POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PL - 002

03/09/2020

Sumário

HISTÓRICO DE REVISÕES

Versão	Revisão	Data de Aprovação	Descrição das Alterações
1	0	03/09/2020	Versão Inicial.

FINALIDADE

Estabelecer diretrizes, responsabilidades e competências, para assegurar a disponibilidade, integridade, autenticidade e confidencialidade das informações produzidas, armazenadas e transmitidas pela Firjan e suas Instituições nos aspectos físico, lógico e comportamental.

ABRANGÊNCIA

Esta Política aplica-se a todos os colaboradores (efetivos ou temporários), fornecedores, associados e parceiros, em qualquer nível hierárquico, que atuem em nome da Federação das Indústrias do Rio de Janeiro - FIRJAN, do Serviço Nacional de Aprendizagem Industrial Departamento Regional do Estado do Rio de Janeiro - SENAI/RJ, do Serviço Social da Indústria Departamento Regional do Estado do Rio de Janeiro - SESI/RJ, do Instituto Euvaldo Lodi Núcleo Regional do Estado do Rio de Janeiro - IEL e do Centro Industrial do Rio de Janeiro - CIRJ, denominados aqui de Firjan e suas Instituições.

A sua aplicação abrange todas as atividades desenvolvidas no Brasil e/ou no exterior, devendo ser lida e interpretada em conjunto com o Código de Conduta Ética, Programa de Integridade Corporativa e demais Políticas e Normas internas da Firjan e suas Instituições.

CONCEITUAÇÃO

Os termos descritos neste documento deverão ser interpretados de acordo com as definições aqui apresentadas, quando mencionados neste documento, independentemente do gênero adotado e/ou se utilizados no plural ou singular:

Boas práticas de segurança da informação – É um conjunto de métodos e procedimentos utilizados como referências para estabelecer a segurança da informação e da privacidade.

Colaborador – Todos os funcionários (efetivos ou temporários), dos diversos níveis, que atuem, remunerados ou não, em nome da Firjan e suas Instituições.

Comitê de Segurança da Informação (CSI) – Instância administrativa consultiva, no âmbito da Firjan e suas Instituições, para tratar assuntos afetos à segurança da informação.

Conscientização em segurança da informação – São orientações disseminadas por diversos meios, tais como: intranet; palestras; dentre outros, com o intuito de conscientizar todos os usuários sobre boas práticas de segurança da informação.

Controle de acesso – Regula o acesso físico e lógico apenas a pessoas autorizadas.

Cópia de segurança (backup) – É a cópia dos dados de um dispositivo de armazenamento para outro, que pode ser restaurada em caso de perda dos dados originais ou danos no dispositivo principal.

Descarte de recursos computacionais – É adoção na Firjan e suas Instituições de práticas de descarte seguro, a fim de evitar vazamentos de informação.

Desenvolvimento e aquisição de sistemas – São roteiros, manuais de instruções que auxiliam o desenvolvedor ou quem compra um software a respeito dos requisitos de segurança da informação.

Gestão de riscos de segurança da informação – Conjunto de processos que permite identificar, tratar e implementar de forma sistemática e contínua as medidas de proteção necessárias para minimizar ou eliminar os riscos que os ativos de informação estão sujeitos.

Incidente de segurança da informação – Qualquer evento indesejado ou inesperado, que comprometa as operações ou ameace a segurança da informação.

Informação – É o conjunto de dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, que reunidos possuem valor para uma organização ou pessoa.

Informações sigilosas – Informações classificadas como confidenciais, devendo sua utilização ser autorizada pelo seu gestor e/ou pela diretoria responsável por essa informação.

Notificações de segurança da informação - São eventos de comunicação ou alertas realizados por meios tecnológicos, com o intuito de alertar ou orientar.

Plano de Continuidade de Tecnologia da Informação ou Plano de Contingência – Conjunto de estratégias e procedimentos que devem ser adotados com o objetivo de minimizar as perdas decorrentes de um impacto sofrido diante do acontecimento de situações inesperadas, desastres e falhas de segurança.

Prestador de serviço - Todos os profissionais contratados em caráter temporário, que desempenham atividades específicas em determinada área, sob supervisão ou coordenação de um Gestor.

Proteções - São medidas, procedimentos e mecanismos que são adotados para fornecerem segurança aos ativos.

Recursos computacionais de tecnologia da informação - Todos os equipamentos computacionais e seus periféricos, dispositivos de armazenamento de informações em mídia eletrônica, programas, aplicativos de computador, softwares e infraestrutura de rede que interligam computadores da rede corporativa da Firjan e suas Instituições.

