POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Sumário

1. Ficha de Controle

Título	Política de Segurança da Informação e Cibernética
Versão	PSIC_V1
Status	Em vigência
Aprovador	Diretoria
Data de aprovação	06/12/2022
Data de Próxima da política	(01 ano após a data de aprovação)
Escopo de abrangência	Finlev
Escopo geográfico	República Federativa do Brasil

Versão	Motivo de Alteração	Data	Autor	Departamento
1.0	-	06/12/2022	CTC CONSULTORIA	Prestador de Serviços Externo

2. Objetivos

A presente política visa definir diretrizes referentes à Segurança da Informação e Cibernética da Finlev, para tratar requisitos de autenticidade, irretratabilidade, integridade, disponibilidade, confidencialidade e privacidade, por meio de orientações sobre o manuseio, trato, controle e proteção das informações durante todo o seu ciclo de vida contra destruição, modificação e/ou divulgação indevida e acessos não autorizados, sendo acidentais ou intencionais.

Esta política está de acordo com as demais políticas e diretrizes estabelecidas na instituição, regras de conduta, sua missão, visão e valores institucionais. O regulamento aqui descrito foi inteiramente desenvolvido e aprovado pela Diretoria da Finlev, cabendo-lhe todo e qualquer direito aos conteúdos aqui veiculados. No surgimento de quaisquer dúvidas, o leitor poderá entrar em contato com a Diretoria da instituição através do endereço eletrônico: vania.trindade@finlev.com.br

3. Vigência

Esta política entra em vigor na data de sua publicação, tendo sua vigência por prazo indeterminado, devendo ser revisado e aprovado pela Diretoria anualmente ou em prazo inferior, no caso de alteração de legislações aplicáveis, ou se houver alguma alteração das práticas operacionais da Finlev, ou ainda quaisquer eventos que justifiquem, no entender da Diretoria, a necessidade de atualização deste documento.

Após aprovada pela Diretoria, esta política será divulgada internamente e disponibilizada via “Intranet – rede interna” da instituição.

4. Público Alvo

Esta política deverá ser direcionada a todos os colaboradores da Finlev e prestadores de serviços terceirizados (quando aplicável), para que desempenhem suas atribuições respeitando as diretrizes estabelecidas em segurança da informação e cibernética da instituição.

A Diretoria da Finlev exige que todos os componentes da estrutura organizacional, funcionários, colaboradores terceirizados e outros sujeitos à observância deste documento, pautem suas atividades profissionais, mantidas interna ou externamente, com base nesta presente política.

A ciência do contido na Política de Segurança da Informação e Cibernética pelos componentes da estrutura organizacional será evidenciada por meio de assinatura do "Termo de Ciência e Responsabilidade".

5. Disposições Gerais

As diretrizes estabelecidas pela Diretoria da Finlev nesta Política de Segurança da Informação e Cibernética estão de acordo com os valores institucionais da empresa. Esta política, além de basear-se na regulamentação em vigor, baseia-se também nos pilares/diretrizes definidos na Missão, Visão e Valores da Finlev conforme demonstrado abaixo.

5.1. Missão, Visão e Valores da Empresa

Missão:

Democratizar o acesso ao crédito direto com agilidade e sensibilidade à realidade de pessoas e empresas, competindo para o desenvolvimento das regiões onde atua, realizando o sonho de consumo dos nossos clientes, com consciência e educação financeira.

Visão:

Ser plenamente reconhecida como uma fintech sólida de concessão de crédito direto no mercado regional, e nacionalmente, como uma fintech pioneira da Região Norte a oferecer um amplo leque de serviços do mercado financeiro aos clientes.

Valores:

6. Introdução

Com base na Lei 13.709/18, Resolução CMN 4.658/18, Resolução CMN 4.752/19 e Circular 3.909/18, as instituições financeiras e demais instituições autorizadas a funcionar pelo BACEN devem implementar definidos em Políticas procedimentos em segurança da informação e cibernética. Nesse sentido foi elaborada a presente Política de Segurança da Informação e Cibernética.

