



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 1/30

CONTROLE DE APROVAÇÃO:

AUTOR: MAURICIO CASTRO ALVES	CARGO: IMPLEMENTADOR SÊNIOR LÍDER ISO 27001/27701	DATA: 12/06/2023
REVISÃO MARCIO CASTRO ALVES	CARGO: CLO – CHIEF LEGAL OFFICER GOVERTRUST	DATA: 12/06/2023
APROVAÇÃO: ADILSON PAULICENA DA SILVA	CARGO: DIRETORIA EXECUTIVA	DATA: 12/06/2023

CONTROLE DE VERSÕES/ MODIFICAÇÕES

VERSÃO: 001	DATA: 12/06/2023	ALTERAÇÕES EM RELAÇÃO À EMISSÃO ANTERIOR EMISSÃO INICIAL
VERSÃO: 002	DATA: 12/06/2023	ALTERAÇÕES EM RELAÇÃO À EMISSÃO ANTERIOR APONTAMENTO DOS CONTROLES CONSIDERADOS

SUMÁRIO

1. OBJETIVO	01
2. ABRANGÊNCIA	02
3. DEFINIÇÕES	03
4. CONTROLES	04
5. APLICABILIDADE DESTA POLÍTICA	05
6. INTEGRAÇÃO E COMUNICAÇÃO DA PSI	05
7. DOS CUSTODIANTES DA INFORMAÇÃO	11
8. CONTROLES PROPOSTOS	11
9. COMITE DE PRIVACIDADE E SEGURANÇA	17
10. CORREIO ELETRÔNICO	18
11. INTERNET	18
12. IDENTIFICAÇÃO	20
13. DISPOSITIVOS TECNOLÓGICOS	22
14. DISPOSITIVOS MÓVEIS	22
15. DATACENTER	24
16. BACKUP	25
17. MONITORAMENTO	25
18. CONTROLE DE ACESSO	26
19. LGPD	27
20. BYOD	29
21. DISPOSIÇÕES FINAIS	30

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 2/30

1. OBJETIVO:

NOVA XS Tecnologia da Informação LTDA, inscrita no **C.N.P.J.** sob o nº **18.494.220/0001-84**, com sede à Praça Gilson Ribeiro Macedo nº 15, sala PD LE 10, Shopping Tropical, Setor Centro, Caldas Novas - GO, CEP: 75.680-012, neste ato representada por **Douglas Fernandes, RG nº 12.794.327 SSP/SP** e **C.P.F. nº 040.497.558-58**, doravante denominada “**NOSSA ORGANIZAÇÃO**”.

Este documento estabelece as diretrizes que permitam aos colaboradores e prestadores de serviços da **NOSSA ORGANIZAÇÃO** seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal das informações e do indivíduo, norteando a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento observando os seguinte tópicos:

I. Preservar as informações da **NOSSA ORGANIZAÇÃO** quanto à:

Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

II. **Sobre a Lei 13.709/2018 (LGPD)** – Esta política possui a relevância sobre a forma de tratamento das informações (dados identificáveis e (ou) sensíveis) dos colaboradores, e (ou) Prestadores de serviços que tratam dados identificáveis estritamente necessários e justificados em nome da **NOSSA ORGANIZAÇÃO**, Informações de tratamento devidamente ratificadas através das declarações (anexas) aos contratos de prestação de serviços e (ou) acordo de trabalho entre o Controlador e Operadores de dados subordinados. Estes documentos, permanecem em constante atualização e identificados por indicadores

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 3/30

únicos e de versões aprovadas. Esta declaração, torna-se respaldada pelas seguintes bases legais da LGPD: (**Consentimento, Legítimo interesse, Contratos, Obrigação legal, Execução de políticas públicas, Estudos de órgãos de pesquisa, Processo Judicial, Proteção à vida, Tutela da vida, Proteção ao crédito**), e obedece os seguintes princípios para o tratamento destas informações: (**Finalidade, Adequação, Livre Acesso, Necessidade, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação, Prestação de contas**).

2. ABRANGÊNCIA:

Colaboradores internos, prestadores de serviços, integrantes de corpos clínicos e quaisquer outros profissionais atuantes nas dependências, físicas ou virtuais, da **NOSSA ORGANIZAÇÃO** em todas as suas unidades.

- I. As cláusulas e indicações dos controles em segurança da Informação dispostos nesta política, deverão ser considerados por todos os colaboradores internos e externos da **NOSSA ORGANIZAÇÃO**, sendo esta norma, a referência adotada para o tratamento de informações físicas ou digitais em qualquer formato e (ou) origem, e da mesma forma, todos os dispositivos informáticos desta Organização relacionados ao tratamento, de informações, **devendo ser apresentada aos antigos e novos colaboradores** para o conhecimento integral das regras de tratamento de dados da **NOSSA ORGANIZAÇÃO**; fica estabelecido, que os controles efetuados aos ativos de informação da **NOSSA ORGANIZAÇÃO**, permanecerão sob a tutela, monitoramento e controle integral da Administração sem a necessidade de aviso prévio, tomando como base as normais ISO/IEC 27001 | 27701.
- II. É de obrigação de todos os colaboradores da **NOSSA ORGANIZAÇÃO**, manterem-se atualizados acerca das versões atualizadas desta política de Segurança da informação, sendo livre o acesso aos canais de comunicação para dirimir qualquer dúvida referente ao modo de tratamento de qualquer tipo de informação dentro da **NOSSA ORGANIZAÇÃO**.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 4/30

3. DEFINIÇÕES:

PSI: Política de Segurança da Informação.

