Instituto **Janela**
para o **Mundo**

Política de segurança da informação

Aprovado em 02/06/2025 pelo Conselho
Deliberativo do Instituto Janela para o Mundo.

1. Introdução

Esta política define normas e diretrizes que buscam assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pelo Instituto Janela para o Mundo.

A proteção adequada dos ativos e dos dados utilizados é fundamental para que possibilite a identificação, proteção, detecção, resposta e recuperação de eventos em caso de eventual falha da segurança da informação.

Além disso, a Política complementa a Seção 11 do Código de Conduta do Instituto, no que diz respeito às diretrizes e às condutas esperadas dos colaboradores, terceiros, parceiros, fornecedores e prestadores de serviços, quanto à proteção dos ativos e dados com intuito de assegurar a confidencialidade, a integridade e disponibilidade das informações.

Aprovada pelo Conselho Deliberativo em 02 de junho de 2025, esta Política será disponibilizada no website, rede interna e na plataforma do Microsoft Teams para todo Instituto. Sempre que necessário, e com uma periodicidade mínima de 2 (dois) anos, a Política será verificada pelo Conselho Deliberativo e poderá ser revisada.

A adesão a essa Política e eventuais desvios de conduta serão endereçados pela Diretoria de Tecnologia das empresas fundadoras do Instituto.

Será mantido um programa de revisão/atualização, que assegure que os requisitos de segurança técnicos e legais implementados estão sendo cumpridos e em conformidade com a legislação vigente, incluindo também a revisão periódica dos planos de ação e sua adesão a iniciativas de compartilhamento de informações sobre incidentes cibernéticos.

2. Regras básicas de segurança da informação

2.1 Princípios da Segurança da Informação

Nosso compromisso com o tratamento adequado das informações do Instituto, alunos e público em geral estão fundamentados nos seguintes princípios:

Confidencialidade

Assegurar que a informação não será divulgada a indivíduos, entidades ou aplicativos sem autorização prévia dos seus titulares ou do Instituto.

Integridade

Assegurar que o conteúdo da informação não tenha sido alterado e, portanto, seja íntegro e autêntico.

Disponibilidade

Permitir que a informação confidencial seja utilizada apenas quando necessário pelos usuários e destinatários.

2.2 Ciclo de Vida da Informação

Para efeito desta política, considera-se como ciclo de vida da informação:

Manuseio: é a etapa em que a informação é criada e manipulada.

Armazenamento: é a guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.

Transporte: ocorre quando a informação é transportada para algum local, não importando o meio em que ela está armazenada.

Descarte: é a eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives) por completo.

2.3 Classificação da Informação:

A classificação das informações deve ser avaliada de acordo com seu conteúdo, relevância do conhecimento externo e pelos elementos específicos do documento.

O acesso, divulgação e tratamento de documento (físico ou digitalizado), dado ou informação são restritos aos colaboradores que tenham necessidade de conhecê-los em razão de suas atividades dentro do Instituto, sendo esse acesso pautado pelas regras previstas nesta Política e demais normas do Instituto. Toda informação interna deve ser classificada de acordo com o grau de sigilo para o Instituto, considerando-se três níveis:

Confidencial

É o mais alto grau de sigilo, aplicadas às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem do Instituto.

Interno

São informações específicas para uso interno, com circulação exclusiva dentro do Instituto. Essas informações podem estar disponíveis a todos os colaboradores e prestadores de serviço e devem ser utilizadas somente para atividades do Instituto. Esse conteúdo, mesmo sendo de circulação livre dentro do Instituto, não deve ser divulgados para externos sem os devidos cuidados, incluindo, quando necessário, a assinatura de acordos de confidencialidade ou de autorização formal previamente avaliada pela área responsável.

Externo

Esta categoria inclui dados destinados a uso fora da organização, mas que não estão disponíveis publicamente. Exemplos de dados externos incluem dados de fornecedores e dados de marketing.

