Política de Segurança da Informação e Comunicação

Niva Tecnologia da Informação

www.nivati.com.br
SIG QUADRA 01 N° 985 SALAS 236 A 243 - CENTRO EMPRESARIAL PARQUE BRASILIA
- CEP: 70.610.410 - BRASILIA – DF TEL: (61) 3326-8673

ÍNDICE

1. OBJETIVOS 3
2. DECLARAÇÃO DE COMPROMETIMENTO DA DIRETORIA 3
3. APLICAÇÃO 3
4. PRINCÍPIOS 3
5. DIRETRIZES GERAIS 3
6. PAPÉIS E RESPONSABILIDADES 8
7. PENALIDADES 14
8. DISPOSIÇÕES FINAIS 14
9. DOCUMENTOS DE REFERÊNCIA 15
10. DEFINIÇÕES PSIC, NORMAS E PROCEDIMENTOS 15

1. OBJETIVOS

1.1. Esta **Política de Segurança da Informação e Comunicação (PSIC)** tem por objetivos:

1.1.1. Definir os princípios e diretrizes gerais que visam a preservação da segurança da informação, primando pela confidencialidade, integridade, disponibilidade, autenticidade e legalidade dos processos que amparam a operacionalização e gestão do negócio;

1.1.2. Estabelecer as responsabilidades e limites de atuação dos dirigentes, colaboradores, parceiros e fornecedores em relação à segurança da informação e comunicação, reforçando uma cultura interna baseada em integridade.

2. DECLARAÇÃO DE COMPROMETIMENTO DA DIRETORIA

2.1. A **Diretoria** da **NIVA** está comprometida e apoia os princípios estabelecidos nesta PSIC de proteção de seus recursos tangíveis e intangíveis de acordo com as necessidades de negócio e em conformidade com o ambiente legal, primando pela confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

3. APLICAÇÃO

3.1. Esta PSIC é um documento com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, aos dirigentes, colaboradores, parceiros e fornecedores**.**

4. PRINCÍPIOS

4.1. Preservar e proteger as informações da **NIVA** e os recursos de Tecnologia da Informação e Comunicação (TIC), que estejam sob sua responsabilidade, dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas contidas em qualquer suporte ou formato.

4.2. Prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.

4.3. Assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade, assim como a legalidade no desenvolvimento das atividades do negócio.

4.4. Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados ao negócio no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.

5. DIRETRIZES GERAIS

5.1. **Interpretação**: Esta PSIC e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, tudo o que não estiver expressamente permitido só deve ser realizado após prévia autorização

do Comitê de Segurança da Informação e Comunicação (CSIC), devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

5.2. **Publicidade**: Esta PSIC e seus documentos complementares devem ser divulgados aos seus dirigentes, colaboradores e terceiros, visando a sua disponibilidade para todos que se relacionam com a **NIVA** ou que, direta ou indiretamente, são impactados.

5.3. **Propriedade:** As informações geradas, acessadas, manuseadas, armazenadas ou descartadas pelos dirigentes, colaboradores, parceiros e fornecedores no exercício de suas atividades profissionais com a **NIVA**, bem como os demais recursos tangíveis e intangíveis disponibilizados pela instituição a esses atores, são de propriedade e direito de uso exclusivo da **NIVA** e devem ser empregadas exclusivamente em atividades de seu interesse.

5.4. **Classificação da Informação:** Todas as informações de propriedade ou sob a responsabilidade da **NIVA** devem ser classificadas e protegidas com controles compatíveis em todo o seu ciclo de vida, por meio da implementação de ferramentas e formalização de processos em instrumento específico, nos termos dos Normativos Internos de Segurança da Informação.

5.5. **Sigilo**: É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade da **NIVA**, por seus dirigentes, colaboradores e terceiros, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja previamente classificada como “pública”.