DPO: Data Protection Officer – Encarregado de Proteção de Dados.

Comitê de Privacidade e Segurança da Informação: Gestores das áreas Administrativas da NOSSA ORGANIZAÇÃO, eleitos como representantes, e multiplicadores da cultura de Segurança da Informação, exemplo: áreas: Marketing, Jurídico, Tecnologia, Segurança, Fiscal, financeiro, etc.

SGSI – Sistema de Gestão de Segurança da Informação

SGPI – Sistema de Gestão de Privacidade da Informação

4. CONTROLE:

O Controle é efetuado pelas áreas de Tecnologia, Segurança da Informação e Jurídico da NOSSA ORGANIZAÇÃO, com base nas normas de Governança de Dados ISO/IEC 27001 | 27701, e declaram os seguintes relatórios de conformidade como dispositivos para ratificação do nosso Programa de Governança de Dados: Declaração de escopo do SGSI, Política de Segurança da Informação, Processo de risco de Segurança da Informação (avaliação, tratamento e resultados), Objetivos de segurança da Informação, Competências de pessoas, Controle de Informação documentada, Planejamento e controle operacional, Resultados de monitorização e medição, Programa de auditoria interna e resultados, Comentários da gestão, Não conformidades e ações corretivas com seus respectivos resultados, e a última declaração de aplicabilidade aprovada pela diretoria.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 5/30

5. APLICABILIDADE DESTA POLÍTICA:

- I. Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela **NOSSA ORGANIZAÇÃO** pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.
- II. Os equipamentos de informática e comunicação, sistemas e informações, são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços e não desvirtuará a natureza corporativa de todos os dados assim classificados pelas normas internas aplicáveis, tampouco da natureza sigilosa ou confidencial de determinadas informações. Toda a informação classificada como CONFIDENCIAL, deverá ser referenciada em aditivo contratual e assinada pela parte receptora, com o intuito de definir os direitos e obrigações acerca do tratamento orientado para a conduta do receptor com relação às informações referenciadas com o teor CONFIDENCIAL e (ou) Restrito.na NOSSA ORGANIZAÇÃO.
- III. A **NOSSA ORGANIZAÇÃO**, por meio do COMITÊ DE PRIVACIDADE E SEGURANÇA poderá registrar todo o uso dos sistemas e serviços, visando a garantir a disponibilidade e a segurança das informações utilizadas.

6. INTEGRAÇÃO E COMUNICAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- I. A PSI – Política de Segurança da Informação, deverá ser comunicada em toda a organização; durante o processo de integração dos novos colaboradores, faz-se necessário, o acompanhamento das equipes de Segurança e Tecnologia da Informação para exercer treinamento específico para o reconhecimento do ambiente por parte do colaborador, e da mesma forma, acompanhar um roteiro de dicas de boas práticas através de checklist apropriado, e acultramento sobre as principais definições que envolvam a segurança da Informação, como

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO
SGSI | SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E
PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES
INTERNOS E EXTERNOS.

CLASSIFICAÇÃO:
RESTRITA

VERSÃO:
002

IDENTIFICADOR ÚNICO:

PSI_NOVAXS_05_2023.

DATA:
12/06/2023

PÁGINA:
6/30

por exemplo, a definição hierárquica da instituição, os principais canais de comunicação com as áreas de RH, Jurídico, Tecnologia e Segurança, e acompanhamento do colaborador para aferir a absorção de conhecimento e a coleta do termo de aceite e ciência acerca dos procedimentos institucionais.

- II. Deverá o COMITÊ DE PRIVACIDADE E SEGURANÇA, definir as melhores práticas para a integração dos novos colaboradores e a otimização cultural dos colaboradores antigos acerca das boas práticas de Tratamento de informações.
- III. As versões posteriores da PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, deverão ser revisadas anualmente e aprovadas pelo Comitê de Privacidade, Jurídico, e Diretoria da NOSSA ORGANIZAÇÃO, sendo observada a necessidade antecipada de revisão se necessário conforme a última declaração de Aplicabilidade e Controles de medidas corretivas dos ambientes informáticos.
- IV. Deverá constar em todos os contratos da **NOSSA ORGANIZAÇÃO** o anexo de Acordo de Confidencialidade ou a Cláusula de Confidencialidade, como condição imprescindível para que possam ser concedidos os acessos aos ativos de informação disponibilizados pela instituição.
- V. A responsabilidade em relação à segurança da informação deve ser comunicada em quaisquer fases de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.
- VI. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à área de Segurança da Informação e ao Comitê de Privacidade e Segurança da Informação para análise.
- VII. Os mecanismos do PCN – Plano de continuidade dos negócios, deverão ser Implementados através do SGSI – Sistema de Gestão de Segurança da Informação, e do SGPI – Sistema de Gestão de Privacidade da Informação, e executado anualmente com base nas matrizes de

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 7/30

gerenciamento de riscos da Organização pelas áreas de Tecnologia e Segurança da Informação.

Os seguintes procedimentos deverão ser observados para a Implementação dos SGSI | SGPI; Objetivo: Identificar vulnerabilidades no ciclo de vida das informações e realizar uma reflexão em conjunto com o ANEXO A da norma ISO\IEC 27001| 27701, onde existem 114 controles com a funcionalidade de mitigar as vulnerabilidades identificadas, corrigindo as imperfeições que podem interferir no fluxo sadio das informações dentro de uma organização.