Público

São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

2.4 Incidentes de Segurança da Informação

Para efeito desta Política, um incidente de segurança é definido como qualquer evento prejudicial, decorrente da ação ou omissão de colaboradores e de terceiros ou, ainda, de uma ameaça que ataque os princípios da Segurança da Informação.

3. Sistema de gestão da segurança da informação

O Sistema de Gestão da Segurança da Informação é o conjunto de processos e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação com ações em quatro grandes frentes de atuação:

· Governança das políticas e procedimentos de segurança da informação;
· Recursos e componentes de segurança da informação;
· Monitoramento contínuo do ambiente de tecnologia da informação;
· Gestão de crises e continuidade de negócios.

4. Controles internos de segurança da informação e cyber security.

4.1 Identificação/Avaliação de Ameaças e Vulnerabilidades.

Caberá à área de Segurança da Informação a identificação e avaliação dos riscos a que os processos e ativos estejam sujeitos e possíveis cenários de ameaça.

O Instituto revisa as cláusulas contratuais obrigatórias para a contratação de fornecedores e prestadores de serviços para adequar todos às políticas vigentes.

4.2 Ações de Prevenção e Proteção.

Serão adotadas rotinas padronizadas de prevenção e proteção dos processos e ativo, conforme previstas na norma interna, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

Destacando a execução periódica de testes de ataque e invasão, visando monitorar a eficiência de seu sistema de proteção a vulnerabilidades cibernéticas, a área de Segurança da Informação realiza testes, tanto em ambiente interno (na modalidade Gray Box) como o externo (na modalidade Black Box).

4.3 Monitoramento e Testes.

Devem ser implementados controles internos efetivos para proteção dos RTICs (Recursos de Tecnologia da Informação e Comunicação) do Instituto, garantindo a sua confidencialidade, integridade, disponibilidade sempre observando as melhores práticas de mercado e regulamentações vigentes.

A área de Segurança da Informação pode monitorar ou inspecionar os RTICs que estiverem em suas dependências ou que interajam com os ambientes do Instituto sempre que considerar necessário.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre ambientes de produção e homologação. As ameaças cibernéticas devem ser analisadas em conjunto com as vulnerabilidades detectadas pela Segurança da Informação nos ativos de informação e devem possuir monitoramento proativo da área de Segurança da Informação.

4.4 Plano de Ação e de Resposta a Incidentes.

Os incidentes de Segurança da Informação devem ser identificados e registrados para acompanhamento dos planos de ação e análise das vulnerabilidades respeitando o nível de exposição a risco definido pelo Instituto.

Comunicação de incidentes

Os usuários devem comunicar imediatamente os casos de incidentes ao responsável por Segurança da Informação. Os incidentes deverão ser avaliados e investigados de forma a construir uma análise consistente de causa, riscos, partes envolvidas e planos de respostas. A avaliação deverá ser direcionada ao Diretor responsável pela Segurança Cibernética das Fundadoras para decisão das ações iniciais a serem tomadas. Classificada a relevância do incidente, o instituto deverá emitir comunicação aos envolvidos, informando a situação ocorrida e ações definidas, ao menos, de forma preliminar, informando/notificando sobre as atividades que serão tomadas posteriormente. Além disso, o responsável pela Segurança da Informação deve elaborar e divulgar ao Conselho de Administração o relatório anual sobre os planos de ação e resposta aos incidentes.

Tentativa de burlar

A mera tentativa de burlar às diretrizes e controles estabelecidos pelo Instituto, quando constatada, deve ser tratada como uma violação/incidente.

Tratamento de vulnerabilidade identificadas

O tratamento e as correções proativas das principais fragilidades ou fraquezas dos ativos de informação a serem utilizados devem estar registradas, sendo necessário avaliar o risco residual e ser sustentado pelos envolvidos no plano.