5.6. **Privacidade e Proteção de Dados:** A **NIVA** respeita a privacidade dos titulares de dados e garante a disponibilidade, integridade e confidencialidade dos dados pessoais em todo o seu ciclo de vida, que vai desde a coleta, armazenamento, compartilhamento, até o descarte, em qualquer tipo de formato de armazenamento e suporte e de acordo com a sensibilidade do dado pessoal, a finalidade e a gravidade dos riscos. Para tanto, a **NIVA** deverá dispor de:

5.6.1. Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente;

5.6.2. Adoção de medidas de segurança para proteger os dados pessoais de acesso não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado;

5.6.3. Armazenamento de modo seguro, controlado e protegido;

5.6.4. Processos de anonimização e pseudonimização, sempre que necessário;

5.6.5. Protocolos de criptografia na transmissão e armazenamento, sempre que necessário;

5.6.6. Registro lógico de todas as operações de tratamento;

5.6.7. Descarte seguro dos dados pessoais ao término de sua finalidade e sua conservação de acordo com as hipóteses legais e regulatórias;

5.6.8. Transferência a terceiros de modo seguro e contratualmente previsto, atendendo aos requisitos de expressa autorização estabelecidos na legislação de proteção de dados pessoais vigentes para este processo;

5.6.9. Avaliação padronizada e contínua da utilização dos dados pessoais visando a realização de ações que visam minimizar riscos de violação da privacidade de seus titulares;

5.6.10. Gestão e tratamento adequado de incidentes que envolvam dados pessoais;

5.6.11. Testes, monitoramento e avaliações periódicas de sua efetividade.

5.7. Uso dos Recursos de TIC: Os recursos de TIC de propriedade da **NIVA** devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.

5.7.1. Os dirigentes, colaboradores, parceiros e fornecedores devem utilizar apenas recursos de TIC previamente homologados e autorizados pela **NIVA** para a realização de suas atividades profissionais, sejam eles onerosos, gratuitos, livres ou licenciados.

5.8. Manutenção dos Recursos de TIC: Todos os recursos de TIC em uso no ambiente institucional devem atender as recomendações de seus fabricantes ou desenvolvedores, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança.

5.9. Mobilidade: Os recursos de TIC que permitem mais mobilidade devem ser utilizados somente quando fornecidos ou autorizados pela **NIVA**. Além disso, devem estar diretamente relacionados a uma justificativa do negócio, com motivo estritamente profissional, no âmbito das atribuições dos dirigentes, colaboradores, parceiros e fornecedores.

5.10. Recursos de TIC Particulares: O uso de recursos de TIC particulares na execução de qualquer atividade profissional, na interação com os ambientes físicos ou lógicos ou com as informações da **NIVA**, não poderão ocorrer por meio da rede cabeada de transmissão de dados, exceto quando autorizado pela **NIVA**.

5.11. Repositórios digitais: É vedado aos dirigentes, colaboradores, parceiros e fornecedores o uso de repositórios digitais não homologados pela **NIVA** para armazenar ou publicar informações de propriedade da **NIVA** ou sob sua responsabilidade, salvo casos onde a informação esteja previamente classificada como “pública”.

5.12. Softwares de comunicação instantânea: É vedado aos colaboradores a instalação e o uso de softwares de comunicação instantânea não homologados pela **NIVA**.

5.13. Mídias Sociais: A participação do colaborador nas mídias sociais por meio dos recursos de TIC da **NIVA** deve estar relacionada às atividades profissionais.

5.13.1. Dirigentes, colaboradores, parceiros e fornecedores são responsáveis por suas condutas no uso das mídias sociais. Por isso, cuidados devem ser tomados em relação ao excesso de exposição (rotinas, trajetos, intimidade, etc.), no uso de conteúdos autorizados e legítimos e na preservação do sigilo profissional.

5.14. **Controle de acesso:** A **NIVA** controla o acesso físico e lógico às suas dependências e aos seus recursos de TIC. Desse modo, dirigentes, colaboradores, parceiros e fornecedores devem possuir uma credencial de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

5.14.1. Dirigentes, colaboradores, parceiros e fornecedores são responsáveis pelo uso e sigilo de suas credenciais de acesso. Não é permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de credenciais de terceiros, sendo responsável direto pela conduta ou/e dano causado, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

5.15. **Ambientes Lógicos:** Os sistemas e recursos de TIC que suportam os processos e as informações devem ser confiáveis, íntegros, seguros e disponíveis a quem deles necessitem para execução de suas atividades profissionais. Para garantir a segurança acima estabelecida, a **NIVA** utiliza os seguintes sistemas de proteções de forma ativa e sempre atualizados:

5.15.1. Contra programas maliciosos e acessos indevidos, como serviços de autenticação, antivírus e firewall;

5.15.2. Para indicar tentativas de intrusão realizada aos ambientes lógicos, como Sistemas de Detecção a Intrusão (*Intrusion Detection Systems*) ou IPS (*Intrusion Protection Systems*);

