ASSOCIAÇÃO PRÓ-ENSINO EM SANTA CRUZ DO SUL

Política Geral de Segurança da Informação da APESC

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

ÍNDICE

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

1. INTRODUÇÃO

1.1. Segurança da Informação é o conjunto de processos, políticas e controles voltados à proteção de dados contra acessos não autorizados, alterações indevidas, destruição ou divulgação imprópria. Na APESC, ela é considerada elemento estratégico essencial à continuidade e integridade das operações e relacionamentos institucionais.

1.2. A APESC compreende que a manipulação de sua informação e/ou de seus CLIENTES passa por diferentes meios de armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

1.3. A APESC utiliza metodologias de Gestão de Riscos, Gestão de Vulnerabilidades, Gestão de Incidentes, Gestão de Identidade e Controle de Acesso, Controles de Acesso Físico, Desenvolvimento Seguro de Aplicações e Sistemas, Planos de Resposta a Incidentes, Classificação, Manuseio e Rotulagem da Informação e Campanhas de Conscientização para que os objetivos de proteção da informação sejam alcançados.

1.4. A APESC utiliza mecanismos, ferramentas e serviços de fabricantes mundialmente reconhecidos e certificados nos mais diversos padrões de segurança para suportar sua estratégia de Segurança da Informação.

1.5. A APESC estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas e normas legais, administrativas e internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção das suas informações e de seus CLIENTES.

2. PROPÓSITO

2.1. Esta política tem por propósito estabelecer diretrizes e normas de Segurança da Informação que permitam à APESC adotar padrões de comportamento seguros, adequados às suas metas e necessidades.

2.2. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para segurança da informação.

2.3. Resguardar as informações da APESC, e de seus CLIENTES, garantindo requisitos adequados de confidencialidade, integridade, disponibilidade e privacidade.

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal da APESC.

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

2.5. Minimizar os riscos de perdas financeiras, prejuízo da imagem, de participação no mercado, da confiança de CLIENTES ou de qualquer outro impacto negativo nas atividades da APESC como resultado de falhas de segurança.

3. ESCOPO

3.1. Esta política se aplica a todos os empregados, prestadores de serviço, contratados, parceiros comerciais e quaisquer terceiros que, de forma direta ou indireta, tenham acesso às informações da APESC, por qualquer meio (presencial ou remoto).

4. DIRETRIZES

4.1. O objetivo da Gestão de Segurança da Informação da APESC é garantir a administração sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos.

4.2. O Comitê Gestor de Segurança da Informação está comprometido com uma gestão efetiva de segurança da informação na APESC, adotando todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e cumprida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da APESC.

4.3. É responsabilidade da APESC:

4.3.1. Elaborar, implantar e cumprir políticas, normas legais e administrativas e procedimentos de segurança da informação, garantindo que os requisitos adequados de confidencialidade, integridade, disponibilidade e privacidade da informação da APESC e de seus CLIENTES sejam atingidos através da adoção de controles contra ameaças provenientes de fontes externas e internas.

4.3.2. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas.

4.3.3. Garantir a educação e conscientização sobre as práticas de Segurança da Informação adotadas pela APESC.

4.3.4. Atender integralmente aos requisitos de Segurança da Informação aplicáveis ou exigidos por regulamentações, leis e cláusulas contratuais.

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

4.3.5. Tratar integralmente incidentes de Segurança da Informação, garantindo que eles sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicado às autoridades apropriadas.

4.3.6. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de resposta a incidentes.

4.3.7. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

5. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A APESC disponibiliza o endereço de e-mail seguranca@unisc.br e os ramais 7420 (Setor de Tecnologia UNISC) e 7441 (Setor de Tecnologia HSC) para reporte de incidentes de segurança, com prazo de resposta inicial de até 24 horas úteis.

A APESC comunicará à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidentes de segurança, que possam acarretar risco ou dano relevante aos titulares, cuja comunicação deverá mencionar, no mínimo:

I. a descrição da natureza dos dados pessoais afetados;

II. as informações sobre os titulares envolvidos;

III. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comerciais e industriais;

IV. os riscos relacionados ao incidente;

V. a causa do incidente;

VI. o impacto do incidente;

VII. os motivos da demora, no caso da comunicação não ter sido imediata; e

VIII. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

6. PAPÉIS E RESPONSABILIDADES

6.1. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

6.1.1. É responsabilidade do COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE:

6.1.1.1. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à Segurança da Informação.