Objetivos de Segurança da Informação, cláusulas (4 a 10) da norma ISO/IEC 27001:2013

I - Declaração de escopo do Sistema de Gestão de Segurança da Informação (SGSI): Trata-se do reconhecimento dos canais de comunicação da organização e delimitação das áreas de atuação do framework; é o momento onde a área de Segurança da Informação, identifica os heads da organização propondo a participação do comitê de Privacidade e Segurança da Informação para identificarem juntos, o fluxo de dados em cada célula, comumente reconhecido como Data Mapping de dados, também faz parte do planejamento para a adequação das organizações frente à Lei 13.709/2018 Lei geral de Proteção de Dados, pois através do reconhecimento dos canais de comunicação e apontamentos das bases de dados, inicia-se a delimitação dos ativos que deverão receber as tratativas de classificação das informações, definindo os níveis: Local, Público, Privado, Restrito, e Confidencial, possibilitando a delimitação do Escopo de Aplicação do Sistema de Gestão de Segurança da Informação.

II - PSI - Política de Segurança da Informação: é o documento que ratifica a introdução do SGSI definindo o modo de tratamento de tecnologia e informação por toda a organização devendo ser aprovado pela alta Gestão. Trata-se do documento central que definirá os procedimentos a serem realizados pelas áreas de controle da informação como o setor de Tecnologia, Marketing, Jurídico, Recursos Humanos e tantas outras. Este documento possui característica normativa dentro de uma organização, pois através dele, a alta gestão poderá instituir regras e sanções anexas, para todos

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 8/30

que a este documento, estiverem atrelados. Tipos de controles comuns em uma PSI: Política de cadastramento de usuários, política de senhas fortes, políticas de acesso às dependências da organização, política de identificação de agentes externos, política de resposta a incidentes, política de uso de imagem e recursos da organização etc.

III - Processos de Risco de Segurança da Informação (avaliação, e resultados): Trata-se da parte dos SGSI|SGPI onde são mapeadas as vulnerabilidades envolvendo todos os ativos de informação; a análise de riscos deverá considerar a classificação das prioridades urgentes do negócio para que sejam inseridos controles adequados na fase de tratamento de riscos. Alguns tipos de riscos que poderão ser identificados na fase de avaliação: Riscos relacionados a atualizações de softwares e sistemas de segurança, acesso não permitido a informações sensíveis para o negócio, exposição de ativos físicos a ameaças naturais, retomada de operações em caso de indisponibilidade de acesso ou comprometimento da integridade ou confidencialidade das informações etc.

IV - Processo de avaliação de Risco de Segurança da Informação (tratamento e resultados): Fase da gestão dos processos de governança de dados onde a área de Segurança da Informação poderá conduzir o Tratamento das vulnerabilidades reconhecidas com base na reflexão do ANEXO A da norma ISO/IEC 27001:2013 e na escolha entre um dos 114 controles elencados para mitigar os problemas relacionado à segurança das informações através do desenho de planos de ação direcionados às equipes correspondentes de cada setor do negócio.

V - Objetivos de Segurança da Informação: Parte fundamental do programa de governança onde será avaliada a efetividade dos planos de ação já desenhados e a reflexão acerca do cenário corrente do negócio com o intuito de aferir a produtividade do programa de governança e o escopo desenhado inicialmente. Trata-se do momento em que a organização já possui níveis de maturidade em segurança das informações com níveis aceitáveis e almeja perpetuar o ciclo sadio de tratamento das informações. Atingir os objetivos de segurança da informação, promove a eficiência do plano de comunicação geral e de continuidade do negócio PCN.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 9/30

VI - Competência de Pessoas: Este requisito, possui a relevância de desenvolver a capacitação de times e membros dos comitês de segurança e privacidade indicados pela organização referente as boas práticas de governança de dados e planos onda através de treinamentos de Instruções de trabalhos específicas às contingências do negócio para difundir a cultura de proteção de dados a todos os colaboradores.

VII - Controle de Informação documentada: providenciar a manutenção e o controle de toda documentação referente aos processos relacionados à segurança da informação e as rotinas associadas ao cuidado com as informações já classificadas **mantendo os cabeçalhos descritivos: Título, tipo de documento, indicador único, versão, classificação, data corrente e de emissão, autor, revisor, e aprovador do documento. A manutenção da informação ajuda no processo de reconhecimento do conteúdo e aculturamento sobre o controle da Segurança da Informação!**

VIII - Planejamento e controle operacional: Momento em que os gestores dos processos do SGSI estabelecerão indicadores de desempenho para processos continuados e melhoria do SGSI e apresentara-los aos times responsáveis pela Gestão da Corporação.

IX - Resultados de monitorização e medição: Trata-se dos processos de coleta e armazenamento de evidências físicas e (ou) digitais que ratificarão o compromisso da organização frente aos órgãos de fiscalização, com o intuito de legitimar o compromisso da organização com as boas práticas de governança de dados.

X - Programa de auditoria interna e resultados: Após os requisitos pretéritos terem sido atingidos, iniciam-se os procedimentos para perpetuar as rotinas já positivadas e aprovadas dentro do ambiente corporativo, trata-se de aferir os resultados e evidências colhidos a partir do desenho inicial do escopo do SGSI categorizando as evidências oriundas de cada setor da organização com o intuito de comprovar as boas práticas de governança.

XI - Comentários da Gestão: A organização já atingiu níveis de maturidade em um SGSI muito satisfatórios, e a alta gestão, deverá propor as linhas de informações direta aos stakeholders para

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 10/30

que consigam estabelecer uma avaliação crítica sobre os processos definidos e a relação destes procedimentos com a organização.