5.15.3. Contra mensagens eletrônicas indesejadas ou não autorizadas, como AntiSpam.

5.16. **Ambientes Físicos**: A **NIVA** deve estabelecer perímetros de segurança para proteção de suas propriedades, além de:

5.16.1. Implementar controles de identificação e registro de acesso em suas dependências para assegurar o acesso somente de colaboradores, parceiros e fornecedores autorizados e recursos de TIC homologados, constando data, hora e área onde será realizado o acesso;

5.16.2. Implementar, monitorar e gerenciar a segurança patrimonial com o uso de profissionais, câmeras, alarmes, fechaduras entre outros.

5.17. **Áudio, Vídeos e Fotos:** É vedada qualquer atividade relacionada a captura de dados e seu compartilhamento público, inclusive no âmbito acadêmico, na internet e/ou nas mídias sociais, envolvendo gravação de áudio, vídeo ou foto de informações confidenciais, sensíveis ou enquadradas como dados pessoais, que sejam utilizadas na realização das atividades profissionais dentro das dependências da **NIVA** por seus colaboradores, sem a prévia e formal autorização para tanto, exceto se ocorrer em razão justificável como necessário para cumprimento das atividades profissionais prestadas pelo colaborador.

5.18. **Contratação, Terceirização ou Prestação de Serviços:** Os relacionamentos e contratações, inclusive de colaboradores, em que ocorra o compartilhamento de

5.19. informações da **NIVA** ou a concessão de qualquer tipo de acesso aos seus ambientes e recursos de TIC, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à Segurança da Informação e Comunicação, além de preverem a

realização de auditorias eventuais ou periódicas para certificar a conformidade com a PSIC e seus documentos complementares.

5.20. **Documentação:** A **NIVA** deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam recursos de TIC.

5.21. **Salvaguarda (backup):** A **NIVA** deve definir e manter um processo de salvaguarda e restauração das informações e de seus recursos de TIC críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

5.22. **Análise dos processos e Recursos de TIC**: A **NIVA** deve analisar, em intervalos regulares, seus processos e recursos de TIC, visando assegurar que estejam devidamente mapeados, inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

5.23. **Monitoramento:** A **NIVA** realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, recursos de TIC e seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.

5.24. **Inspeção dos Recursos de TIC:** A **NIVA**, sempre que considerar necessário, pode auditar ou inspecionar os recursos de TIC que interagem com seus ambientes lógicos, físicos ou com suas informações, incluindo os recursos de TIC de propriedade de terceiros, quando autorizada a entrada em suas dependências, independentemente da interação com seus ambientes e informações.

5.25. **Continuidade do Negócio:** No escopo das ações de Segurança da Informação e Comunicação, os procedimentos de Gestão da Continuidade de Negócios devem ser executados em conformidade com os requisitos de segurança da informação e comunicação estabelecidos para proteção dos recursos de TIC.

5.26. **Conformidade:** A **NIVA** deve possuir e manter um programa de revisão/atualização desta PSIC e de seus documentos complementares no mínimo a cada **dois anos**, visando a garantia de que todos os requisitos de segurança técnicos e legais implementados sejam cumpridos, atualizados e em conformidade com a legislação vigente.

5.27. **Capacitação:** A **NIVA** deve possuir um Programa Contínuo de Conscientização em Segurança da Informação e Comunicação para capacitação e disseminação da cultura de Segurança da Informação junto aos seus colaboradores.

5.28. **Investimentos:** Os investimentos em Segurança da Informação e Comunicação devem ser estudados e deliberados pela **Diretoria da NIVA**, considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio.

5.29. **Comitê de Segurança da Informação e Comunicação** (**CSIC**): A **NIVA** deve criar e manter um Comitê de Segurança da Informação e Comunicação (CSIC), cuja principal função está em assessorar a implementação das ações relacionadas à Segurança da Informação e Comunicação, além de avaliar os controles e incidentes relacionados.

5.30. **Equipe de Resposta a Incidentes:** A **NIVA** deve manter uma Equipe de Resposta a Incidentes em Segurança da Informação e Comunicação, interna ou terceirizada, com composição fixa ou variável, competente e preparada para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação.