6.1.1.2. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação.

6.1.1.3. Garantir que as atividades de Segurança da Informação sejam executadas em conformidade com a Política Geral de Segurança da Informação e com a Lei Geral de Proteção de Dados.

6.1.1.4. Promover a divulgação das Políticas de Segurança da Informação e tomar as ações necessárias para disseminar uma cultura de Segurança da Informação no ambiente da APESC.

6.1.1.5. Analisar casos que se aplicam as sanções citadas no item 7 deste documento.

6.2. ÁREA DE SEGURANÇA DA INFORMAÇÃO

6.2.1. É responsabilidade da área de Segurança da Informação:

6.2.1.1. Conduzir a Gestão e Operação da Segurança da Informação, tendo como base esta política e demais resoluções do Comitê Gestor de Segurança da Informação e Privacidade.

6.2.1.2. Apoiar o Comitê Gestor de Segurança da Informação e Privacidade em suas deliberações.

6.2.1.3. Elaborar e propor ao Comitê Gestor de Segurança da Informação e Privacidade as normas e procedimentos de Segurança da Informação, necessários para se fazer cumprir a Política Geral de Segurança da Informação.

6.2.1.4. Identificar e avaliar as principais ameaças à Segurança da Informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

6.2.1.5. Efetivar as ações cabíveis para se fazer cumprir os termos desta política;

6.2.1.6. Realizar a gestão dos incidentes de Segurança da Informação, garantindo tratamento adequado.

6.3. SETOR DE RECURSOS HUMANOS

6.3.1. É responsabilidade do Setor de Recursos Humanos:

6.3.1.1. Auxiliar na disseminação da cultura de Segurança da Informação.

6.3.1.2. Suportar a definição e execução de ações disciplinares aplicadas pela APESC.

6.4. GESTORES

6.4.1. É responsabilidade dos gestores:

6.4.1.1. Solicitar à equipe de tecnologia da informação a concessão ou revogação de acesso à informação ou sistemas de informação para os empregados da sua área conforme suas atividades laborais.

6.4.1.2. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os empregados sob sua gestão.

6.4.1.3. Auxiliar na disseminação da cultura de Segurança da Informação.

6.4.1.4. Exigir dos empregados sob sua gestão o conhecimento da política e normas de Segurança da Informação, assim como a participação das campanhas ofertadas pela Área de Segurança da Informação.

6.5. ASSESSORIA JURÍDICA

6.5.1. É responsabilidade da assessoria jurídica:

6.5.1.1. Acompanhar eventuais alterações legais e/ou regulatórias.

6.5.1.2. Incluir nos contratos cláusulas específicas relacionadas à Segurança da Informação.

6.5.1.3. Tomar as providências jurídicas cabíveis em casos de incidentes.

6.5.1.4. Garantir que as bases legais utilizadas no tratamento de dados pessoais estejam de acordo com a legislação.

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

6.6. TECNOLOGIA DA INFORMAÇÃO

6.6.1. É responsabilidade da gerência de tecnologia da informação:

6.6.1.1. Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para empregados e/ou prestadores de serviços.

6.6.1.2. Conceder, quando autorizado, o acesso aos empregados e/ou prestadores de serviços, conforme indicado pelos gestores das áreas.

6.6.1.3. Revogar, quando solicitado, o acesso dos empregados e/ou prestadores de serviço, conforme indicado pelos gestores da informação.

6.6.1.4. Apoiar a revisão periódica da validade de credenciais de acesso dos empregados e/ou prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

6.6.1.5. Executar procedimentos de descarte de informações ao término da vida útil dos ativos no âmbito tecnológico, utilizando as boas práticas e técnicas que tornem as informações originais irrecuperáveis.

6.6.1.6. Manter o inventário dos equipamentos fornecidos pela APESC aos seus empregados para o desempenho de suas atividades segundo as normas definidas pela Gerência de Segurança da Informação.

6.6.1.7. Documentar e monitorar todas as contas bem como analisar atividades suspeitas reportadas pelas ferramentas disponíveis.