Está Política tem por diretrizes:

a) Orientar as ações de comportamento e segurança, minimizando riscos contra a integridade, sigilo e disponibilidade da informação e dos seus elementos constituintes;

b) Estabelecer um ideário para as práticas funcionais, de forma que estejam de acordo com as responsabilidades da instituição, relacionadas com as regulamentações ou leis que regem a utilização de recursos computacionais, incluindo a definição de padrões de segurança em tecnologia da informação que visem garantir a continuidade operacional do negócio;

c) Conscientizar os colaboradores a protegerem diligentemente os ativos de informação;

d) Estabelecer diretrizes que possam responder às mudanças dos negócios, da legislação, das normas regulatórias e da tecnologia;

e) Servir de referência para auditorias, verificações de conformidade e determinação de responsabilidades.

7. Governança de Segurança da Informação

As informações geradas internamente, adquiridas no mercado ou absorvidas pela Finlev são consideradas patrimônio, devendo ser tratadas como ativo e confidencial. No caso de exceção, informações cuja divulgação seja obrigatória ao mercado e clientes por exigência de órgãos reguladores devem ser cuidadosamente avaliadas e passar por autorização da Diretoria. Tal autorização deve ser respeitada durante todo o ciclo de vida desta informação.

A infraestrutura de tecnologia da informação da Finlev mantém mecanismos e repositórios para manutenção de trilhas de auditoria, logs e demais notificações de incidentes. A área de Segurança da Informação é acionada a qualquer tentativa de violação que seja informada ou detectada, tomando as medidas cabíveis para prover uma defesa ativa e corretiva contra os ataques empreendidos e mecanismos ou incidentes que os envolvam.

Qualquer colaborador da Finlev que for autorizado a participar de entrevistas e assemelhados deverá restringir-se a fazer comentários estritamente técnicos, precisos e completos, evitando-se o uso de juízos de valor desnecessários e qualquer comentário que possa ser considerado discriminatório. As declarações prestadas devem ser pautadas pela precisão terminológica e extrema cautela na divulgação de informações sensíveis.

A informação de terceiro que estiver provisoriamente sob custódia da Finlev deve ser tratada e mantida, com os mesmos cuidados, respeitando o nível de confidencialidade que o proprietário recomendar.

A Tecnologia da Informação e seus ativos envolvidos nos negócios da Finlev devem ser preservados e mantidos a fim de deter sempre o controle sobre a informação.

A Tecnologia da Informação utilizada nos negócios da Finlev deve possuir documentação que permita a continuidade e o controle, independentemente de ter sido desenvolvida internamente ou por terceiros.

São expressamente proibidas ligações telefônicas, envio de e-mails, mensagem de texto e mensageria instantânea e/ou afins, campanhas de doações de valores para débitos em nome ou titularidade da Finlev.

Os responsáveis pela segurança da informação e ativos tecnológicos devem desenvolver e usar mecanismos que protejam e garantam a continuidade dos processos. A necessidade e o tipo de contingência serão determinados com base na importância para o negócio e o tempo de indisponibilidade aceitável para este recurso, sem afetar a continuidade dos negócios da Finlev. A definição dos critérios de importância e tempo aceitável de indisponibilidade é de responsabilidade do gestor da informação.

O acesso aos recursos da informação deve ser controlado e liberado através de autorização formal solicitada pelo gestor da pessoa que necessite dos recursos. Essa autorização formal é solicitada no preenchimento da ficha de admissão ou quando for necessária a disponibilização da informação.

Todos os recursos da informação, sejam eles tecnológicos ou não, devem ser utilizados exclusivamente para o desenvolvimento de atividades profissionais referentes aos negócios da Finlev.

A identificação do usuário deve permitir o seu claro reconhecimento e, no caso de credenciais de acesso a sistemas e ativos tecnológicos, deve ser único, pessoal e intransferível. Eventuais danos e incidentes causados pelo uso indevido de credenciais de acesso e identificação, mesmo por parte de terceiros, serão de inteira responsabilidade do dono da credencial, incluído crachás, certificados digitais, tokens e senhas.