5.31. **Comissão de Ética e Ouvidoria:** A **NIVA** deve possuir um canal divulgado aos dirigentes, colaboradores, parceiros e fornecedores para reportar, imediatamente, os possíveis casos de incidentes de segurança da informação e comunicação, podendo fazê-lo formalmente ou com uso de denúncia anônima. Os comunicados categorizados como incidentes de segurança da informação e comunicação serão tratados como prioridade, sendo feito o encaminhamento adequado aos profissionais envolvidos na tratativa dos incidentes.

5.32. **Alterações:** As alterações desta PSIC e de seus documentos complementares devem ser devidamente comunicadas aos dirigentes, colaboradores, parceiros e fornecedores.

5.33. **Exceções:** As solicitações de tratamento diferenciado em situações que ocorram de forma exclusiva e excepcional a essa PSIC devem ser formalizadas e fundamentadas pelo solicitante e podem ser revogadas a qualquer tempo por decisão unilateral da **NIVA.**

6. PAPÉIS E RESPONSABILIDADES

6.1. Diretoria

6.1.1. Cumprir e fazer cumprir esta PSIC e demais documentos que a compõem;

6.1.2. Analisar e aprovar a PSIC;

6.1.3. Aprovar o Plano Contínuo de Capacitação e Conscientização aos colaboradores da **NIVA;**

6.1.4. Orientar para que as atividades desempenhadas pelo CSIC estejam adequadas ao negócio;

6.1.5. Instaurar, quando couber, procedimento administrativo disciplinar para apuração de responsabilidades dos envolvidos em violações dos documentos que a compõem;

6.1.6. Autorizar a aquisição de recurso de TIC existente ou que tenham o objetivo de realizar interação com os ambientes e informações da **NIVA**, sejam eles físicos ou lógicos (hardware e software).

6.2. Comissão de Ética e Ouvidoria

6.2.1. Estabelecer e manter um canal de relacionamento com a Equipe de resposta a incidentes de segurança e CSIC com objetivo de assegurar tratamento adequado aos eventos de segurança reportados;

6.2.2. Enviar ao CSIC, quando solicitado, relatório com as ocorrências tratadas relativas aos incidentes de segurança da informação.

6.3. Comitê de Segurança da Informação e Comunicação (CSIC)

6.3.1. Cumprir e fazer cumprir esta PSIC e demais documentos que a compõem;

6.3.2. Promover e realizar a gestão desta PSIC, zelando pela observância dos controles, modelos, padrões e recursos necessários à sua implantação;

6.3.3. Analisar criticamente e de forma periódica a PSIC, visando a sua conformidade legal e manutenção contínua com os requisitos de negócio da **NIVA** e propondo melhorias para aprovação da **Diretoria**;

6.3.4. Definir, analisar e priorizar ações necessárias, balanceando custo e benefício em cumprimento da PSIC;

6.3.5. Analisar os documentos complementares relacionados a esta PSIC e apresentar recomendações no que couber;

6.3.6. Recomendar a elaboração de documentos complementares a esta PSIC aos responsáveis pelas áreas internas da **NIVA**;

6.3.7. Garantir a publicidade dos documentos que compõem esta PSIC;

6.3.8. Orientar para que as atividades desempenhadas pelas áreas internas estejam adequadas às diretrizes desta PSIC;

6.3.9. Analisar os incidentes reportados relativos à segurança da informação;

6.3.10. Acionar as áreas internas impactadas ou os responsáveis, sempre que necessário, na análise dos eventos relativos à segurança da informação e comunicação;

6.3.11. Manifestar-se, quando solicitado, sobre questões de competência e relacionadas a esta PSIC.

6.4. Equipe de Resposta a Incidentes de Segurança da Informação e Comunicação

6.4.1. Receber, analisar, tratar e responder as notificações e atividades relacionadas aos eventos de segurança da informação e comunicação;

6.4.2. Apresentar medidas preventivas/corretivas dos eventos e incidentes analisados visando mitigar o risco/impacto;

6.4.3. Definir as práticas, padrões e limites de utilização dos recursos de TIC.

6.5. Canal de atendimento (Suporte TI):

6.5.1. Cumprir e fazer cumprir esta PSIC e demais documentos que a compõem;

6.5.2. Apoiar as áreas internas na definição de controles adequados de segurança da informação e comunicação;

6.5.3. Identificar e avaliar os riscos relacionados aos recursos de TIC e propor melhorias, quando couber;

6.5.4. Atuar proativamente em relação às ameaças e aos incidentes de segurança, reportando-os ao CSIC;

6.5.5. Garantir que todos os recursos de TIC em uso no ambiente corporativo atendam as recomendações de seus fabricantes ou desenvolvedores, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança;

