenho das atividades do usuário pelo tempo que for necessário e são revisados pelo menos a cada 12 meses.

As senhas são pessoais e intransferíveis, cabendo ao integrante a responsabilidade por mantê-las em segurança e preservar seu sigilo. Cabe ao responsável por Tecnologia da Informação definir os parâmetros obrigatórios a utilizar para o gerenciamento de senhas, visando assegurar a confidencialidade, integridade, autenticidade e legalidade das informações.

4.4 Uso da Infraestrutura de Tecnologia Informação e Sistemas de Informação

A Infraestrutura de Tecnologia da Informação e Sistemas de Informação colocada à disposição dos integrantes, prestadores de serviço e parceiros de negócios autorizados, é utilizada somente para o atendimento dos interesses de negócio da FORESEA.

O acesso à internet disponibilizado tem natureza de ferramenta de trabalho e deve ser utilizado para atender aos objetivos dos negócios da empresa. A FORESEA pode bloquear o acesso a websites e aplicações que julgar incompatíveis com o objetivo do negócio, suspeitos ou com reputação duvidosa.

Todos os equipamentos corporativos, tais como desktops, notebooks e dispositivos móveis, sob guarda dos integrantes e parceiros, devem ter implantados os requisitos mínimos de segurança definidos pelo Responsável por Tecnologia da FORESEA para acesso interno e remoto à rede corporativa.

Equipamentos e dispositivos móveis pessoais para acesso aos sistemas corporativos da FORESEA podem ser utilizados desde que sejam cumpridos os requisitos especificados pela Área de Tecnologia da Informação.

Somente softwares homologados pela equipe de Tecnologia da Informação devem ser instalados na Infraestrutura de Tecnologia da Informação da FORESEA, sendo a instalação de responsabilidade exclusiva da equipe de TI. Cabe também à equipe de TI o monitoramento do uso dos softwares nos equipamentos corporativos, visando retirar todo e qualquer software não homologado ou não licenciado.

É proibida qualquer utilização da Infraestrutura de Tecnologia da Informação e Sistemas de Informação da FORESEA para expressar opinião pessoal de qualquer caráter, distribuir ou acessar material protegido por direito autoral, anúncios, piadas, conteúdos pornográficos, correntes de solidariedade, jogos eletrônicos ou conteúdo que viole direitos da FORESEA ou de terceiros.

O acesso e uso de e-mail corporativo com conteúdo pornográfico, pedofilia, que defenda atividades ilegais, que menospreze, deprecie ou incite o preconceito a quaisquer classes, que promova discussão pública sem autorização sobre os negócios da FORESEA ou a qualquer outro conteúdo não aderente ao Código de Conduta da FORESEA são passíveis de aplicação de medidas disciplinares.

O Responsável por Tecnologia da Informação, em conjunto com o Responsável pela Gestão da Informação na FORESEA, define as regras para rotina de criação das cópias de segurança (backup) dos sistemas ou ativos da informação, de forma a garantir a retenção das informações pelos prazos legais estabelecidos e a continuidade das atividades dos negócios.

A administração dos serviços de e-mail e certificados digitais da FORESEA é atribuição do Responsável por Tecnologia da Informação.

Toda a Infraestrutura de Tecnologia da Informação, Sistemas de Informação, computadores e dispositivos móveis estão sujeitos a monitoramento pela FORESEA, estando o integrante ciente de que pode ser auditado a qualquer momento na utilização dos mesmos e responsabilizado por suas ações.

4.5 Proteção da Infraestrutura de Tecnologia da Informação

Cabe ao Responsável por Tecnologia da Informação da FORESEA:

- Garantir que sejam aplicadas boas práticas de segurança da informação na aquisição de equipamentos e sistemas, na configuração do ambiente, testes preventivos, revisões periódicas e no treinamento, tanto da equipe de Tecnologia quanto dos integrantes da

FORESEA, a fim de prevenir perda de dados e ataques externos ao ambiente corporativo;

- Prevenir qualquer acesso físico e lógico não autorizado, riscos de danos ou interferências nos recursos de processamento das informações;
- Definir os processos e meios de monitoramento que certifiquem que somente agentes autorizados acessam os ambientes da FORESEA;
- Definir e administrar os firewalls, equipamentos indispensáveis para assegurar o acesso lógico ao ambiente corporativo.
- Proporcionar barreiras físicas e acesso controlado, por meio de sistemas e mecanismos de segurança apropriados, aos locais dedicados à instalação de equipamentos de Tecnologia da Informação críticos da FORESEA, incluindo Data Centers e Centro de Processamento de Dados.

4.6 Segurança com Fornecedores e Parceiros de Negócio

Os requisitos de segurança da informação para prevenir e/ou mitigar riscos associados ao acesso de fornecedores e parceiros de negócios aos ativos da FORESEA devem ser formalmente acordados e documentados.

O integrante responsável pelo contrato endereça os riscos de segurança da informação em cada contratação, consultando o Responsável por Tecnologia da Informação da FORESEA a respeito dos riscos de segurança e controles a serem utilizados para prevenção e/ou mitigação, sempre que necessário.