Todos os recursos da informação devem ser aprovados e homologados para uso. O processo de homologação deve considerar a padronização para permitir substituição em caso de falha, garantindo a continuidade dos processos e o atendimento às necessidades existentes. A aprovação da homologação, autorizando o uso em produção é de responsabilidade da área que o administra.

Todos os recursos da informação devem ser devidamente inventariados conforme suas características, de tal maneira que possam ser identificados de forma individual e única. Este processo de inventário deverá ser atualizado periodicamente, a fim de garantir a sua consistência.

Os recursos da informação homologados e autorizados para uso deverão ser de propriedade da Finlev ou ter seus direitos de uso cedidos, arrendados ou alugados. Tais recursos devem, obrigatoriamente, estar em conformidade com a legislação brasileira vigente.

Não deve ser utilizado dentro das dependências da Finlev nenhum recurso da informação de procedência pessoal, mesmo que para fins profissionais, à exceção de recursos previamente autorizados pela área de Segurança da Informação e/ou pela Diretoria, devidamente auditados e monitorados.

Toda informação que deixe de ter utilidade para a Finlev deverá ser destruída, sem possibilidade de recuperação antes de seu descarte com base nos seguintes procedimentos:

a) Caso não seja possível garantir a destruição sem que haja a possibilidade de recuperação de dados, o armazenamento desta informação deverá ser previamente criptografado e, ao término de sua utilidade, as chaves de criptografia deverão ser destruídas sem que haja possibilidade de recuperação;

b) Exceções deverão ser tratadas e aprovadas pela área de Segurança da Informação.

A segurança das informações contidas em qualquer equipamento portátil utilizado deverá seguir, no mínimo, os mesmos cuidados dos equipamentos equivalentes em uso internamente na empresa. A segurança física do equipamento portátil será de responsabilidade do seu usuário, e este deve respeitar as orientações fornecidas por quem disponibilizar tal recurso.

Ao final do expediente e sempre que necessário ausentar-se da mesa de trabalho, todos os colaboradores devem ter o cuidado de bloquear/desligar seus computadores e guardar documentos confidenciais em local fora da visão e alcance de pessoas não autorizadas. Deve-se também evitar conversas sobre informações sigilosas em ambientes onde a confidencialidade da informação não poderá ser garantida.

O acesso físico às dependências da Finlev é determinado por faixas de horários e dias da semana. É concedido conforme cargo e função do colaborador. Em algumas ocasiões, exceções são feitas pelos gestores e o acesso é concedido através do registro e aprovação pela área de Segurança da Informação ou do diretor responsável.

O acesso como administrador aos sistemas em nuvem de ambientes produtivos ou que possuam ativos críticos do qual fazem gestão de infraestruturas, plataformas e softwares/funções, como serviço, devem ser restritos aos administradores da Nuvem. Qualquer tipo de exceção deverá ser previamente autorizado pela equipe de Segurança da Informação.

Caso algum colaborador perceba o descumprimento de alguma das diretrizes da Política de Segurança da Informação e Cibernética, deverá comunicar seu superior direto e este à área de Segurança da Informação e/ou a Diretoria da Finlev.

O não cumprimento das diretrizes da Política de Segurança da Informação e Cibernética, seja intencional ou não, sujeita o colaborador a sanções administrativas, definidas de acordo com o grau de importância do incidente.

8. Controle de Acesso Lógico

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal e deve respeitar as seguintes premissas:

a) Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos). Orienta-se a não utilizar como senha informações pessoais fáceis de serem obtidas, tais como, nome, número de telefone ou data de nascimento;

b) Utilizar um método próprio para lembrar-se da senha, caso necessário, utilizar sistemas de cofre de senha aprovados pela área de Segurança da Informação;

c) Não incluir senhas em processos automáticos de acesso ao sistema, como por exemplo, armazenadas em macros ou teclas de função.

Todas as senhas geradas pela área de TI (Tecnologia da Informação), sejam elas de um novo acesso ou quando bloqueadas, devem ser alteradas pelo colaborador/usuário cadastrando uma nova senha conforme os padrões estabelecidos pela TI.