XII - Objetivos de Segurança da Informação: Parte fundamental do programa de governança onde será avaliada a efetividade dos planos de ação já desenhados e a reflexão acerca do cenário corrente do negócio com o intuito de aferir a produtividade do programa de governança e o escopo desenhado inicialmente. Trata-se do momento em que a organização já possui níveis de maturidade em segurança das informações com níveis aceitáveis e almeja perpetuar o ciclo sadio de tratamento das informações. Attingir os objetivos de segurança da informação, promove a eficiência do plano de comunicação geral e de continuidade do negócio PCN.

- VIII. Esta PSI será implementada na **NOSSA ORGANIZAÇÃO** por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou de prestação de serviço.
- IX. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação representará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

DAS RESPONSABILIDADES ESPECÍFICAS:

- X. Dos Colaboradores em Geral. Entende-se por colaborador toda e qualquer pessoa física, empregada, integrante de corpo clínico, prestadora de serviço preposta de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da **NOSSA ORGANIZAÇÃO**, mas a ela relacionada por suas funções e tarefas.
- XI. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a **NOSSA ORGANIZAÇÃO** e (ou) a terceiros, em decorrência da sua inobservância às diretrizes e normas aqui referidas.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 11/30

DOS COLABORADORES EM REGIME DE EXCEÇÃO TEMPORÁRIOS:

- XII. Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Privacidade e Segurança da Informação desta política através de Aditivo específico limitando a responsabilidade cível da Organização em caso de vazamento de dados.
- XIII. A concessão de acesso a informações poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

DOS GESTORES DE PESSOAS E (OU) PROCESSOS E COLABORADORES DA NOSSA ORGANIZAÇÃO:

- XIV. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para todas as partes envolvidas nos processos de tratamento de informações.

7. DOS CUSTODIANTES DA INFORMAÇÃO – CONTROLES DOS SGSI | SGPI INDICADOS

A5 - Política de Segurança da Informação
A6 - Organização da segurança da Informação
A7 - Segurança em RH
A8 - Gestão de Ativos
A9- Controle de Acesso
A10 - Criptografia
A11 - Segurança Física e do Ambiente
A12 - Segurança nas Operações
A13 - Segurança nas Comunicações
A14 - Aquisição, desenvolvimento e manutenção de Sistemas
A15 - Relacionamento na cadeia de suprimento
A16 - Incidentes de Segurança da Informação

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



**PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
SISTEMA DE GESTÃO DE SEGURANÇA E
PRIVACIDADE DAS INFORMAÇÕES.**

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 12/30

A17 - Continuidade de Negócios
A18 - Conformidade

CONTROLES PROPOSTOS

Section	Controle de segurança da informação
A5	Políticas de segurança da informação
A5.1	Orientação da direção para segurança da informação
A5.1.1	Políticas para segurança da informação
A5.1.2	Revisão das políticas de segurança da informação
A6	Organização da segurança da informação
A6.1	Organização interna
A6.1.1	Funções e responsabilidades de segurança da informação
A6.1.2	Segregação de funções
A6.1.3	Contato com autoridades
A6.1.4	Contato com grupos especiais
A6.1.5	Segurança da informação no gerenciamento de projetos
A6.2	Dispositivos moveis e trabalho remoto
A6.2.1	Política de dispositivo móvel
A6.2.2	Trabalho remoto
A7	Segurança em recursos Humanos
A7.1	Antes da contratação
A7.1.1	Seleção
A7.1.2	Termos e condições de contratação
A7.2	Durante a contratação
A7.2.1	Responsabilidades da Direção
A7.2.2	Conscientização, educação e treinamento em segurança da informação
A7.2.3	Processo disciplinar
A7.3	Encerramento e mudança da contratação
A7.3.1	Responsabilidades pelo encerramento ou mudanças da contratação
A8	Gestão de ativos
A8.1	Responsabilidade pelos ativos
A8.1.1	Inventário dos ativos
A8.1.2	Proprietário dos ativos

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 13/30

A8.1.3	Uso aceitável dos ativos
A8.1.4	Devolução de ativos
A8.2	Classificação da Informação
A8.2.1	Classificação da Informação
A8.2.2	Rótulos e tratamento da informação
A8.2.3	Tratamento dos ativos
A8.3	Tratamento de mídias
A8.3.1	Gerenciamento de mídias removíveis
A8.3.2	Descarte de mídias
A8.3.3	Transfêrência física de mídias
A9	Controle de acesso
A9.1	Requisitos de negócio para controle de acesso
A9.1.1	política de controle e de acesso
A9.1.2	Acesso às redes e aos serviços de redes
A9.2	Gerenciamento de acesso do usuário
A9.2.1	Registro e cancelamento de usuário
A9.2.2	Provisionamento para acesso de usuário
A9.2.3	Gerenciamento de direitos de acesso privilegiados
A9.2.4	Gerenciamento de informações de autenticação secreta dos usuários
A9.2.5	Análise crítica dos direitos de acesso de usuário
A9.2.6	Retirada do ajuste de direitos de acesso
A9.3	Responsabilidades dos usuários
A9.3.1	Uso de informações de autenticação secreta
A9.4	Controle de acesso a sistemas e aplicativos
A9.4.1	Restrição de acesso à informação
A9.4.2	Procedimentos de logon seguro
A9.4.3	Sistema de gerenciamento de senhas
A9.4.4	Uso de programas utilitários privilegiados
A9.4.5	Controle de acesso ao código fonte do programa
A10	Criptografia
A10.1	Controles criptográficos
A10.1.1	Política de uso de controles criptográficos
A10.1.2	Gerenciamento de chaves
A11	Segurança física e do ambiente
A11.1	Áreas Seguras
A11.1.1	Perímetro de segurança física