6.5.6. Disponibilizar e realizar a gestão das credenciais individuais de acesso ao ambiente lógico;

6.5.7. Realizar o monitoramento dos ambientes lógicos visando a eficácia dos controles implantados, a proteção de seu patrimônio e a reputação da **NIVA**;

6.5.8. Apoiar o Departamento Administrativo na inspeção dos recursos de TIC, sempre que considerar necessário;

6.5.9. Avaliar os requisitos de segurança presentes antes da aquisição ou desenvolvimento de softwares;

6.5.10. Instalar, remover, homologar, monitorar, realizar verificações e inspeções de todo e qualquer recurso de TIC existente ou em interação com os ambientes e informações da **NIVA**, sejam eles físicos ou lógicos (hardware e software);

6.5.11. Garantir que o andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica, preservem os controles relacionados a disponibilidade, integridade, confiabilidade, sigilo e autenticidade das informações;

6.5.12. Participar na contratação e definição de métricas de qualidade e temporalidade (SLA) de quaisquer serviços relacionados à gestão e segurança dos recursos de TIC;

6.5.13. Elaborar, solicitar e manter documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam os recursos de TIC;

6.5.14. Definir e manter, em documento específico, procedimentos de salvaguarda das informações dos recursos de TIC, visando atender requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes de segurança;

6.5.15. Assegurar que os procedimentos de Gestão da Continuidade de Negócios sejam executados em conformidade com os requisitos de segurança da informação e comunicação estabelecidos;

6.5.16. Autorizar a liberação do uso de dispositivos móveis, institucionais ou particulares, pelos colaboradores, somente quando estritamente necessário ao desenvolvimento da atividade profissional;

6.5.17. Gerenciar as vulnerabilidades e ameaças nos processos e atividades, as quais devem ser tratadas diligentemente de modo a mitigar os riscos ao negócio.

6.6. Consultoria Jurídica

6.6.1. Apoiar a **NIVA** nos processos de contratações e aquisições, validando se os controles de segurança da informação estão aplicados;

6.6.2. Fornecer ao CSIC orientações a respeito da conformidade legal nos seguintes temas:

6.6.2.1. Direitos de propriedade intelectual;

6.6.2.2. Proteção de registros organizacionais;

6.6.2.3. Proteção de dados e privacidade de informações pessoais;

6.6.2.4. Prevenção de mau uso de recursos de processamento de informação;

6.6.2.5. Segurança da Informação e Comunicação;

6.6.2.6. Guarda de registros de conexão e dados cadastrais;

6.6.2.7. Combate à corrupção;

6.6.2.8. Regulamentação de controles de criptografia.

6.7. Departamento de Recursos Humanos

6.7.1. Apoiar o CSIC na elaboração de campanhas de conscientização e materiais de divulgação e alerta em segurança da informação e comunicação;

6.7.2. Estipular controles de segurança especificamente relacionados aos processos de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões);

6.7.3. Comunicar ao Canal de Atendimento o fim do contrato de trabalho de empregado para que os acessos destes sejam desativados;

6.7.4. Comunicar ao Departamento Administrativo o fim do contrato de trabalho de empregado para que sejam recolhidos os recursos de TIC de posse do colaborador;

6.7.5. Cabe ao Departamento de Recursos Humanos entregar a PSIC aos novos empregados na ocasião da admissão.

6.8. Departamento de Marketing

6.8.1. Apoiar o CSIC na elaboração de campanhas de conscientização e materiais de divulgação e alerta em segurança da informação e comunicação;

6.8.2. Monitorar e orientar as atividades das equipes responsáveis pela gestão dos perfis oficiais da **NIVA** nas mídias sociais, assim como por quaisquer outros canais de comunicação oficiais com o público externo.