Além disso, os usuários devem alterar a senha de rede a cada 90 (noventa) dias, sendo que o sistema irá enviar notificações de necessidade de alteração 10 (dez) dias antes da sua expiração.

9. Estações de Trabalho

As estações de trabalho disponibilizadas para o usuário tem por objetivo o desempenho das atividades profissionais do colaborador/usuário na organização.

As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidas contra danos ou perdas, bem como o acesso, uso ou exposição indevida.

A integridade física e o perfeito funcionamento da estação de trabalho são de responsabilidade do colaborador/usuário, seguindo as regras e orientações fornecidas pela área de infraestrutura.

São responsabilidades do usuário/colaborador:

a) Encerrar a estação de trabalho no final do expediente, desligando o equipamento;

b) Quando ausentar-se da mesa, o usuário/colaborador deverá bloquear a estação de trabalho e ativá-la com sua senha de acesso (Obs. Esta ação aplica-se a todos os usuários/colaboradores com estações de trabalho, incluindo equipamentos portáteis);

c) Caso o usuário/colaborador não realize o bloqueio da estação de trabalho, será bloqueada automaticamente após um período inativa;

d) Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo a Finlev, só devem ser utilizadas em equipamentos com controles adequados.

10.Desenvolvimento e Implantação

A Finlev trabalha com a possibilidade de adquirir ou desenvolver seus sistemas internamente. É de responsabilidade da equipe de desenvolvimento garantir que os sistemas desenvolvidos ou adquiridos possuam:

a) Os requisitos solicitados por órgãos reguladores e pelas regras de conformidade interna da instituição;

b) Sistema de autenticação que obedeçam às regras de senha da empresa;

c) Segregação de acessos;

d) Trilhas de auditoria;

e) Acesso garantido ao Banco Central do Brasil, quando necessário;

f) Alta disponibilidade;

g) Restrição e controle do código fonte dos sistemas;

h) Proteção contra malwares e vírus e ataques comuns de rede;

i) Processo de gestão de mudança da instituição;

j) Sistemas disponibilizados em redes públicas deverão:

- Possuir conexões criptografadas;
- Proteção contra negação de serviço;
- Bloqueio de ataques contra aplicações web;
- Segundo fator de autenticação (SMS, push, restrição por IP ou token).

As equipes de Infraestrutura e Operações de TI deverão garantir o bom funcionamento e a integridade através das seguintes atividades:

a) Publicação de novas versões das aplicações;

b) Corrigir incidentes comuns ao sistema e documentar eles;

c) Monitorar a disponibilidade;

d) Controlar as licenças de uso e renovação dos sistemas adquiridos;

e) Efetuar as restrições de acesso à rede;

f) Atuar no processo de resposta a incidentes, quando necessário;

g) Rotinas de cópia de segurança;

h) Quando adquiridos, garantir que seja notificado sobre qualquer limitação sobre os serviços ou sistema contratado.

A Segurança da Informação deverá:

a) Revisar a arquitetura e conformidade dos sistemas antes de serem implantados em produção;

b) Efetuar buscas por falhas de segurança (vulnerabilidades) regularmente;

c) Monitorar o acesso ao banco de dados, sistemas e servidores;

d) Treinar a equipe de operações e manter o processo de resposta a incidentes atualizado;

e) Detectar e tratar possíveis incidentes de segurança da informação;

f) Não permitir que os dados sejam utilizados para funções que não tenham sido previamente aprovadas pelo cliente ou pelo órgão regulador (Banco Central do Brasil, CMN, dentre outros);

g) Conceder acesso irrestrito ao Banco Central do Brasil sobre os dados, informações de processamento e copias de segurança, caso necessário em due diligences presenciais ou solicitações remotas via SISCOM;

h) Plano de recuperação de desastres;

i) Quando adquiridos, deve também:

- Garantir que o fornecedor forneça a cópia e a exclusão dos dados ao solicitar o cancelamento do serviço ou sistema;
- Ser notificado sobre incidentes que tenham ocorrido, assim como também sob o seu tratamento;
- Garantir que o compartilhamento de informações confidenciais com terceiros seja restrito mediante a aprovação da equipe de Segurança da Informação;
- Conceder acesso ao Banco Central a contratos e acordos prestados.