Segurança da informação – É a utilização de medidas técnicas e administrativas aptas à protegerem a informação de acessos não autorizados e/ou situações acidentais, ilícitas de destruição, perda, alteração, comunicação ou difusão.

Termo de Confidencialidade – É o documento, de cunho jurídico, que prevê o comprometimento de não utilização ou divulgação de informações importantes fora do âmbito do contrato, visando preservar a confidencialidade das informações ou dos materiais compartilhados em determinada relação.

REFERÊNCIAS

ABNT NBR/ISO/IEC 15999-1:2008 – Institui o Código de melhores práticas para Gestão de continuidade de negócios

ABNT NBR ISO/IEC 27.001:2013 – Diretrizes para implementação de Sistemas de Gestão de Segurança da Informação

ABNT NBR ISO/IEC 27.002:2013 – Institui o Código de melhores práticas para Gestão de Segurança da Informação e Comunicações

ABNT NBR ISO/IEC 27.005:2008 - Fornece as diretrizes para a Gestão de Riscos de Segurança da Informação e Comunicações

ABNT NBR ISO/IEC 27.701:2019 - Fornece as diretrizes para gerenciamento de informações de privacidade e tratamento de dados pessoais

Cartilha de Boas Prática de Segurança da Informação do Tribunal de Contas da União (TCU)

Modelo de Governança da Confederação Nacional das Indústrias (CNI) Resolução nº 563/2012

Política de Privacidade da Firjan e suas Instituições

DIRETRIZES

A Firjan e suas Instituições entendem que a informação é um dos principais ativos que compõem o seu patrimônio, ou seja, é um bem que possui valor, que deve ser protegido e cautelosamente utilizado, independentemente de estar armazenado em meio físico ou digital.

1. PRINCÍPIOS

As ações de Segurança da Informação, no âmbito da Firjan e suas Instituições, são norteadas pelos seguintes princípios:

a) Autenticidade: Garantia de que a informação foi produzida, expedida, modificada ou destruída dentro de preceitos legais e normativos, por sistema, por pessoa física ou jurídica;

b) Confidencialidade: Garantia de que a informação não esteja disponível ou revelada a sistema, à pessoa física, ou entidade não autorizada;

c) Disponibilidade: Garantia de que a informação esteja acessível e utilizável sob demanda por sistemas de informação, pessoa física ou jurídica, desde que o acesso esteja devidamente autorizado;

d) Ética: Os direitos e interesses legítimos dos usuários devem ser preservados, sem comprometimento desta Política;

e) Integridade: Consiste na fidedignidade de informações. Garantia de não violação da informação com o intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital;

f) Irretratabilidade ou não repúdio: Propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita e devidamente registrado; e

g) Privacidade: Garantia ao direito pessoal e coletivo e ao sigilo das informações de cunho pessoal, sem que haja o comprometimento desta Política.

2. INSTÂNCIAS DA SEGURANÇA DA INFORMAÇÃO

Com a finalidade de gerir de forma uníssona, a Firjan e suas Instituições possuem as seguintes estruturas para Gestão da Segurança da Informação:

a) Comitê de Segurança da Informação; e
b) Comitê de Implantação da Lei Geral de Proteção de Dados (LGPD).

3. SEGURANÇA DE DADOS

Em relação à segurança de dados, a Firjan e suas Instituições comprometem-se a prover a proteção adequada das informações de acordo com as diretrizes de Segurança da Informação, observando todo o seu ciclo de vida: criação, transmissão, armazenamento, transporte e descarte.

A Firjan e suas Instituições prezam pela organização das informações, e por isso possuem normas internas que visam promover a correta classificação da Informação a fim de definir níveis e critérios de proteção adequados às informações trabalhadas durante suas atividades.

4. SEGURANÇA EM RECURSOS COMPUTACIONAIS

4.1. Ativos e Recursos de Tecnologia da Informação

É dever de todos os colaboradores da Firjan e suas Instituições, bem como de terceiros com os quais as Instituições se relacionam, zelarem pelos recursos computacionais sob sua responsabilidade, mantendo sua conservação e bom estado, bem como promoverem a proteção adequada contra perdas, roubos, furtos e acessos não autorizados.

Todos os ativos e recursos de tecnologia de informação da Firjan e suas Instituições devem ser devidamente licenciados, identificados e documentados, bem como possuem regramento específico.

Para aquisição de um novo ativo ou aquisições e/ou contratações de serviços para projetos de tecnologia da Firjan e suas Instituições torna-se necessário observar normativo interno.

No que tange às normas sobre Segurança da Informação, estas deverão ser periodicamente atualizadas e avaliadas.