6.9. Departamento Administrativo

6.9.1. Estabelecer perímetros de segurança e controles de identificação e registro de acesso nas dependências da **NIVA** visando assegurar o acesso somente a terceiros e visitantes autorizados aos recursos de TIC homologados;

6.9.2. Realizar o monitoramento dos ambientes físicos visando a eficácia dos controles implantados, a proteção de seu patrimônio e a reputação da **NIVA**;

6.9.3. Apoiar o Canal de Atendimento na inspeção dos recursos de TIC, sempre que considerar necessário;

6.9.4. Realizar o controle de fornecimento e devolução de recursos de TIC e credenciais de acesso sob sua responsabilidade, especialmente daqueles que detenham características de mobilidade;

6.9.5. Mapear e inventariar os recursos de TIC da **NIVA**.

6.10. Gestores da NIVA

6.10.1. Cumprir, fazer cumprir e gerenciar o cumprimento desta PSIC e demais documentos complementares por parte dos colaboradores de suas equipes;

6.10.2. Gerenciar os controles de segurança da informação e comunicação específicos dos processos de seus Departamentos, especialmente daquelas atividades que não sejam dependentes de recursos de TIC;

6.10.3. Zelar pelo bom uso dos recursos de TIC relacionados aos processos de seu Departamento;

6.10.4. Implementar ou solicitar os controles adicionais de segurança necessários e capazes de garantir a continuidade do negócio de seu Departamento;

6.10.5. Comunicar de forma imediata e formalmente ao Canal de Atendimento quando do término dos contratos de prestação de serviços, para que os acessos dos envolvidos sejam revogados;

6.10.6. Ao identificar eventos de segurança de informação e comunicação ou qualquer ação duvidosa praticada por seus empregados, acionar a Equipe de resposta a incidentes de Segurança;

6.10.7. Quando necessário, elaborar documentos complementares a PSIC relacionados aos seus processos e submetê-los para avaliação do CSIC;

6.10.8. Realizar a gestão, inclusive da segurança da informação e comunicação, dos recursos de TIC de propriedade da **NIVA** ou que estão sob sua responsabilidade.

6.11. Colaboradores e Terceiros

6.11.1. Cumprir e fazer cumprir, manter-se atualizado com esta PSIC e demais documentos que a compõem;

6.11.2. Utilizar de forma responsável, profissional, ética e legal as informações e os recursos de TIC, respeitando os direitos e as permissões de uso concedidas pela **NIVA**;

6.11.3. Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia;

6.11.4. Não revelar e/ou divulgar qualquer informação de propriedade ou sob a responsabilidade sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico;

6.11.5. Utilizar todos os recursos tangíveis e intangíveis, quando autorizados, somente para fins profissionais;

6.11.6. Utilizar as marcas e outros sinais distintivos, patentes, desenhos industriais, softwares e demais direitos de propriedade intelectual de titularidade da **NIVA** somente para finalidades profissionais, que estejam adequadas com visão, missão e os valores da empresa e de acordo com a atividade e função exercida;

6.11.7. Assegurar a proteção das informações que tiver contato, além de manter seu sigilo de acordo com a classificação imposta;

6.11.8. Zelar pela segurança da sua credencial de acesso, não a compartilhando, divulgando ou transferindo a terceiros;

6.11.9. Comunicar imediatamente ao Canal de Atendimento em caso de perda, extravio ou furto de recursos de TIC e credenciais de acesso para que possa ser feita a remoção destes acessos aos ambientes físicos e lógicos da **NIVA**;

6.11.10. Responder por toda e qualquer atividade nos recursos de TIC da **NIVA** realizada mediante o uso de suas credenciais de acesso;

6.11.11. Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais da **NIVA**;

6.11.12. Reportar formalmente ao CSIC quaisquer eventos relativos à violação de segurança de informação e comunicação ou atividades suspeitas das quais tiver conhecimento.

7. PENALIDADES

7.1. **Violações:** Os incidentes de segurança da informação identificados devem ser avaliados pelo CSIC. Ao se constatar uma violação, o CSIC deve encaminhar o relatório para a Comissão de Ética e Ouvidoria que, após análise, poderá instaurar e apurar as

responsabilidades dos envolvidos, visando aplicação de sanções administrativas cabíveis previstas em cláusulas contratuais, regimento pessoal e outros documentos normativos da **NIVA**, além da legislação vigente.

7.2. **Tentativa de Burla**: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

8. DISPOSIÇÕES FINAIS

8.1. O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas e Procedimentos aplicáveis pela **NIVA**.

8.2. Esta PSIC, bem como os demais documentos que a complementam, encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao CSIC.