11.Instalação de Software e Hardware

Toda instalação de software e hardware deve ser feita pela área de Tecnologia da Informação, sendo que todos os softwares e hardwares devem ser homologados e licenciados. Qualquer software que, por necessidade do serviço, precisar ser instalado, deverá ser homologado pela área de TI e só assim serem disponibilizados para a área requerente.

A Finlev respeita os direitos autorais dos softwares que utiliza e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) pela Finlev.

Toda aquisição e manutenção de sistema devem zelar pela observância dos princípios de controle sobre informações processadas e armazenadas, incluindo a adequada segregação de perfis de acesso e ao controle de vazamento de informações. Após a aquisição e implantação do novo hardware e software, será atualizado o bem no Inventário de TI e nos controles de licenças de software.

A habilitação de usuários para uso dos softwares de rede ou em nuvem será realizado mediante senha de acesso. Dependendo da criticidade do sistema a área de Segurança da Informação, poderá solicitar a obrigatoriedade do uso de um MFA (“Multifactor Authentication”) e/ou restrição por IP, garantindo o sigilo e controle dos dados. A área de Segurança da Informação poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso.

12.Trilha de Auditoria

A trilha de auditoria estabelece as regras para que os sistemas computacionais que suportam os processos de negócio registrem todos os eventos relevantes ocorridos durante a realização de atividades fins, possibilitando a identificação de autores de atividades ou diagnósticos dos sistemas utilizados pela Finlev.

Todos os sistemas transacionais ou de sustentação assim como os seus recursos de conectividade, devem conter trilhas de auditoria suficientes para assegurar o rastreamento de eventos, incluindo: Identificação do usuário, data e horário de ocorrência do evento e identificação do evento (inclusão, alteração, exclusão).

Para os sistemas eletrônicos de negociação, os eventos das trilhas de auditoria devem ser suficientes para assegurar o rastreamento do cliente, da origem da oferta (IP do usuário e/ou de outros que permitam identificação da origem), do profissional de operações (quando aplicável), do ativo, das condições de negociação e da sessão de negociação utilizada.

A rede interna de computadores e os sistemas eletrônicos de negociação devem conter trilhas de auditoria com registro dos acessos de entrada e saída (usuário, data e horário). O período de retenção das trilhas de auditoria deve ser de, no mínimo, 05 (cinco) anos. Os sistemas devem registrar eventos ou gerar logs sempre que uma das seguintes atividades for realizada:

a) Criar, ler, atualizar ou excluir informações confidenciais, incluindo informações de autenticação, como senhas;

b) Criar, atualizar ou excluir informações não cobertas pelo item anterior;

c) Uma conexão de rede for iniciada;

d) Uma conexão de rede for aceita;

e) Autenticação e autorização do usuário para atividades relacionadas aos itens em “A” ou “B”, bem como, o login/logout do usuário;

f) Conceder, modificar ou revogar os direitos de acesso, incluindo a adição de um novo usuário ou grupo, mudar níveis de privilégio de usuário, alteração de permissões de arquivos, alteração de permissões de objeto de banco de dados, alteração das regras de firewall e as alterações de senha do usuário;

g) Mudanças na configuração do sistema, rede ou serviços, incluindo a instalação de patches de correção ou atualizações que provoquem alteração do software;

h) Inicialização, desligamento ou reinício do processo de aplicação;

i) O processo de aplicação for suspenso, falhar ou finalizar de forma anormal, especialmente devido ao esgotamento de recursos ou atingir um limite (CPU, memória, conexões de rede, largura de banda de rede, espaço em disco ou outros recursos), a falha de serviços de rede, como DHCP ou DNS, ou falha de hardware;

j) Detecção de atividade suspeita / mal-intencionada, como por exemplo, Sistema de Detecção ou Prevenção de Intrusão (IDS / IPS), sistema antivírus ou anti-spyware.

