E-INVEST
By PREVIERICSSON

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Conteúdo

ANEXO I – MANUAL DE PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

A presente Política tem como objetivo dispor os pilares, atribuições e procedimentos voltados a garantir a segurança da informação, no âmbito das atividades desenvolvidas pela E-INVEST BY PREVI-ERICSSON.

2. ABRANGÊNCIA

Aplica-se a todos os colaboradores e diretores da E-INVEST, no desempenho de suas respectivas atividades.

3. PILARES

A E-INVEST garante a segurança da informação a partir dos seguintes pilares:

(I) Confidencialidade, para que somente pessoas autorizadas possuam acesso às informações;

(II) Disponibilidade, a assegurar o funcionamento e a utilização plena de sistemas e ativos para as pessoas autorizadas;

(III) Integridade e exatidão das informações, sem modificações de caráter não autorizado, durante toda a cadeia de processamento.

(IV) Autenticidade para de identificação da informação e do usuário de ativos;

(V) Respeito à Privacidade e Proteção de Dados, da inviolabilidade da intimidade, da autodeterminação informativa; da liberdade de expressão e de informação, de comunicação e de opinião; da honra e da imagem; do desenvolvimento econômico, tecnológico e da inovação, em alinhamento estratégico e operacional com a Política de Proteção de Dados.

4. DIRETRIZES

A segurança da informação é tratada pela E-INVEST com a observância das seguintes diretrizes:

Toda informação, gerada, custodiada, manipulada, utilizada ou armazenada, em formato digital ou físico, e seus suportes (sistemas, rede, arquivo, depósitos) será classificada e organizada, a fim de garantir a disponibilidade e confidencialidade das informações.

Independentemente da forma apresentada, compartilhada ou armazenada, os ativos de informação devem ser utilizados apenas para a sua finalidade devidamente autorizada.

As informações devem ter classificação de segurança e medidas de proteção aplicáveis de acordo com critérios estabelecidos quando da sua criação, utilização, custódia e descarte, bem como com o nível de confidencialidade e criticidade para gestão da segurança.

4.1. Controle de Acessos

A **E-INVEST** possui controles aptos a assegurar a confidencialidade da informação, através de gestão de acessos a sistemas, rede corporativa e arquivos físicos, de modo que o acesso seja realizado somente para quem possua permissão para tanto.

4.2. Rastreabilidade

A **E-INVEST** mantém controle de rastreabilidade como logs e trilhas de auditoria, mantendo registro dos acessos e modificações realizadas em arquivos e sistemas utilizados.

Os logs e registros são armazenados e preservados em ambiente seguros, a fim de preservar a cadeia de custódia dos dados mantidos pela **E-INVEST.**

4.3. Segurança cibernética

A **E-INVEST** avalia, monitora e implementa melhorias aos riscos associados às informações que mantém sob sua guarda, como objetivo de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Também são avaliados previamente o risco e o impacto na segurança da informação no desenvolvimento de novos produtos ou reformulação de processos, bem como na contratação de fornecedores quando com estes houver a troca de informações.

4.4. Plano de Continuidade

A **E-INVEST** mantém plano de contingência, visando a garantia absoluta da disponibilidade das informações e a continuidade do negócio, inclusive na ocorrência de incidentes ou ameaças à segurança.

4.5. Propriedade Intelectual

Todas as informações sob guarda da **E-INVEST,** independentemente da origem – se coletada diretamente ou obtida através de terceiros – são consideradas de propriedade intelectual da **E-INVEST,** devendo os colaboradores, utilizarem única e exclusivamente para as finalidades constantes do contrato de trabalho.

Os equipamentos, meios de comunicação e sistemas estão sujeitos a monitoramento, sendo certo que eventuais informações de cunho pessoal tratadas por esses meios serão abrangidas por referido controle, pela sua indissociabilidade.

A utilização indevida de tais informações configura infração ética pelo colaborador e deverá ser encaminhada para o Conselho Deliberativo para determinar a abertura de um processo administrativo.