4.7 Aquisição, Desenvolvimento e Manutenção de Sistemas

Os requisitos de segurança da informação devem ser parte integrante de todo o ciclo de vida dos sistemas de informação desde a aquisição, desenvolvimento de novos sistemas e/ou melhoria dos sistemas existentes.

Qualquer atividade que envolva o ciclo de vida dos sistemas de informação deve ser avaliada, homologada e aprovada pelo Responsável por Tecnologia da Informação da FORESEA.

4.8 Rescisão de Contratos de Trabalho

Em casos de rescisão de contrato de trabalho, o integrante devolverá para a equipe de Tecnologia da Informação todos os dispositivos de Tecnologia da Informação (celular, notebook, tablet, etc.) que estiverem sob sua posse. Antes de efetivar a rescisão do contrato do integrante, a equipe de Pessoas assegura junto à equipe de Tecnologia da Informação que os equipamentos foram devolvidos.

4.9 Plano de Continuidade de Serviços de TI

Cabe ao Responsável por Tecnologia da Informação da FORESEA implantar medidas para que os serviços críticos de TI possuam um plano de continuidade para mitigar indisponibilidade e perda de dados em caso de incidente, assegurando a continuidade das ações para cumprimento dos compromissos da empresa.

4.10 Disposições gerais

Se houver dúvida sobre o conteúdo da Política sobre Tecnologia e Segurança da Informação, o integrante não pode se omitir e deve procurar esclarecimento por intermédio de seu líder direto ou, se necessário, por intermédio da equipe de Tecnologia da Informação da FORESEA.

Integrantes, estagiários e empregados temporários que violem ou tentem violar as orientações descritas nesta Política e seus desdobramentos estão sujeitos a aplicação de medidas disciplinares.

Para Terceiros que contrariem o disposto nesta Política e seus desdobramentos, ações cabíveis serão tomadas, podendo, inclusive, acarretar aplicação de penalidades contratuais, encerramento do contrato e acionamento legal de reparações por prejuízos sofridos pela FORESEA.

4.11 Ciência e Certificação

Todos os integrantes da FORESEA e demais públicos de abrangência deste documento deverão ter ciência desta Política sobre Tecnologia e Segurança da Informação em, no máximo, 90 dias após a data de sua aprovação.

5 RESPONSABILIDADES

5.1 Integrantes

- Devem estar familiarizados e agem em conformidade com esta política quando da criação, recepção, gestão, armazenamento e descarte de dados, registros e informações da FORESEA;
- Preservam a integridade e guardam sigilo de dados e informações de que fazem uso, bem como zelam e protegem os respectivos recursos de processamento de informações;
- Mantêm o caráter sigiloso das senhas de acesso aos recursos e sistemas de Informação da FORESEA;
- Não devem compartilhar, sob qualquer forma, dados e informações sigilosas com outros que não tenham a devida autorização de acesso;
- Não devem violar a legislação pertinente aplicada a cada país onde a FORESEA atua;
- Protegem no nível físico e lógico, e zelam pelos ativos que armazenam ou processam dados da FORESEA;

- Devem comunicar imediatamente, ao seu líder e/ou através do Canal Linha de Ética, o conhecimento de qualquer irregularidade ou desvio (incidente de segurança) desta Política.

5.2 Líderes

- Devem comunicar e incentivar os seus liderados sobre a importância da proteção aos dados e às informações da FORESEA e asseguram a observância das orientações e regras dispostas neste documento;
- Sempre que questionados, devem reportar ao Responsável por Tecnologia da Informação da FORESEA sobre a segurança da informação em seus negócios, áreas e sobre seus liderados.

5.3 Grupo de Trabalho em Segurança da Informação

- Trata das questões ligadas à Segurança da Informação da FORESEA, assegurando o alinhamento e cumprimento desta Política, além de analisar eventuais infrações a esta Política cometidas por Integrantes e/ou parceiros.

5.4 Responsável por Tecnologia da Informação

- Desenvolve e mantém atualizada a Política sobre Tecnologia e Segurança da Informação e os desdobramentos desta;
- Lidera o Grupo de Trabalho em Segurança da Informação e orienta o Presidente, Vice-Presidentes e demais líderes da FORESEA;
- Promove ações de conscientização e treinamentos desta Política e seus desdobramentos;
- Reporta sobre o desempenho de Tecnologia e da Segurança da Informação da FORESEA para o COMEX e para o CA-FORESEA, por meio de comitê de assessoramento específico.

5.5 Responsável pela Gestão da Informação

- Desenvolve e mantem atualizadas as diretrizes e demais desdobramentos desta política, visando orientar a ação do Responsável por Tecnologia da Informação, líderes e demais integrantes.
- Responde como encarregado pelo tratamento de dados pessoais da FORESEA, assumindo como tal as responsabilidades estabelecidas na Lei Geral de Proteção de Dados.

6 DOCUMENTOS DE REFERÊNCIA

- ABNT ISO/IEC 27001:2013.
- ABNT ISO/IEC 27002:2013.
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD).
- Código de Conduta FORESEA.

7 MAPAS DE PROCESSOS DE REFERÊNCIA

NA

8 ANEXOS

NA