12.1 Registros que devem conter nos “Logs”

Esses registros devem identificar ou conter pelo menos os seguintes elementos, direta ou indiretamente:

a) Tipo de ação - (exemplos como autorizar, criar, ler, atualizar, excluir e aceitar a conexão de rede);

b) Subsistema executando a ação - (exemplos como incluir o nome do processo ou da transação, o processo ou o identificador da transação);

c) Identificadores, relacionado ao contexto específico da ação solicitada - (exemplos como nome do usuário, nome do computador, endereço IP e endereço MAC.). Esses identificadores devem ser padronizados para facilitar a correlação do log;

d) Identificadores, relacionado ao objetivo específico da ação solicitada - (exemplos como nomes de arquivos acessados, identificadores exclusivos de registros acessados em um banco de dados, parâmetros de consulta usados para determinar os registros acessados em um banco de dados, nome do computador e endereço IP). Tais identificadores devem ser padronizados em todos os sistemas para facilitar a correlação de logs;

e) Valores - registro de valores antes e depois quando a ação envolve a atualização de um elemento de dados;

f) Data e hora - registro de data e hora em que a ação foi realizada;

g) Ação - se ação foi permitida ou negada pelos mecanismos de controle de acesso;

h) Descrição ou código de ação - descrição ou código informando a razão pelo qual a ação foi negada pelo mecanismo de controle de acesso, quando aplicável.

13.Uso de Mídias Removíveis, da Internet e E-mail

13.1 Mídias Removíveis

O uso de mídias removíveis na Finlev não é estimulado, devendo ser tratado como exceção à regra. As mídias removíveis são o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, nesse caso, os modens 4G e pen-drives merecem especial atenção. Para liberação de mídias removíveis dos desktops e notebooks, é necessário justificar o uso e aprovação da área de Segurança da Informação.

13.2 Uso da Internet

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa. O acesso às páginas e web sites é de responsabilidade de cada usuário, ficando vedado o acesso a sites com conteúdo impróprio e páginas de relacionamento. Os acessos à internet são monitorados através de identificação e autenticação do usuário.

13.3 Uso de E-mail

É vedado o uso de sistemas e-mail externos não pertencentes à Finlev. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através sistema oficial da empresa. É proibido o uso do correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro. Deve-se evitar utilizar o e-mail da empresa para assuntos pessoais.

Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas (.bat, .exe, .src, .lnk e .com), ou de quaisquer outros formatos alertados pela área de TI.

Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, entre outros.

14.Configuração de Senhas

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal. Utilizar um método próprio para lembrar-se da senha, ou, se necessário, solicitar um sistema de cofre de senhas digital que seja aprovado pela área de Segurança da Informação. O padrão de senhas dos sistemas internos da Finlev deverá ser um só:

a) Número Máximo de Tentativas de Acesso ao Sistema, 3 tentativas;

b) Desbloqueio para ser feito somente pelo administrador do sistema;

c) Troca a cada 90 (noventa) dias;

d) Não ser igual ao nome da conta;

e) Não ter mais de dois caracteres consecutivos como parte da senha;

f) Ter pelo menos seis caracteres;

g) Deve ser diferente das últimas 6 senhas;

h) Complexibilidade de: no mínimo, dois dos itens a seguir – letras maiúsculas e minúsculas, símbolos e números;

i) Armazenado de forma criptografada.

15.Monitoramento

Todos os colaboradores da Finlev possuem o monitoramento dos seguintes canais:

a) Ramais telefônicos:

b) E-mails;

c) Acesso à internet.

É efetuada a verificação do funcionamento dos monitoramentos feitos, por amostragem semanalmente.

16.Segregação e Gestão de Acessos

A segregação de funções da Finlev é criada usando os departamentos atrelados as funções executadas, facilitando assim a análise de conflitos de interesse e qualquer possível falha de concessão acesso.

A segregação de acessos lógica e física irá aplicar as análises feitas pela segregação de funções nos sistemas e ambientes físicos e virtuais da Finlev.