8.3. Qualquer dúvida relativa a esta PSIC deve ser encaminhada ao CSIC para tratamento.

8.4. Esta PSIC entra em vigor na data de sua publicação.

9. DOCUMENTOS DE REFERÊNCIA

Esta PSIC é complementada pelos documentos de Normas e Procedimentos da **NIVA**.

10. DEFINIÇÕES PSIC, NORMAS E PROCEDIMENTOS

10.1. **Ambiente Lógico**: Ambiente virtual composto pelos recursos de TIC, sistemas, bases de dados, da **NIVA**, de forma intangível.

10.2. **Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano à **NIVA**.

10.3. **Aplicativos de Comunicação Instantânea:** Conjuntos de códigos e instruções compilados, executados ou interpretados por um recurso de Tecnologia da Informação e Comunicação, armazenados em um dispositivo ou na nuvem, que são usados para troca rápida de mensagens, conteúdos e informações multimídia.

10.4. **Autenticidade:** Garantia de que a informação foi criada, editada ou emitida por quem se disse ter sido, sendo capaz de gerar evidências não repudiáveis em relação ao criador, editor ou emissor.

10.5. ***Backup*:** Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de restauração.

10.6. **Bens imóveis:** aqueles que não podem ser deslocados de lugar, exemplo: terrenos, edificações.

10.7. **Bens móveis:** São aqueles que podem ser deslocados do lugar sem alteração de sua forma física, classificados como: Móveis, Utensílios, Veículos e Acessórios, Máquinas, Aparelhos, Equipamentos de Informática entre outros.

10.8. **Colaborador:** Empregado, estagiário, menor aprendiz ou qualquer outro indivíduo ocupante de cargo ou emprego na **NIVA**, exceto os dirigentes.

10.9. **Dirigentes:** Gestores da **NIVA**.

10.10. **Confidencialidade:** Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não autorizados.

10.11. **Credencial de Acesso:** É a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.

10.12. **Disponibilidade:** Garantia de que as informações e os recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

10.13. **Dispositivos Móveis:** equipamentos que podem ser facilmente transportados devido a sua portabilidade, com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexões com a Internet e outros sistemas, redes ou qualquer dispositivo.

10.14. **Dispositivos Removíveis de Armazenamento de Informação:** Dispositivos capazes de armazenar informações que pode ser removida do equipamento, possibilitando a portabilidade dos dados, como CD, DVD, *pen drive e* HD externo.

10.15. **Homologação:** Processo de avaliação e aprovação técnica de recursos de TIC para serem utilizados dentro do ambiente da **NIVA.**

10.16. **Incidente de Segurança da Informação e Comunicação:** Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede que indica possível violação à Política de Segurança da Informação e Comunicação ou documentos complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à Segurança da Informação.

10.17. **Informação:** É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

10.18. **Integridade:** Garantia de que as informações estejam fidedignas em relação à última alteração durante o seu ciclo de vida.

10.19. **Internet:** Rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente.

10.20. **Legalidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

10.21. Recurso: É qualquer coisa que tenha valor material ou imaterial, sendo tangível ou intangível, para a **NIVA** e precisa ser adequadamente protegido.

10.22. Recurso Tangível: Caracteriza-se por possuir um corpo físico.

10.23. Recurso Intangível: Todo elemento que possui valor para a **NIVA** e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando a dados, reputação, imagem, marca e conhecimento.

10.24. Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC): Hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

10.25. Repositórios Digitais: Plataformas de armazenamento na Internet, a exemplo, mas não se limitando ao *Google Drive, OneDrive, Dropbox, iCloud, Box*, *SugarSync*, *Slideshare* e *Scribd.*

10.26. Risco: Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

10.27. Segurança da Informação e Comunicação: É a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação e os recursos de TIC que as contêm dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos às atividades em caso de incidentes, além de maximizar o retorno dos investimentos e de novas oportunidades de transação.

10.28. Sigilo profissional: Trata da manutenção de segredo para informação valiosa, cujo domínio de divulgação deva ser fechado, ou seja, restrito a um cliente, a uma organização ou a um grupo, uma vez que a ele é confiada a manipulação da informação.

10.29. Tentativa de Burla: Atos que busquem violar as diretrizes estabelecidas nos documentos normativos da **NIVA** e sejam frustrados por erro durante o planejamento ou durante sua execução.

10.30. Terceiro: Prestador de serviço, terceirizado, fornecedor, credenciado, consultor, instrutor e parceiro.

10.31. Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos da **NIVA.**