Conflitos de interesse

O Instituto deve possuir um processo de concessão de acessos que utiliza critérios claros e objetivos para identificar conflitos de interesse que decorrem de limitações técnicas ou de situações devidamente autorizadas. Deverá haver monitoramento das atividades dos acessos e das ameaças cibernéticas.

Elaboração de plano de ação

O plano de ação deverá ser elaborado pelos responsáveis de Segurança da Informação, podendo ser envolvidos outros departamentos caso necessários para implementação das soluções e para administração de eventuais contingências. Tal plano deve conter definição expressa dos papéis e responsabilidades na solução do impasse, prevendo acionamento dos colaboradores chave e contatos externos relevantes, caso aplicáveis. Deverão ser levados em consideração os cenários de ameaças previstos na avaliação de risco, havendo critérios para classificação dos incidentes, dependendo da gravidade. O plano de ação deverá prever os casos de necessidade de utilização das instalações de contingências nos casos mais severos, assim como o processo de retorno às instalações originais após o término do incidente. A documentação relacionada ao gerenciamento dos incidentes deverá ser arquivada para fins de auditoria.

Comunicado aos Órgãos Externos

O Instituto comunicará os incidentes relevantes e interrupções de serviços relevantes que configurem uma situação de crise, bem como providências adotadas para o reinício dessas atividades para os órgãos externos, quando necessário, através do Departamento Jurídico e Departamento de Comunicação.

5. Programa de capacitação e conscientização.

Através das suas plataformas internas, o Instituto promove um plano de conscientização recorrente sobre a importância da Segurança da Informação voltada para todo público interno, além de um resumo de segurança divulgado nos portais do Instituto.

6. Gestão de Acessos.

Objetivo

O processo de concessão de acesso aos ativos de informação do Instituto deve levar em conta os recursos necessários para execução de suas tarefas e cargo e função dentro do Instituto, além da autenticidade dessas credenciais de acesso.

Processo

6.1. Criação de Conta de Acesso

Todo acesso deve decorrer de uma solicitação formal da gestão do Instituto para gerar os devidos fluxos de validações e aprovações, além de garantir a segurança da informação, dados para auditoria e estatísticas de atendimento.

6.2. Alteração de Conta de Acesso

Em sua maioria, é derivado do processo de transferência e deve ser descrito em solicitação formal, nele devem estar contidas as informações da nova Unidade de Negócio, Centro de Custo e/ou Gestor.

O gestor anterior é responsável por verificar junto ao funcionário se há alguma pendência nos processos e o gestor futuro responsável pela validação de acessos do liderado, caso haja necessidade de manutenção de funções ou unidades de negócio, realizar a abertura de chamado destacando as possíveis revogações e/ou inclusões.

6.3. Bloqueio de Conta de Acesso

É derivado do processo de rescisão de contrato ou alteração de função. Caso a exclusão seja pelo desligamento os processos deverão iniciar com a equipe de gestão de pessoas e gestor a fim de validar possíveis pendências e somente depois abrir chamado para revogação de acessos, a fim de garantir a confidencialidade no processo.

Cabe à Tecnologia da informação realizar uma nova validação de pendências e encerrar os acessos nos sistemas.

Para casos de desligamento com riscos de segurança e/ou confidenciais, a solicitação de bloqueio poderá ser direcionada para a Diretoria de Tecnologia para ação imediata e de exceção. O processo estará evidenciado por e-mail e posterior criação de chamado técnico.

6.4. Revisão de Acessos e mitigação de erro de processo.

Mensalmente é realizada uma revisão dos acessos concedidos a todos os usuários e/ou colaboradores do Instituto, com base na planilha disponibilizada pelo RH sendo possível liberar, bloquear e/ou ajustar o que for necessário para observância à Política.

Semestralmente é feita a revisão de perfis de acesso em duas frentes. (i) Matriz de Acesso (ii) Usuários por perfil de acesso, conforme exemplo abaixo.