4.2. Controle de Acessos

De forma a manter a segurança nos acessos às informações da organização, a Firjan e suas Instituições devem adotar processos de gerenciamento de todas as credenciais de acesso, sejam elas físicas ou lógicas.

Devem ser estabelecidos processos de revisão de senhas inativas, e a garantia de que todos os colaboradores alterarem suas senhas de acesso periodicamente, conforme normativo interno.

A conta eletrônica e senha de acesso são para uso exclusivo de cada usuário, não sendo permitida, em nenhuma hipótese, o seu compartilhamento ou a sua disponibilização para terceiros.

Todos os acessos à base de dados corporativa devem ser monitorados e restritos somente por meio de sistemas de informação.

4.3. O uso da internet

O acesso à Internet disponibilizado aos usuários pela Firjan e suas Instituições, por meio da rede corporativa, possui a finalidade de servir às atividades necessárias ao desenvolvimento das atividades corporativas, respeitando a imagem, proteção da informação e reputação das Instituições.

Com o objetivo de preservar os conceitos de confidencialidade, disponibilidade e integridade das informações, a Firjan e suas Instituições devem realizar o monitoramento de todo o acesso à Internet, bem como instalar bloqueadores de acesso conforme a necessidade de preservação da imagem e proteção de suas informações.

4.4. O uso de e-mail

O correio eletrônico corporativo deve ser utilizado somente para o desenvolvimento de atividades corporativas e representação da empresa perante a terceiros de forma eficiente, respeitando a nossa imagem e reputação.

Todas as informações trocadas por meio das contas correio eletrônico corporativo passam automaticamente a fazer parte do patrimônio e propriedade da devida Instituição, podendo esta, dispor das mesmas para apuração de suspeita de uso indevido ou apuração de irregularidades no intuito de resguardar seus direitos.

Todo o tráfego do sistema de correio eletrônico corporativo deve ser monitorado por razões técnicas necessárias à manutenção e segurança do sistema conforme normativas técnicas sobre o tema.

4.5. O uso dos recursos de computacionais

Os recursos computacionais disponibilizados aos usuários estão sob responsabilidade das Instituições que compõem a Firjan e têm por finalidade servir às atividades necessárias ao desenvolvimento das atividades corporativas de forma eficiente respeitando a imagem e reputação destas Instituições.

Todas as informações criadas por meio de softwares ou sistemas de informações, armazenadas sob a forma de arquivos, sejam eles locais nas estações de trabalho ou em ambientes de rede e banco de dados, passam automaticamente a fazer parte do patrimônio de propriedade de sua respectiva Instituição, podendo esta dispor das mesmas em qualquer momento no intuito de resguardar seus direitos.

Os recursos computacionais devem ser monitorados, sejam eles equipamentos, credenciais de acesso lógicas, informações em sistemas ou em qualquer outro meio, dispositivos de comunicação, segurança, entre outros.

A Firjan e suas Instituições exoneram-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos computacionais concedidos aos seus colaboradores e reservam-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

4.6. Diretrizes de backups

Devem ser estabelecidos procedimentos e controles para a cópia, guarda e proteção de todos dados da organização de forma a garantir a continuidade dos negócios da Firjan e suas Instituições.

4.7. Manutenção de testes de equipamentos e sistemas

A Firjan e suas Instituições devem manter processos e controles que permitam realizar testes controlados em equipamentos ou sistemas de forma a mantê-los funcionais e seguros. Periodicamente a Organização deve realizar testes de segurança em seus equipamentos de perímetro para certificar que os controles de segurança adotados estejam funcionais.

5. Segurança cibernética

5.1. Proteções contra softwares maliciosos

A Firjan e suas Instituições devem estabelecer procedimentos que visem os controles de detecção, prevenção e combate à códigos maliciosos, de forma a impedir que eles sejam executados, disseminados ou transportado por diferentes meios, incluindo acessos à Internet, correio eletrônico, anexos de correio eletrônico, dispositivos de armazenamento portáteis, entre outros.

5.2. Segurança e tratamentos de mídias

Todas as mídias utilizadas para o transporte de informações confidenciais devem possuir mecanismos criptográficos de forma a proteger a informação.

5.3. Coletas de registros de falhas

É necessário a guarda de logs e trilhas de auditoria em sistemas, dispositivos de rede e segurança, de forma que seja possível rastrear as falhas de segurança e responder a incidentes.

5.4. Gerenciamento e controle de redes

Como boa prática de segurança em redes, deve ser realizado o gerenciamento e controle de redes comunicação e seus respectivos dispositivos, de forma com que se estabeleça uma segregação das mesmas, permitindo assim responder de forma mais rápida incidentes nesses ativos.