6.6.1.8. Implementar e manter os controles de segurança definidos pela Gerência de Segurança da Informação no âmbito tecnológico.

6.6.1.9. Revogar as contas de acesso durante o desligamento e/ou encerramento de contrato de empregados e prestadores de serviço.

6.6.1.10. Auxiliar na disseminação da cultura de Segurança da Informação.

6.7. USUÁRIOS DA INFORMAÇÃO

6.7.1. É responsabilidade dos Usuários da Informação:

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

6.7.1.1. Cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

6.7.1.2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos à Gerência de Segurança da Informação através do e-mail seguranca@unisc.br;

6.7.1.3. Participar das campanhas de conscientização de segurança da informação.

6.7.1.4. Zelar pela segurança de suas credenciais (nome de usuário, senha, múltiplo fator de autenticação e chaves privadas) corporativas, departamentais ou de rede.

6.7.1.5. Zelar pela segurança dos documentos de sua responsabilidade (físicos e digitais), informações institucionais e de ativos computacionais.

6.7.1.6. Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política e que exponha ou possa expor a risco a segurança das informações ou dos recursos computacionais da APESC.

7. SANÇÕES

7.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política e das demais normas e procedimentos de Segurança da Informação da APESC, estão sujeitas a incidência de penalidades e medidas disciplinares, inclusive rescisão contratual por justa causa.

7.2. A apuração de violações segue rito formal conduzido pelas áreas Jurídica, de Segurança da Informação e Recursos Humanos, assegurando direito à ampla defesa e ao contraditório aos envolvidos

8. CASOS OMISSOS

8.1. Os casos omissos são avaliados pelo Comitê Gestor de Segurança da Informação e Privacidade para posterior deliberação.

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

9. REVISÕES

9.1. Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação e Privacidade.

10. COMPROMETIMENTO DA ALTA DIREÇÃO

10.1. O conselho da APESC possui o compromisso para a melhoria contínua dos procedimentos relacionados à Segurança da Informação, mantendo a APESC em conformidade com normas legais e regulamentares sobre os referidos temas e guiada pelos princípios, conceitos, valores e práticas aqui adotados, tem o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da APESC ou por ela controlados e dos sistemas de informação por ela utilizados, objetivando garantir sua preservação, além de proteger os direitos fundamentais de liberdade e de privacidade da pessoa natural.

11. GESTÃO DA POLÍTICA

11.1. A Política Geral de Segurança da Informação é aprovada pelo Comitê Gestor de Segurança da Informação e Privacidade, em conjunto com o conselho da APESC.

11.2. Todos os usuários com acesso às informações da APESC devem formalizar ciência e aceitação desta política, mediante assinatura física ou eletrônica, como parte dos processos de admissão, contratação de terceiros e concessão de acesso.

11.3. A presente política foi aprovada no dia 09/06/2025.

rafaelh@unisc.br
Rafael Henn
Presidência da APESC

heron@unisc.br
Heron Begnis
Reitoria

rolf@unisc.br
Rolf Molz
Diretoria Hospital Santa Cruz

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

neimar@unisc.br
Neimar dos Santos
Assessoria Jurídica

leandro@unisc.br
Leandro Pinto Fava
Setor de Tecnologia

felipesantos@unisc.br
Felipe dos Santos
Hospital Santa Cruz

luci@unisc.br
Luci Elaine Kramer

Cepru

annie1@unisc.br
Annie Carniel
LGPD Hospital Santa Cruz

fabianam@unisc.br
Fabiana da Silva
Recursos Humanos

libano@unisc.br
Luluani Libano
Comunicação e Marketing

cpereira@unisc.br
Cristiano Pereira
Segurança da Informação

crism@unisc.br
Cristiane Iserhard Machado Educar-se

apesc DOCUMENTO PÚBLICO

Documento assinado eletronicamente nos moldes do art. 10 da MP 2200/01 e Lei 14063/20
[Hash SHA256] bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON) em 12/06/2025 às 17:39:27

Versao2-Política Geral da Seguranca da Informacao da APESC

Data e Hora de Criação: 09/06/2025 às 16:34:48

Documentos que originaram esse envelope:
- Versao2-Política Geral da Seguranca da Informacao.pdf (Arquivo PDF) - 11 página(s)