5. PAPÉIS E RESPONSABILIDADES

Para a eficiência da Segurança da Informação na E-INVEST, é instituída uma rede de responsabilidades a todos os colaboradores da entidade. São estas:

5.1. Dos colaboradores

Zelar pelo sigilo das informações de que faz uso, devendo utilizá-las somente para fins profissionais; não destruir/alterar/modificar equipamentos e instalações; obedecer aos procedimentos constantes do **ANEXO I – MANUAL DE PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO;** comunicar ao seu superior imediatamente qualquer suspeita de incidente de segurança.

5.2. Gestores e Diretores

Zelar pelo sigilo das informações de que faz uso, devendo utilizá-las somente para fins profissionais; não destruir/alterar/modificar equipamentos e instalações; obedecer aos procedimentos constantes do **ANEXO I – MANUAL DE PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO;** comunicar ao seu superior imediatamente qualquer suspeita de incidente de segurança.

5.3. Tecnologia da Informação

Cabe à área de Tecnologia da Informação ou empresa contratada a devida manutenção e suporte de servidores, sistemas e demais recursos tecnológicos utilizados pela E-INVEST; a educação e treinamento dos colaboradores sobre as melhores práticas em segurança da informação; receber as comunicações de incidente e comunicar ao Encarregado de Proteção de Dados (DPO – Data Protection Officier) sobre sua ocorrência, caso envolva dados pessoais.

6. SANÇÕES

Eventuais violações às disposições desta Política serão consideradas e tratadas conforme o Código de Ética da **E-INVEST**, sem o prejuízo da aplicação de sanções previstas na legislação.

7. REVISÕES

A **E-INVEST** revisará periodicamente a sua Política de Segurança da Informação, avaliando se os procedimentos estão de acordo com a legislação aplicável e as melhores práticas disponíveis no mercado.

8. APROVAÇÃO

A presente versão desta Política foi aprovada pela Diretoria Executiva na reunião 10/2020 realizada no dia 29/10/2020.

ANEXO I – MANUAL DE PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

Este Manual tem o objetivo de definir os procedimentos necessários para a garantia da segurança da informação na **E-INVEST.**

2. DEFINIÇÕES

Aplicativo: Conjunto de programas de computador desenvolvidos internamente ou adquiridos de terceiros.

Chamado: É o registro de uma solicitação ou suporte ao usuário que contém todas as informações inerentes ao atendimento, possibilitando seu acompanhamento.

Chave de Acesso: Identificação do usuário no ambiente informatizado.

Documento confidencial: É aquele que, por sua natureza, deva ser de conhecimento restrito e, portanto, requeira medidas especiais para sua segurança.

Equipamentos portáteis: "Laptops" e demais equipamentos com poder de processamentos que possam ser transportados pelo usuário.

Estação de trabalho: Microcomputador utilizado para acesso e manuseio de informações e aplicativos.

Homologação: Processo de avaliação e aprovação técnica de equipamento de informática e de aplicativo que antecede sua aquisição.

Inventário: Levantamento e registro individualizado de equipamentos de informática e de aplicativos.

Lixo informático: Recursos de informação danificados ou obsoletos.

Operação remota: Utilização de aplicativos de produção por usuários devidamente autorizados fora das instalações da E-INVEST com intuito de dar continuidade às atividades desempenhadas.

Rede corporativa: Conjunto de recursos de informação de uso corporativo.

Rede Wireless: Extensão da rede corporativa de dados propagada via tecnologia de ondas de rádio, sem contato físico para acesso.

Senha: Código secreto do usuário que autentica a identidade de uma chave de acesso.

Service Desk: É o serviço de atendimento e suporte ao usuário nos recursos da Tecnologia da Informação.

Terceiros: Funcionários de empresas contratadas que prestam serviços à E-INVEST

Usuário: Pessoa autorizada e capacitada para utilizar os recursos de informação da E-INVEST.