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 14/30

A11.1.2	Controles de entrada física
A11.1.3	Segurança em escritórios, salas e instalações
A11.1.4	Proteção contra ameaças externas e ambientais
A11.1.5	Trabalhando em áreas seguras
A11.1.6	Áreas de entrega e carregamento
A11.2	Equipamentos
A11.2.1	Escolha de local e proteção do equipamento
A11.2.2	Utilitários de suporte
A11.2.3	Segurança do cabeamento
A11.2.4	Manutenção dos equipamentos
A11.2.5	Remoção de ativos
A11.2.6	Segurança de equipamentos e ativos fora das dependências da organização
A11.2.7	Reutilização e alienação seguras de equipamentos
A11.2.8	Equipamento de usuário sem monitoração
A11.2.9	Política de mesa limpa e tela limpa
A12	Segurança nas operações
A12.1	Procedimentos e responsabilidades operacionais
A12.1.1	Documentação dos procedimentos de operação
A12.1.2	Gestão de mudanças
A12.1.3	Gestão de capacidade
A12.1.4	Separação dos ambientes de desenvolvimento, teste e de produção
A12.2	Proteção contra malware
A12.2.1	Controles contra malware
A12.3	Backup
A12.3.1	Cópia de segurança das informações
A12.4	Registros e monitoramento
A12.4.1	Registros de eventos
A12.4.2	Proteção das informações dos registros de eventos (log)
A12.4.3	Registros de eventos (log) de Administrador e Operador
A12.4.4	Sincronização dos relógios
A12.5	Controle de software operacional
A12.5.1	Instalação de software em sistemas operacionais
A12.6	Gerenciamento técnico de vulnerabilidades
A12.6.1	Gerenciamento de vulnerabilidades técnicas
A12.6.2	Restrições quanto a instalação de software
A12.7	Considerações sobre auditoria de sistemas de informação

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 15/30

A12.7.1	Controles de auditoria de sistemas de informação
A13	Segurança nas comunicações
A13.1	Gerenciamento da segurança em redes
A13.1.1	Controle de redes
A13.1.2	Segurança dos serviços de rede
A13.1.3	Segregação de rdes
A13.2	Transferencia de informação
A13.2.1	Políticas e procedimentos para transfêrencia de informações
A13.2.2	Acordos para transfêrencia de informações
A13.2.3	Mensagens eletrônicas
A13.2.4	Acordos de confidencialidade e não divulgação
A14	Aquisição, desenvolvimento e manutenção de sistemas
A14.1	Requisitos de segurança dos sistemas de informação
A14.1.1	Análise e especificação de requisitos de segurança da informação
A14.1.2	Serviços de aplicação seguros sobre redes publicas
A14.1.3	protegendo as transações nos aplicativos de serviços
A14.2	Segurança em processos de desenvolvimento e de suporte
A14.2.1	Política de desenvolvimento seguro
A14.2.2	Procedimentos para controle de mudanças de sistemas
A14.2.3	Revisão técnica de aplicativos após alterações na plataforma operacional
A14.2.4	Restrições sobre mudanças nos pacotes de software
A14.2.5	Princípios para projetar sistemas seguros
A14.2.6	Ambiente seguro para desenvolvimento
A14.2.7	Desenvolvimento terceirizado
A14.2.8	Teste de segurança de sistemas
A14.2.9	Teste de aceitação de sistemas
A14.3	Dados para teste
A14.3.1	Proteção dos dados para teste
A15	Relacionamento na cadeia de suprimento
A15.1	Segurança da informação na cadeia de suprimento
A15.1.1	Política de segurança da informação no relagionamento com os fornecedores
A15.1.2	Identificando segurança da informação nos acordos com fornecedores
A15.1.3	Cadeia de suprimento na tecnologia da comunicação e informação
A15.2	Gerenciamento da entrega do serviço do fornecedor
A15.2.1	Monitoramento e análise crítica de serviços com fornecedores

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



**PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
SISTEMA DE GESTÃO DE SEGURANÇA E
PRIVACIDADE DAS INFORMAÇÕES.**

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 16/30

A15.2.2	Gerenciamento de mudanças para serviços com fornecedores
A16	Gestão de incidentes de segurança da informação
A16.1	Gestão de incidências de segurança da informação e melhorias
A16.1.1	Responsabilidades e procedimentos
A16.1.2	Notificação de eventos de segurança da informação
A16.1.3	Notificando fragilidades de segurança da informação
A16.1.4	Avaliação e decisão dos eventos de segurança da informação
A16.1.5	resposta aos incidentes de segurança da informação
A16.1.6	Aprendendo com os incidentes de segurança da informação
A16.1.7	Coleta de evidências
A17	Aspectos de segurança da informação na gestão da continuidade do negócio
A17.1	Continuidade da segurança da informação
A17.1.1	Planejando a continuidade da segurança da informação
A17.1.2	Implementando a continuidade da segurança da informação
A17.1.3	Verificação, análise crítica e avaliação da continuidade da segurança da informação
A17.2	Redundâncias
A17.2.1	Disponibilidade dos recursos de processamento da informação
A18	Conformidade
A18.1	Conformidade com requisitos legais e contratuais
A18.1.1	Identificação da legislação aplicável e de requisitos contratuais
A18.1.2	Direitos de propriedade
A18.1.3	Proteção de registros
A18.1.4	Proteção e privacidade de informações de identificação de pessoal
A18.1.5	Regulamentação de controles de criptografia
A18.2	Análise crítica da segurança da informação
A18.2.1	Análise crítica independente da segurança da informação
A18.2.2	Conformidade com as políticas e normas de segurança da informação
A18.2.3	Análise crítica da conformidade técnica