As análises feitas pela segregação de funções consideram o máximo de acesso que um colaborador pode ter, porém a segregação de acessos poderá ter acessos mais restritos, a fim de proteger o processo de erros comuns que podem ser causados por colaboradores que não possuem conhecimentos plenos dos processos.

17.Mudanças e Aprovações do Processo

Esta norma estabelece que os processos de segregação de funções, acessos físicos e lógicos são atividades operacionais contínuas e que devem ser atribuídas as análises e aprovações para da Diretoria a fim de manter a conformidade do processo de forma ágil.

A Segurança da Informação deverá manter o versionamento do mapa de Segregações de Funções e Acessos Físicos e Lógicos que foram aprovados, assim como também as suas atas, pelo prazo mínimo de 5 (cinco) anos.

18.Acesso Remoto

A Finlev permite o acesso remoto pelos Colaboradores em posições chave, conforme determinação da Diretoria de acordo com a seguinte regra - o Colaborador deve ser devidamente cadastrado no grupo de segurança do firewall, ter o certificado instalado em seu computador e conectar-se através de uma VPN. Ademais, os Colaboradores autorizados são instruídos a:

a) Manter softwares de proteção contra malware/antivírus nos dispositivos remotos;

b) Relatar a Tecnologia da Informação qualquer violação ou ameaça Finlev durante o trabalho remoto;

c) Não armazenar informações confidenciais ou sensíveis em dispositivos pessoais.

19.Gestão de Acessos

19.1 Credenciamento

O credenciamento dos novos colaboradores deverá ser feito pelos administradores dos sistemas obedecendo as regras estabelecidas nos documentos vigentes de segregação de acesso aprovados pela Diretoria.

19.2 Descredenciamento

O descredenciamento dos colaboradores ocorre no processo de desligamento ou término de contrato, não se importando o motivo da ocorrência. Todos os acessos devem ser removidos pelo menos até ao final do dia.

19.3 Troca de Departamento pelo Colaborador

Entendemos que a troca de departamentos pode ocorrer de forma súbita para suprir ocorrências emergências, portanto é permitido que acúmulo de dois perfis de acesso para o mesmo colaborador desde que não existam conflitos de interesse nos acessos. A adequação destes acessos deve ocorrer em um período máximo de 60 (sessenta) dias.

19.4 Novos Acessos ou Novos Sistemas

A entrada de novos sistemas ou a necessidade de alterações dos acessos por mudanças sistemáticas ou ambientais podem ocorrer sem que tenha tempo hábil para uma análise formal da Diretoria. Nesses casos, a equipe de Segurança da Informação terá autonomia para decidir as melhores estratégias de acessos até que seja revisado e aprovado formalmente pela Diretoria.

19.5 Ambientes Lógicos de Homologação, Pré Produção e Reprodução

A segregação de funções e acessos estende-se também a processos de tecnologia, garantindo que não existam conflitos de interesses e falta de integridade dos sistemas em produção.

19.6 Contas de Serviço

Contas de serviços (ou contas sistêmicas) são credenciais de acessos criados nos sistemas e utilizados para integração de serviços e sistemas entre si. Essas integrações são utilizadas para automatizações e uso de componentes externos. Estas contas não devem ser utilizadas pelos colaboradores. Haverá responsáveis diretos por cada conta criada e responderam por qualquer infração causada por ela. A equipe de segurança da informação deverá manter monitoramentos de uso sobre estas contas.

20.Revisão de Acessos

A equipe de Segurança da Informação deverá pelo menos a cada 6 (seis) meses executar revisões completas sobre os acessos concedidos aos sistemas e ambientes da Finlev. Caso na revisão se identificado conflito nos acessos concedidos, e por questões internas a Diretoria entender que deverá manter tais acessos, caberá a Diretoria a aprovação destes acessos conflituosos.

21.Backup

O backup deve possuir uma rotina de armazenamento que obedeça às orientações e estratégias descritas neste documento de tempo de retenção, confidencialidade e integridade da informação. O processo de restauração do backup também deve atuar em tempo hábil que possa atender a necessidade do negócio relacionado a incidentes e desastres.