3. PROCEDIMENTOS

3.1. Utilização de Recursos Tecnológicos da E-INVEST

3.1.1. Documentos em papel

Os colaboradores deverão possuir cuidado com a exposição de arquivos em papel. O usuário somente poderá imprimir o documento quando necessário.

Ao se ausentar da estação de trabalho, os colaboradores deverão guardar em local apropriado ou colocar o documento em papel com a face em branco virada para cima.

Ao atestar que um documento ou impressão não será mais necessária, ou após a sua digitalização, o usuário deverá triturar o papel e realizar o seu descarte.

É proibido o uso de papéis para utilização como rascunho, exceto se o papel estiver em branco.

3.1.2. Aplicativos

Somente poderão ser utilizados aplicativos que foram previamente homologados e testados, sendo proibido o uso de aplicativos com a finalidade estranha à atividade desempenhada pela **E-INVEST.**

É necessário estudo prévio sempre que necessária a aquisição, homologação, desenvolvimento e instalação ou remoção de aplicativos nos equipamentos da **E-INVEST.**

É vedada a cópia, alteração ou utilização de quaisquer aplicativos de propriedade ou licenciados à **E-INVEST** cuja finalidade não seja a pretendida.

Quaisquer iniciativas de uso corporativo de aplicativos pela internet ou aplicativos que interagem com provedores externos (nuvem de dados) e que utilizem ou façam integração com dados provenientes ou de propriedade da **E-INVEST,** devem ser homologados o seu uso e padronizar acessos, interfaces e requisitos de segurança da informação.

3.1.3. Equipamentos de informática

Todo equipamento de informática deve ser adquirido mediante homologação prévia. O usuário deve zelar pela conservação dos equipamentos de informática sob sua responsabilidade.

Somente poderão ser conectados à rede corporativa os equipamentos configurados, testados e homologados.

Toda manutenção ou reparo – seja de hardware ou software – deverá ser realizado por empresa responsável, ainda que o usuário tenha conhecimento da medida a ser adotada.

A **E-INVEST** manterá inventário contendo os equipamentos de informática e poderá solicitar a devolução dos equipamentos concedidos, devendo estes ser entregues em perfeitas condições de uso e conservação.

3.1.4. Equipamentos portáteis

É vedada a entrada de equipamentos portáteis de terceiros na área da **E-INVEST.**

Equipamentos portáteis de propriedade da **E-INVEST** devem usar mecanismos de proteção física afim de proteger as informações, bem como o equipamento.

É vedado a utilização de equipamentos portáteis próprios dos colaboradores para acesso à internet, rede corporativa ou sistemas, exceto se expressamente autorizado.

3.1.5. Utilização de senhas

Somente usuários autorizados poderão acessar a informações e sistemas da **E-INVEST,** o usuário é responsável pela sua chave de acesso, sua senha e por todos os acessos e operações realizadas através destas.

As chaves de acesso deverão possuir robustez de segurança, com combinação de números, letras e caracteres especiais, as chaves de acesso deverão ser atualizadas periodicamente.

A chave de acesso é pessoal e intransferível, devendo o colaborador manter o sigilo de acesso e em nenhuma circunstância, compartilhar a senha com demais colaboradores e terceiros.

As chaves de acesso devem ser genéricas, sendo vedado o uso de senhas iguais ou similares a utilizadas em plataformas externas, como redes sociais, e-mail, bancos, dentre outros.

Em casos extremos de risco de impacto nos negócios, qualquer recurso de TI da **E-INVEST** na posse de um usuário poderá ser acessado por outros usuários, sujeito à aprovação prévia do gestor imediato, por qualquer motivo de continuidade de atividades de negócio coerente com esse acesso, inclusive em caso de usuários em licença médica, férias, licença maternidade, e em caso de suspensão ou rescisão do contrato de trabalho ou de quaisquer outros contratos, independentemente do motivo.

3.1.6. Chaves de acesso de terceiros

Os terceiros devem ter ciência, através dos gestores dos contratos, dos procedimentos da Política de Segurança da Informação e deste Anexo, devendo prezar pelo seu cumprimento.