8.0 O COMITÊ DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 17/30

- I. Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano;
- II. A composição mínima deve incluir um colaborador de cada uma das áreas: TI, Operacional, DP, DH, Financeiro, Fiscal, Marketing, Comercial, Jurídico, e diretoria Executiva;
- III. Exigir do Gerente de Tecnologia reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a **NOSSA ORGANIZAÇÃO**;
- IV. O Comitê de Privacidade e Segurança da Informação ou sob a orientação do DPO, poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico;
- V. Cabe ao Comitê de Privacidade e Segurança da Informação e/ou ao Gerente Tecnologia:
 - (a) Propor investimentos relacionados à privacidade e segurança da informação com o objetivo de reduzir mais os riscos;
 - (b) Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
 - (c) Avaliar os incidentes de segurança e propor ações corretivas;
 - (d) Definir as medidas cabíveis nos casos de descumprimento da PSI e (ou) das Normas de Segurança da Informação complementares.

9.0 CORREIO ELETRÔNICO.

- I. O uso do correio eletrônico da **NOSSA ORGANIZAÇÃO** é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a **NOSSA ORGANIZAÇÃO**.
- II. É proibido aos colaboradores o uso do correio eletrônico da **NOSSA ORGANIZAÇÃO** para:
 - a) Cadastrar o endereço corporativo em site de notícias e (ou) e-commerce;
 - b) Enviar mensagens contendo conteúdo impróprio como imagens pornográficas, links suspeitos, correntes do tipo Spam, Fake News, injúrias ou difamações, e qualquer outra ação que venha a comprometer a imagem da instituição;

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 18/30

- c) Utilizar o endereço de E-mail de outro colaborador ou solicitar o mesmo para sua conta pessoal;
 - d) Enviar material de qualquer tipo gerado pela NOSSA ORGANIZAÇÃO que não esteja no escopo das atividades do colaborador;
 - e) Associar o E-mail corporativo às redes sociais como Facebook, Instagram, etc sem autorização da diretoria executiva.
 - f) Utilizar a conta de e-mail para encaminhar mensagens em massa caracterizadas como SPAM, e (ou) conteúdo fora do escopo das atividades de trabalho sem a autorização da equipe de Tecnologia;
- III. As mensagens de correio eletrônico sempre deverão incluir assinatura padrão disponibilizada pelo gestor da célula.

10. INTERNET.

- I. A NOSSA ORGANIZAÇÃO, disponibiliza interfaces de comunicação digital e acesso à internet, estes meios de comunicação, estão sob camadas de proteção que permitem o completo gerenciamento das informações trafegadas por estes canais; esta conduta, faz parte do modelo de avaliação de vulnerabilidades e ameaças à nossa organização.
- II. São permitidos aos usuários, a execução de procedimentos que viabilizem acesso a informações particulares, tendo como objetivo, realizar a interação com suas atividades pessoais, e manter uma comunicação segura com o meio externo fora da nossa organização. Para que o controle do tráfego de rede não seja afetado com a utilização e acesso à conteúdos que possam impactar na performance das nossas infraestruturas, ficam estabelecidos os seguintes limites aos usuários a partir da integração às dependências da NOSSA ORGANIZAÇÃO.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.

PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 19/30

- g) Os equipamentos fornecidos pela NOSSA ORGANIZAÇÃO, são identificados e permanecem sob sistemas de auditoria ininterruptas;
- h) Todos os softwares fornecidos pela NOSSA ORGANIZAÇÃO possuem licenciamento.
- i) É proibida a utilização dos equipamentos da corporação para efetuar práticas de envio de mensagens a partir de qualquer conta de comunicação que contenham material com conotação ofensiva, difamatória, política, ou que possam associar atividades ilícitas por parte do colaborador da NOSSA ORGANIZAÇÃO; Estando estas ações sujeitas a investigação nas esferas Cíveis e (ou) criminais.
- j) O envio de mensagens com documentos internos produzidos na NOSSA ORGANIZAÇÃO, tornam-se passíveis de monitoramento e auditoria a qualquer tempo, sendo expressamente proibido o envio de material eletrônico a partir do ambiente da NOSSA ORGANIZAÇÃO para Drives virtuais e (ou) contas de outros domínios senão aqueles associados e aprovados pela NOSSA ORGANIZAÇÃO ou que não façam parte da relação de trabalho do colaborador validadas como legítimas pela NOSSA ORGANIZAÇÃO.
- k) Fica expressamente proibido a utilização de qualquer mídia que associe a imagem da NOSSA ORGANIZAÇÃO em redes sociais, ou grupos de mensagens sem autorização formal expressa pelo setor jurídico da NOSSA ORGANIZAÇÃO, e da mesma forma atribuir mensagens com cunho e opinião pessoal associadas à NOSSA ORGANIZAÇÃO sem prévia autorização do setor jurídico.
- l) Toda e qualquer imagem associada a colaboradores, documentos, e dependências da NOSSA ORGANIZAÇÃO, só poderão ser divulgadas pelos setores autorizados da Organização, e qualquer intensão fora deste escopo, deverá ser autorizada expressamente pelos setores jurídicos e de comunicação da instituição.