Hashs únicas referente à esse envelope de documentos

[SHA256]: bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a
[SHA512]: d670e8356703c68d08b6060cd77a8f1c934491c20c99d0cee4e12063071efc1def0efc6b48e0a50896d50447c45a16620eb77237ec880c681e1195088b08049a

Lista de assinaturas solicitadas e associadas à esse envelope

ASSINADO - Annie Carniel (annie1@unisc.br)
Data/Hora: 10/06/2025 - 10:10:29, IP: 200.17.83.174
[SHA256]: b2a50410c27e2e251323e0d173fef4dc441540dd04c0e64f20498f47a292d9ec

ASSINADO - Cristiano Maynart Pereira (cpereira@unisc.br)
Data/Hora: 09/06/2025 - 16:42:31, IP: 200.17.83.229
[SHA256]: 2ec634acee0a1005a05136f0af7c31f1eecf856fd0cce7d21319f9feeb957de0

ASSINADO - Cristiane Iserhard Machado (crism@unisc.br)
Data/Hora: 10/06/2025 - 09:43:42, IP: 200.17.83.238, Geolocalização: [-29.697184, -52.437297]
[SHA256]: c05d32cc55a287cc7041011cabae8ff9fa5327a7f95b69326cba50554a0a8a0b

ASSINADO - Fabiana Metzdorf Da Silva (fabianam@unisc.br)
Data/Hora: 09/06/2025 - 16:44:07, IP: 200.17.83.239
[SHA256]: 7e348d96d6b52b3037e2a30d73306cedb2787c801c7f8706794a1a4870149073

ASSINADO - Felipe dos Santos (felipesantos@unisc.br)
Data/Hora: 09/06/2025 - 16:51:25, IP: 200.17.83.174
[SHA256]: 4639ec2a41500da2514dfa65e41c34720a28650d15861c0815ef8143e6f56516

ASSINADO - Heron Begnis (heron@unisc.br)
Data/Hora: 10/06/2025 - 11:39:06, IP: 200.17.83.238, Geolocalização: [-29.697178, -52.438402]
[SHA256]: a4e474a9ed2a5504d18844346fc73e5bd84276cd0b5a76b11996ba5780fff0b5

ASSINADO - Leandro Pinto Fava (leandro@unisc.br)
Data/Hora: 11/06/2025 - 11:09:37, IP: 200.17.83.230
[SHA256]: 91832d2bb2ba392b4ccd3a8e100dd35c828e966818f7e7c42bed467336310a69

ASSINADO - Luluani Libano (libano@unisc.br)
Data/Hora: 09/06/2025 - 17:06:18, IP: 200.17.83.239
[SHA256]: 68afb514ab74bf6e02a51213f6ff4feb2a5e21fa6d9a4394f3759748a0479d6d

ASSINADO - Luci Elaine Kramer (luci@unisc.br)
Data/Hora: 12/06/2025 - 17:39:27, IP: 200.17.83.235
[SHA256]: 08f34d3d441b5e45b610581c47936dd5c7027b88fdd5a5c79aec9e3546b2ca34

ASSINADO - Neimar Santos Da Silva (neimar@unisc.br)
Data/Hora: 11/06/2025 - 11:15:02, IP: 200.17.83.232
[SHA256]: e6057e91fb42e35e87fa9ec4188ac9c20cc154890ea74b0c90a7476bde9b6ac0

ASSINADO - Rafael Frederico Henn (rafaelh@unisc.br)
Data/Hora: 10/06/2025 - 08:21:13, IP: 200.17.83.231, Geolocalização: [-29.697177, -52.438414]
[SHA256]: 46f8d197c9e7ac78b7d3a44688274d70207891d642b7d25f1e7b4555541c8ee9

Documento em conformidade com o padrão de assinatura digital ICP-Brasil e validado de acordo com o Instituto Nacional de Tecnologia da Informação

Os registros de assinatura presentes nesse documento pertencem única e exclusivamente a esse envelope.
Documento final gerado e certificado por **Universidade de Santa Cruz do Sul**

Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON) em 12/06/2025 às 17:39:27

Versao2-Política Geral da Seguranca da Informacao da APESC

Data e Hora de Criação: 09/06/2025 às 16:34:48

Documentos que originaram esse envelope:

- Versao2-Política Geral da Seguranca da Informacao.pdf (Arquivo PDF) - 11 página(s)