Não será permitido a utilização de e-mails corporativos com o domínio da **E-INVEST** ou da ERICSSON por terceiros. Também é proibido o uso da assinatura padrão da **E-INVEST** por terceiros.

3.1.7. Acesso à rede corporativa

Todo acesso à rede corporativa se dá mediante a apresentação de chave de acesso e senha. Ao se ausentar ou sair, o usuário deve encerrar a sua conexão ao bloquear sua estação de trabalho, para que não haja utilização indevida ao equipamento.

3.1.8. Acesso remoto

O acesso remoto à rede corporativa pode utilizar, além da chave de acesso e senha, mecanismos de autenticação que proporcionem um nível de segurança complementar. Exceções devem ser tratadas quando necessário.

O mecanismo de autenticação complementar, pode ser um certificado digital, “token” ou qualquer outro dispositivo ou software para aumentar a segurança no acesso remoto, de acordo com a particularidade do caso.
Quando o equipamento de autenticação complementar for físico, o colaborador deverá zelar do mesmo, evitando a perda, roubo ou destruição.

Devem ser tomados os seguintes cuidados no acesso remoto: a) Não acessar a rede corporativa de um lugar onde a confidencialidade das informações corporativas possa ser comprometida, tais como computadores instalados em locais públicos; b) atenção ao digitar a chave de acesso e senha para evitar observação por terceiros; c) nunca deixar a conexão aberta quando não estiver utilizando a conexão remota; d) sempre efetuar o "logout" da conexão ao fim do acesso à rede; e e) sempre manter o equipamento sob supervisão.

3.1.9. Uso da internet

Os usuários poderão ter acesso à internet mediante autorização e solicitação.

Todo acesso à internet deve ser feito através da rede corporativa, sendo proibido a utilização de "modems" ou rede wireless externa para acesso à internet.

O usuário deve prezar pela boa utilização da rede, sendo vedado o acesso a conteúdos que não sejam vinculados à função exercida ou de cunho pessoal.

Todo o fluxo de informações entre a **E-INVEST** e a internet deve ser monitorado. Relatórios de utilização podem ser disponibilizados sob demanda para conhecimento dos diretores e gestores.

Todo conteúdo recebido ou enviado para a internet deve ser submetido a verificações de segurança para eliminação de virus e bloqueio de qualquer tipo de conteúdo não aderente à norma de segurança.

A **E-INVEST** não se responsabiliza por problemas ocasionados ao fornecimento de informações pessoais de seus usuários, como números de cartão de créditos ou contas e senhas.

Poderá haver bloqueios de acessos a sites que não sejam vinculados à atividade da **E-INVEST**.

Os usuários não podem utilizar contas que não sejam associadas à **E-INVEST**, incluindo contas de e-mail pessoal para transmitir informações de qualquer natureza. Como regra geral, todos os correios eletrônicos ou documentos comerciais devem ser enviados e recebidos através do e-mail fornecido ou de qualquer outro recurso tecnológico da **E-INVEST.**

A **E-INVEST** se reserva o direito de monitorar o uso de cada recurso tecnológico por qualquer motivo comercial ou profissional legítimo, por razões de segurança, em caso de violação ou de suspeita de violação deste padrão empresarial, de acordo com a lei e com a Política de Proteção de Dados da **E-INVEST**, quando aplicável.

3.1.10. Correio eletrônico

O sistema de correio eletrônico deve ser utilizado exclusivamente para atividades relacionadas à **E-INVEST.**

Será concedido acesso aos colaboradores da **E-INVEST** ao recurso de correio eletrônico mediante a necessidade e autorização pelo gestor da área, após participação no treinamento de correio eletrônico.

É vedado o cadastramento do e-mail corporativo em listas de discussão, sites de propagando, vendas de produtos ou eventos.

Quando o usuário não reconhecer a origem do remetente da mensagem eletrônica, não deverá responder, clicar em links, baixar ou executar arquivos anexos.