Será encaminhada aos gestores de áreas uma planilha de acessos por usuário, a fim de validar se as contas de acesso e os perfis atrelados estão em acordo com as regras de gestão e controles. Matriz de Perfil X Revisor.

7. Gestão de Mudanças

Objetivo

O andamento e o resultado de uma mudança em sistema ou infraestrutura tecnológica relevante, zela pela preservação dos controles relacionados à disponibilidade, integridade, confidencialidade e autenticidade dos dados, que são geridos pelo Departamento de Tecnologia da Informação de forma planejada, aprovada, testada e obedecendo ao processo de gerenciamento de mudanças.

1. Implementação da Mudança a. As mudanças devem ser implementadas somente por pessoal autorizado. b. As mudanças devem ser testadas e validadas antes de serem implementadas em produção. c. As mudanças de sistemas críticos devem ser implementadas durante as janelas de manutenção designadas, a menos que seja uma mudança de emergência.

2. Documentação de mudanças a. Todas as mudanças devem ser documentadas no sistema de Gerenciamento de Mudanças. b. A documentação deve incluir os detalhes da mudança, o status de aprovação, a data e hora de implementação e quaisquer resultados de testes. c. A documentação deve ser mantida para fins de auditoria e conformidade.

3. Reversão de Mudanças a. Um plano de reversão deve ser preparado para todas as mudanças. b. O plano de reversão deve ser testado antes de implementar a mudança. c. Se a mudança não puder ser implementada com êxito, o plano de reversão deve ser executado imediatamente.

8. Gestão da Operação

Objetivo

Realizar a gestão do ciclo de vida (aquisição, manutenção, atualização, suporte e descarte) dos recursos de tecnologia e telecomunicações do Instituto e garantir aos usuários do Instituto o pleno uso dos referidos recursos, levando em consideração as boas práticas do mercado e as práticas de segurança da informação definidas nessa Política

Processo

8.1 Suporte e gestão de crises

A área de tecnologia atende às solicitações dos usuários, considerando que estes devem fazer uso adequado dos recursos de tecnologia, através do registro de incidentes, dúvidas, dificuldades ou problemas no uso dos recursos e tecnologia.

A área de tecnologia disponibiliza e organiza canais de comunicação para organização da operação diária:

• Grupos em plataformas de comunicação.
Há grupos fixos para o acompanhamento da operação e grupos específicos criados para gestões de crises pontuais.

• Sistema para reporte de chamados.
Há o sistema da própria empresa, gerido pela área de tecnologia, e os sistemas de chamados dos fornecedores de serviços, como NOC e SOC

Monitoramento

O Instituto possui monitoramento 24 x 7 em duas frentes:

• NOC (Network Operations Center) Equipe que monitora a disponibilidade e performance do ambiente de tecnologia

Ao ocorrerem alarmes e eventos, o NOC notifica a equipe técnica da área de tecnologia do Instituto e, imediatamente, inicia a atuação (junto à provedores de telecomunicações, fornecedores de tecnologia e demais provedores de serviços).

O NOC também atua reativamente, quando usuários relatam problemas ou dúvidas na utilização de recursos de comunicação do Instituto.

• SOC (Security Operations Center) Essa equipe monitora, através de ferramentas como SIEM e CAS, o ambiente de tecnologia com foco em segurança da informação, acompanhando constantemente os eventos gerados no ambiente (alertas, alarmes e outros dados provenientes das diversas plataformas utilizadas pela empresa, seja em cloud e on premise).

Cada alarme ou alerta é devidamente analisado e tratado. De acordo com os níveis de criticidade de cada evento, ações mais ou menos enérgicas podem ser tomadas.

Os eventos relevantes são notificados por e-mail.

Os eventos críticos requerem contato telefônico com a área de tecnologia do Instituto, em geral após as medidas de mitigação e contenção do risco, ameaça ou incidente terem sido tomadas.

É realizada uma reunião semanal de acompanhamento dos indicadores relacionados à segurança da informação.