Todas as rotinas de backup devem manter um registro de sua execução por um período de pelos menos 05 (cinco) anos. Em caso de falhas na execução, o incidente deve ser documentado, corrigido e notificado à Segurança da Informação.

21.1 Restauração do Backup

O processo de restauração deve ser atendido em tempo hábil, que deverá ser definido entre a área de negócios e tecnologia a fim de minimizar incidentes ou desastres operacionais.

Somente a área de Segurança da Informação, diretores e proprietários das informações podem pedir a restauração dos dados.

22.Testes de Restauração de Dados

A equipe de Infraestrutura deve ser executar testes de restauração de dados pelo menos a cada 06 (seis) meses. Todos os testes devem ser documentados e evidenciados a integridade dos arquivos restaurados.

23.Gestão de Mudanças

O processo de Gestão de Mudanças deve:

a) Garantir que as mudanças críticas foram testadas antes de serem executadas em ambientes de produção, sempre que possível;

b) Descrever o processo de execução retorno da mudança, caso tenha algum erro na execução ou o resultado não seja o esperado;

c) Existir uma análise prévia e adequada do impacto e risco da mudança para o negócio;

d) Garantir a integridade, organização e controle das mudanças que foram executadas.

24.Resposta a Incidentes

Um plano de resposta a incidentes deve incluir procedimentos para detectar, responder e para limitar os efeitos de um incidente de segurança. A equipe de Segurança da Informação deve analisar constantemente possíveis falhas ou incidentes de Segurança que possam ocorrer na Finlev, assim como também em seus parceiros/fornecedores críticos e criar possíveis planos de resposta para esses incidentes.

Considera-se que existam planos para os incidentes abaixo, mas não se restringindo somente a eles:

a) Ataques de negação de serviço;

b) Infecção por “malwares” ou códigos maliciosos;

c) Vazamento e/ou roubo de Informação;

d) Roubo de ambientes virtuais ou “cryptoLockers”;

e) “Phishing” ou páginas falsas do site da instituição;

f) Fornecedores críticos inoperantes.

24.1 Estrutura do Plano de Resposta a Incidentes

O plano de resposta a incidentes deve ser composto por 06 processos:

a) Preparação - preparar usuários e staff para lidar com potenciais incidentes que possam surgir;

b) Identificação - determinar se um evento é verdadeiramente um incidente de segurança;

c) Contenção - limitar o dano do incidente e isolar os sistemas afetados para evitar mais danos;

d) Erradicação - encontrar a causa raiz do incidente, removendo os sistemas afetados do ambiente de produção;

e) Recuperação - permitir aos sistemas afetados que retornem ao ambiente de produção, garantindo que nenhuma ameaça permanece;

f) Lições Aprendidas - completar a documentação do incidente, realizando uma análise para se aprender com o incidente e potencialmente melhorar os esforços futuros de detecção, prevenção e resposta.

25.Disposições Finais

A presente política foi redigida com o objetivo de estabelecer as diretrizes e regras/orientações a serem observadas e fidedignamente respeitadas pelos colaboradores e terceirizados da instituição, quanto à Segurança da Informação e Cibernética da Finlev.

Assim, torna-se proibitivo qualquer desvirtuamento infundado às normas aqui instituídas, mesmo que de forma involuntária, dado que todos os procedimentos e atividades devem ser executados com diligência e responsabilidade. Em casos fortuitos ou nos quais a excepcionalidade da matéria exija, poderá haver tratamento distinto ao convencionado neste código, necessitando, para tanto, demonstrações cabais e tangíveis que justifiquem esse tratamento excepcional inclusive com a aprovação da Diretoria.

Por fim, fica desde já determinado que o descumprimento das regras desta política, bem como eventuais descumprimentos de disposições legais e regulatórias, sujeita os colaboradores à aplicação de sanções, que vão desde penalidades administrativas até criminais. Frise-se que a negligência e a falha voluntária, ressaltando a previsão acima citada, são consideradas descumprimento desta política, sendo passível de aplicação de medidas disciplinares previstas na legislação em vigor.