É vedado o envio ou resposta a e-mails de tipo corrente.

No envio de e-mails externos, os usuários deverão sempre atentar para a inclusão de termo de responsabilidade e aviso legal padronizado, informando os direitos do leitor e as responsabilidades assumidas e não assumidas.

É vedado o compartilhamento de arquivos de cunho pornográfico ou que violem direitos autorais. A **E-INVEST** não se responsabiliza por danos causados a terceiros decorrentes do uso inadequado do correio eletrônico.

3.1.11. Vírus

Todos os equipamentos conectados à rede corporativa da **E-INVEST** deverão ser constantemente monitorados e protegidos contra vírus, malwares e outras ameaças.

Em caso de qualquer suspeita de vírus, o colaborador deverá imediatamente consultar sobre os procedimentos necessários para reparo ao equipamento

.

3.1.12. Lixo informático

As mídias eletrônicas que contenham informações sigilosas e dados pessoais sob guarda da **E-INVEST,** deverão ser destruídas de acordo com a tabela de temporalidade dos arquivos.

3.1.13. Suporte

O suporte aos usuários dos recursos de informação deverá ser realizado através de chamado via “Service Desk”.

Sempre que necessário o reparo, configuração, ou outra providência nos sistemas e aplicativos da **E-INVEST,** o colaborador deverá solicitar o auxílio através do canal de suporte.

3.1.14. Arquivos e diretórios

A utilização dos arquivos e diretórios pela **E-INVEST,** deverá observar o controle de acesso lógico aos diretórios, devendo o usuário somente possuir acesso ao estritamente necessário para o desempenho da função.

Quando necessário o compartilhamento de arquivos internamente, deverão ser utilizados através da utilização de senha ou medida de segurança equivalente, que impeça o acesso indevido pelos demais usuários.

3.1.15. Redes wireless

Toda a instalação de rede wireless na **E-INVEST** deve passar por avaliação e autorização. É proibida a sua ativação com a finalidade de expansão da rede corporativa sem a devida autorização.

É proibido o compartilhamento de redes wireless (redes ad-hoc) entre equipamentos pessoais, tais como celulares e computadores protáteis e equipamentos corporativos sem a autorização.

3.1.16. Monitoramento

Os recursos de informação serão submetidos a processos de monitoramento e auditoria para a verificação quanto à aderencia a política de segurança e o comportamento do usuário quanto ao uso dos recursos.

O resultado do monitoramento dos recursos pode ser utilizado como evidência de suporte para futuras ações disciplinares.

A **E-INVEST** não necessita de qualquer tipo de aviso ou autorização judicial para executar tais monitoramentos.

Os usuários devem estar cientes de que a **E-INVEST** pode ser compelida a divulgar ou disponibilizar recursos tecnológicos a terceiros (em particular, seu conteúdo), em obediência a diferentes exigências legais, incluindo intimações, ordens judiciais, mandados de busca, solicitação de documentos em litígios. Quaisquer dessas divulgações ou comunicações somente poderão ser realizadas sob a supervisão do Departamento Jurídico.

3.2. Incidentes de Segurança

Todas as violações de segurança devem ser relatadas imediatamente. Caso o incidente envolva a exposição de dados pessoais sob guarda da **E-INVEST**, também deverá ser comunicado imediatamente ao Encarregado (DPO – Data Protection Officer) da E-INVEST. Assim que tomar conhecimento do incidente, iniciar os procedimentos constantes no plano de resposta a incidentes de vazamentos de dados pessoais, bem como isolar as provas e documentar as ações tomadas e criticidade do incidente. Após contingenciado o incidente de segurança da informação, deverá ser conduzido uma análise acerca da severidade do incidente, documentando-a e implementando melhorias necessárias e treinamento aos colaboradores, se aplicável.

E-INVEST
By PREVIERICSSON

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Av. Nicolas Boer, 399 - 11° andar - sala 11
Torre Corporate Time - Cond. Jardim das
Perdizes · São Paulo/ SP · CEP 01140-060