Serão controladas e monitoradas as redes dos usuários internos, externos e convidados, conforme normativo interno.

5.5. Controle de mecanismos e gerenciamento de chaves

A proteção lógica adicional e os mecanismos tecnológicos que garantem a segurança no armazenamento, recebimento, transmissão e manutenção dos dados em nossos servidores deve ser adotada para evitar o acesso não autorizado às informações. É necessário que as Instituições tenham procedimentos e controles para um eficaz gerenciamento da segurança usada pela organização, onde devem ser detalhadas as regras em normativa de acordo com o tema.

5.6. Monitoramentos de ataques cibernéticos

As Instituições devem definir procedimentos e controles para realização do monitoramento de ataques aos diversos vetores de acesso ao ambiente tecnológicos da organização. Periodicamente a Organização deve realizar testes de segurança em seus equipamentos de perímetro para certificar que os controles de segurança adotados estejam funcionais.

5.7. Riscos cibernéticos

A Firjan e suas Instituições devem definir processos e controles para identificar, classificar, analisar, tratar e monitorar os riscos cibernéticos.

Os riscos mapeados serão comunicados às instituições e terão plano de ação com objetivo de mitigá-los.

6. SEGURANÇA FÍSICA

1.1. Controle de acesso físico

Os controles de acesso físico visam controlar o acesso aos equipamentos, recursos computacionais e documentos confidenciais da Firjan e suas Instituições somente a pessoas autorizadas.

Dessa forma, devem ser adotados controles para restrição de entrada e saída de colaboradores e visitantes.

Câmeras de vigilância devem ser instaladas a fim de monitorar áreas importantes das instalações e todos os colaboradores são orientados a manterem a mesa de trabalho limpa.

6.1.1 Controle de acesso de colaboradores

Todos os colaboradores da Firjan e suas Instituições devem portar um crachá em local visível indicando seu nome, foto e número da matrícula.

As áreas que forem consideradas sensíveis deverão ser restritas somente ao pessoal autorizado, conforme estipulado pelo Gerente responsável, possibilitando seu acesso somente por meio eletrônico.

Os equipamentos e ativos pessoais devem ser utilizados pelos colaboradores para a realização das atividades profissionais.

6.1.2 Controle de acesso físico de visitantes e prestadores de serviços

O acesso de convidados e prestadores de serviços nas áreas da Firjan e suas Instituições deverá ser autorizado por um colaborador responsável. Neste mesmo sentido, o acesso físico ao ambiente do datacenter deverá ser restrito e controlado, somente sendo permitido a entrada de pessoas autorizadas.

Todos os visitantes deverão portar crachá em local visível com o termo “visitante” escrito e deverão ser acompanhados pelo colaborador que autorizou seu ingresso na Instituição.

6.1.3 Monitoramento da Frota Corporativa

Os temas relacionados à monitoramento de frota e utilização de GPS em veículos institucionais serão tratados em normativo interno.

7. DIRETRIZES A SEREM ADOTADAS NA SEGURANÇA E CULTURA ORGANIZACIONAL

7.1 Cultura e Segurança da Informação

A responsabilidade em relação à Segurança da Informação deverá ser observada por todos os colaboradores e prestadores de serviços em todas as atividades realizadas para a Firjan e suas Instituições, conforme regras de normativo interno.

Os colaboradores deverão ser conscientizados constantemente com relação ao tema Segurança da Informação por meio de campanhas e capacitações com objetivo de ampliar a cultura organizacional, bem como garantir a segurança nas ações institucionais.

7.2 Contratos

Todos os contratos decorrentes das relações de trabalho, seja de colaborador ou de terceiros, bem como contratos de negócio e afins deverão observar as diretrizes desta Política.

No tocante aos processos de coleta, tratamento e descarte de informações dos referidos contratos a área responsável deverá estabelecer pessoa responsável pela guarda desses documentos.

Todos os contratos com terceiros e seus respectivos aditamentos deverão obrigatoriamente constar Cláusula de Confidencialidade e o Termo de Confidencialidade, que deverá ser assinado entre as partes e armazenado para consulta sempre que necessário. Os Termos de Confidencialidade deverão ser revistos e aprimorados constantemente.

Em relação ao encerramento dos contratos de trabalho, de prestação de serviços ou quando houver mudanças de área dentro das Instituições, os recursos de tecnologia da informação deverão ser devolvidos ao gestor imediato.