Hashs únicas referente à esse envelope de documentos

[SHA256]: bbaad99430725e5704b838123c6ff0e4d6072ea339e7660c07e64179a2f7ad0a

[SHA512]: d670e8356703c68d08b6060cd77a8f1c934491c20c99d0cee4e12063071efc1def0efc6b48e0a50896d50447c45a16620eb77237ec880c681e1195088b08049a

Lista de assinaturas solicitadas e associadas à esse envelope

ASSINADO - Rolf Molz (rolf@unisc.br)

Data/Hora: 09/06/2025 - 16:45:39, IP: 200.17.83.177

[SHA256]: 56a55a6ffd48921826d9dad5f566b4334808cbb9243f55dca80c96a8973b5f11

Histórico de eventos registrados neste envelope

12/06/2025 17:39:28 - Envelope finalizado por luci@unisc.br, IP 200.17.83.235

12/06/2025 17:39:27 - Assinatura realizada por luci@unisc.br, IP 200.17.83.235

12/06/2025 17:38:29 - Envelope visualizado por luci@unisc.br, IP 200.17.83.235

11/06/2025 11:15:02 - Assinatura realizada por neimar@unisc.br, IP 200.17.83.232

11/06/2025 11:14:53 - Envelope visualizado por neimar@unisc.br, IP 200.17.83.232

11/06/2025 11:09:37 - Assinatura realizada por leandro@unisc.br, IP 200.17.83.230

11/06/2025 11:09:14 - Envelope visualizado por leandro@unisc.br, IP 200.17.83.230

10/06/2025 11:39:06 - Assinatura realizada por heron@unisc.br, IP 200.17.83.238

10/06/2025 11:38:35 - Envelope visualizado por heron@unisc.br, IP 200.17.83.238

10/06/2025 10:10:29 - Assinatura realizada por annie1@unisc.br, IP 200.17.83.174

10/06/2025 09:43:42 - Assinatura realizada por crism@unisc.br, IP 200.17.83.238

10/06/2025 09:43:23 - Envelope visualizado por crism@unisc.br, IP 200.17.83.238

10/06/2025 08:21:13 - Assinatura realizada por rafaelh@unisc.br, IP 200.17.83.231

10/06/2025 08:20:53 - Envelope visualizado por rafaelh@unisc.br, IP 200.17.83.231

09/06/2025 17:06:18 - Assinatura realizada por libano@unisc.br, IP 200.17.83.239

09/06/2025 17:05:26 - Envelope visualizado por libano@unisc.br, IP 200.17.83.239

09/06/2025 16:51:25 - Assinatura realizada por felipesantos@unisc.br, IP 200.17.83.174

09/06/2025 16:50:18 - Envelope visualizado por felipesantos@unisc.br, IP 200.17.83.174

09/06/2025 16:45:39 - Assinatura realizada por rolf@unisc.br, IP 200.17.83.177

09/06/2025 16:45:24 - Envelope visualizado por rolf@unisc.br, IP 200.17.83.177

09/06/2025 16:44:07 - Assinatura realizada por fabianam@unisc.br, IP 200.17.83.239

09/06/2025 16:43:42 - Envelope visualizado por fabianam@unisc.br, IP 200.17.83.239

09/06/2025 16:42:31 - Assinatura realizada por cpereira@unisc.br, IP 200.17.83.229

09/06/2025 16:42:10 - Envelope visualizado por cpereira@unisc.br, IP 200.17.83.229

09/06/2025 16:42:07 - Envelope visualizado por annie1@unisc.br, IP 200.17.83.174

09/06/2025 16:40:33 - Envelope registrado na Blockchain por cpereira@unisc.br, IP 200.17.83.229

09/06/2025 16:40:30 - Envelope encaminhado para assinaturas por cpereira@unisc.br, IP 200.17.83.229

09/06/2025 16:34:50 - Envelope criado por cpereira@unisc.br, IP 200.17.83.229

Documento em conformidade com o padrão de assinatura digital ICP-Brasil e validado de acordo com o Instituto Nacional de Tecnologia da Informação

Os registros de assinatura presentes nesse documento pertencem única e exclusivamente a esse envelope.
Documento final gerado e certificado por **Universidade de Santa Cruz do Sul**