10. IDENTIFICAÇÃO.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.

PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 20/30

- I. Os controles de identificação dentro de um organização devem garantir acessibilidade/disponibilidade apenas aos usuários credenciados e autorizados para tal.
- II. O uso de credenciais de outro usuário pode ser caracterizado como falta grave e passível de punição nas esferas cíveis e (ou) criminais;
- III. Cada usuário é responsável pela salvaguarda de suas credenciais tornando-as intransferíveis.
- IV. Em caso da existência de login compartilhado, devera ser informada a situação aos setores de Segurança da Informação imediatamente.
- V. A área de Gente e Desenvolvimento da **NOSSA ORGANIZAÇÃO** é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.
- VI. Os setores de Tecnologia respondem pela criação da identidade lógica dos colaboradores na instituição, para a realização dos controles de gerenciamento de Contas de Grupos e Usuários.
- VII. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e (ou) jurídicas.
- VIII. Os usuários que não possuam perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # \$ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.
- IX. Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # \$ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 21/30

- X. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos ou documentos a vista de outros colaboradores e não é recomendável a associação a informações pessoais, como o próprio nome, Nome de Familiares, data de nascimento, etc, e não devem ser constituídas por combinações simples, como “MeuNome2022”, “87654321”, entre outras. Indica-se a combinação alternada de letras e números, maiúsculas e minúsculas e a utilização de caracteres especiais (!@#\$\$%).
- XI. Após 3 (três) tentativas equivocadas, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o setor de Tecnologia da **NOSSA ORGANIZAÇÃO**.
- XII. A periodicidade máxima para troca das senhas é 90 dias (três meses), não podendo ser repetidas as 3 (três) últimas senhas.
- XIII. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários ou por interesse da **NOSSA ORGANIZAÇÃO**. No caso de desligamento do colaborador, o setor de Recursos Humanos deverá imediatamente comunicar as áreas de Tecnologia e Segurança da Informação para que os controles já automatizados ou não sejam aferidos para destacar a credencial de acesso aos sistemas da **NOSSA ORGANIZAÇÃO**.

11. DISPOSITIVOS TECNOLÓGICOS

- 1) Os recursos Tecnológicos disponibilizados pela NOSSA ORGANIZAÇÃO, deverão ser utilizados de forma cuidadosa para garantir a vida útil dos dispositivos,
- 2) É vedado ao utilizador efetuar qualquer manutenção sem a autorização da área de Tecnologia da NOSSA ORGANIZAÇÃO.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 22/30

- 3) As atualizações de patches de segurança dos sistemas são desenhadas para que sejam efetuadas de forma automatizada, sem a necessidade da interação do usuário.
- 4) Todos os dispositivos informáticos fornecidos pela NOSSA ORGANIZAÇÃO. Possuem soluções de antivírus e proteção de mensagens eletrônicas.
- 5) Arquivos particulares e não vitais para a atividade do colaborador, como vídeos, músicas e fotos, não deverão ser armazenadas na rede local; este tipo de conteúdo torna-se passível de auditoria e não possui garantia de restauração em caso de decisão pela eliminação do material por parte da Gerência dos Sistemas NOSSA ORGANIZAÇÃO.
- 6) É recomendável que durante a utilização de dispositivos informáticos, mantenha-se afastado dos aparelhos, líquidos ou alimentos que possam ser derramados no corpo do dispositivo.

12. DISPOSITIVOS MÓVEIS.

- I. A NOSSA ORGANIZAÇÃO, disponibiliza a alguns gestores dispositivos móveis corporativos, estes deverão seguir as seguintes indicações:
 1. Manter o dispositivo atualizado com no mínimo uma ferramenta antivírus corporativa;
 2. Manter duplo fator de autenticação para recuperação de senhas com a segunda opção de recuperação destacada do telefone principal;
 3. Manter a tela bloqueada quando o equipamento não estiver em uso;
 4. Disponibilizar os equipamentos às equipes de tecnologia quando requeridos para fins de auditoria.
 5. Manter os logs de operação sem alterações;

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 23/30

6. Não utilizar os números e contas corporativas para cadastrar em sites de vendas do tipo E-commerce sem autorização da diretoria executiva;
7. Em caso de dano ou furto, comunicar imediatamente as autoridades, realizar um BO – Boletim de ocorrência, e avisar as áreas de Tecnologia e Segurança da Informação;
8. Manter informações confidenciais com proteção biométrica ou fora do aparelho telefônico se possível;
9. Armazenar o número IMEI do aparelho em ambiente protegido;
10. Não utilizar o dispositivo corporativo em redes sociais e afins, senão aqueles canais permitidos pela instituição.

PARA OS COLABORADORES QUE NÃO UTILIZAM DISPOSITIVOS CORPORATIVOS **RECONHECIDOS PELA ORGANIZAÇÃO**

11. É expressamente proibido utilizar endereço eletrônico da instituição no aparelho pessoal eu não for reconhecido como autorizado pela organização;
12. É altamente recomendável aderir à uma ferramenta antivírus para o celular particular;
13. Defina duplo fator de autenticação para contas de E-mail e Whats App;
14. Não receba conteúdo de trabalho no celular particular que não tenha sido classificado como seguro pela organização, caso isto ocorra, acione imediatamente a gerência imediata e comunique a área de Segurança da informação.
15. Os utilizadores que trabalham em Home Office e utilizam seus equipamentos particulares para o trabalho, deverão seguir as mesmas orientações acerca da utilização de ferramentas antivírus, e boas práticas de navegação.