7.3 Plano de Continuidade de Tecnologia da Informação ou Plano de Contingência

As Instituições devem elaborar um Plano de Continuidade ou Plano de Contingência a fim de garantir a manutenção dos negócios das Instituições frente à um cenário de desastre, visando a necessidade de reposicionar a Firjan e suas Instituições em situações de violação da confidencialidade, integridade e disponibilidade das informações.

Dessa forma, o Plano possui como objetivo garantir que o funcionamento dos sistemas informatizados seja restabelecido no menor tempo possível a fim de reduzir os impactos causados por fatos imprevistos.

O Plano deverá ser testado anualmente e os colaboradores da Firjan e suas Instituições deverão receber treinamento e capacitação acerca deste documento.

8. DIRETRIZES A SEREM ADOTADAS NO DESCARTE SEGURO

A Firjan e suas Instituições possuem procedimentos para garantir o descarte seguro de documentos e papéis, bem como gerenciar, controlar e testar as mídias de cópias de segurança até o seu último descarte.

O transporte, armazenamento e descarte de documentos seguem procedimentos próprios estabelecidos em norma internas que garantem a Segurança da Informação. No mesmo sentido, o descarte de recursos computacionais obedece aos procedimentos específicos, a fim de evitar o vazamento de informações.

9. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A Firjan e suas Instituições, por meio de um processo formal de gerenciamento de riscos de Segurança da Informação, promovem uma análise crítica constante dos controles, políticas, processos e procedimentos existentes em toda organização, a fim de identificar os riscos críticos, promover ações de mitigação e contingência, comunicar as partes interessadas e registrar eventual aceitação.

10. COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

É responsabilidade de todos os colaboradores, ao tomarem conhecimento de qualquer descumprimento referente à essa Política, comunicarem o fato imediatamente a área de Segurança da Informação por meio de abertura de chamado na central de atendimento.

Todos os incidentes de Segurança da Informação, no âmbito da Firjan e suas Instituições, são registrados e gerenciados por equipe própria definida para tratamento e resposta aos incidentes a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança da Instituição. Se necessário, a equipe de Segurança da Informação acionará o Comitê de Segurança da Informação que, conforme a natureza, gravidade e impacto causado poderá recomendar medidas para averiguar os fatos.

11. COMUNICAÇÃO DE TERCEIROS

Ressaltamos que é dever de todos os colaboradores, fornecedores, clientes e demais terceiros relacionados a Firjan e suas Instituições comunicarem imediatamente à Ouvidoria a ocorrência de fatos contrários a esta Política através de um dos canais de comunicação abaixo descritos:

a) Preenchimento de formulário no Portal da Transparência do SENAI (https://www.firjan.com.br/senai-transparencia/integridade/ouvidoria/) e do SESI (https://www.firjan.com.br/sesi-transparencia/integridade/ouvidoria/);

b) Encaminhamento de e-mail para ouvidoria@firjan.com.br;

c) Atendimento pelo telefone 0800-023-1231.

Seguindo a legislação pátria, a Firjan e suas Instituições possuem canal próprio para informar aos titulares a situação atual dos dados, bem como os tratamentos aplicados e o tempo de manutenção dos mesmos, permitindo assim o controle dos titulares sobre seus dados. O canal é direto com o Encarregado (DPO) pelo e-mail dpo@firjan.com.br

12. SUPERVISÃO

Todos os colaboradores da Firjan e suas Instituições devem estar familiarizados com os princípios e regras contidos na presente Política de Segurança da Informação.

Os gestores têm a obrigação de assegurarem que sua equipe observe tais regras e princípios, buscando evitar que, no âmbito da sua área de responsabilidade, ocorram desvios de conduta que podem ser evitados com a devida supervisão.

13. SANÇÕES

O colaborador ou prestador de serviço, no desempenho de suas atividades, que descumprir quaisquer das determinações previstas nesta Política e/ou nos demais documentos normativos complementares sobre Segurança da Informação estará sujeito às sanções disciplinares previstas no Código de Conduta Ética e na Norma interna de Sanções Disciplinares bem como as penalidades legais cabíveis.

14. ATUALIZAÇÃO

A Política de Segurança da Informação, bem como o conjunto de instrumentos normativos gerados a partir dela, serão revisados de forma periódica, sempre que se fizer necessário.

DISPOSIÇÕES GERAIS

Esta Política vigora a partir da data de sua publicação.

MATRIZ DE RESPONSABILIDADES

Etapas	**Responsáveis**
Elaboração do Documento	Gerência Geral de Tecnologia em conjunto com a Gerência de Integridade Corporativa/Divisão de Compliance
Validação do Documento	Comitê de Segurança da Informação
Aprovação do Documento	Presidência

Política Publicada em 08/09/2020.