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.		
TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 24/30

16. É altamente recomendável que os setores de tecnologia avaliem o equipamento antes da liberação do ambiente corporativo da NOSSA ORGANIZAÇÃO, sendo altamente recomendável que estes aparelhos estejam aptos acerca dos quesitos SUFICIENTES/MÍNIMOS de segurança para utilização dos ambientes Digitais da NOSSA ORGANIZAÇÃO.

13. DATACENTER.

- I.O Acesso as dependências do Data Center, reclamam a identificação por credenciais do tipo Crachá, senha ou biometria.;
- II.Os direitos de acesso deverão ser apontados pelos gestores responsáveis pela salvaguarda do ambiente;
- III.Relatórios de permissão de acesso deverão ser providenciados a qualquer tempo mediante requisição da alta gestão;
- IV.Chaves e credenciais de acesso ao ambiente devem ser concedidas aos brigadistas e equipes de combate a incêndios e (ou) incidentes físicos no local;
- V.O ambiente do Data Center deverá ser mantido organizado, limpo, e constantemente resfriado, livre de possíveis vazamentos de água ou incidentes elétricos;
- VI.É vedada a entrada de pessoas não autorizadas, bebidas ou alimentos no ambiente do Data Center;

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 25/30

14. BACKUP.

- I. As cópias de Segurança, deverão ser monitoradas e realizadas sob a supervisão do Gestor responsável.
- II. Toma-se como premissa básica e conceitual a definição de cópias de backup sadias através das seguintes premissas: a) Deve-se manter não apenas cópias das VMS no cluster secundário, mas também se possível em STORAGE destacado da rede principal; b) Deve-se manter uma cópia criptografada em ambiente local de todas as bases de dados dos bancos principais da organização, efetuadas por export de cada base, sendo todos os arquivos criptografados e armazenados em NAS ou STORAGE offline, ou em nuvem destacada da rede principal seguindo o padrão (3,2,1) – Três cópias locais (Node secundário, Storage Local, e disco local), - (2) Duas cópias offline que intercalarão a cada cópia full das vms e bases de dados, (1) Uma cópia em cofre em disco ou fita destacado do ambiente computacional, se possível fora da organização, com atraso de no máximo 30 dias.
- III. Testes de recuperação devem ser programados dentro do período de 3 em 3 meses.
- IV. Mídias de armazenamento devem ser controladas para observância da validade;
- V. O descarte de mídias deve ser feito com WIPE nível 7 e endereçadas as empresas credenciadas para descarte e material eletrônico.

15. MONITORAMENTO E IMAGENS DE SEGURANÇA.

- I. A **NOSSA ORGANIZAÇÃO** possui a prerrogativa de monitorar as dependências que compõem a organização, exceto aquelas cujo monitoramento possa violar privacidade e intimidade de colaboradores e (ou) outros interessados, através de câmeras de monitoramento que armazenam imagens pelo período de 30 dias com o intuito de atender à



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 26/30

legislação vigente. O armazenamento periódico deve ser referenciado (tempo de armazenamento x substituição de novos registros x cópias de segurança x mecanismos físicos e lógicos de proteção), e para cumprir com as premissas de segurança patrimonial e pessoal de todos os colaboradores.

- II. O acesso às imagens só poderá ser realizado pelos seguintes agentes desde que em legítimo interesse da organização:
 - a) Pela área de Tecnologia e Informação;
 - b) Pela equipe de Segurança;
 - c) Pela diretoria ou setor jurídico da organização;
 - d) Pelos gestores das demais áreas desde que acompanhados pelo jurídico ou diretoria da instituição.
- III. Toda e qualquer imagem resgatada do sistema de vigilância só poderá ser disponibilizada à terceiros desde que sob medida de segurança ou autorização judicial devidamente expedida pelas autoridades competentes e atreladas à legislação do estado/município local.

16. CONTROLE DE ACESSO FÍSICO (PERÍMETRO).

- I. O acesso sem permissão a áreas que contenham informações sensíveis de colaboradores ou de classificação confidencial, restrita, ou privada, torna-se expressamente proibida sem a devida autorização do gestor responsável.
- II. Entre as áreas que necessitam de autorização de acesso enumeram-se:
 - a) Sala da diretoria;
 - b) Sala do departamento de tecnologia e informação (TI/SI);
 - c) Sala do departamento Fiscal;
 - d) Sala do departamento jurídico;

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 27/30

- e) Sala do departamento de recursos e (ou) desenvolvimento humano;
- f) Sala de segurança/monitoramento;

III. O acesso sem autorização a qualquer departamento sem o devido consentimento do gestor responsável, torna-se passível de advertência grave.

17. LGPD – TRATAMENTO DE DADOS IDENTIFICÁVEIS E (OU) SENSÍVEIS DOS COLABORADORES:

- I. Trata-se da declaração de tratamento de informações (dados identificáveis e (ou) sensíveis) dos colaboradores internos e (ou) contratados por parte da **NOSSA ORGANIZAÇÃO**. A aceitação e ciência deste termo providenciada pelo colaborador mediante assinatura de próprio punho ou através de assinatura digital viabilizada por uma “ACT”, torna legítima a comunicação expressa providenciada pela **NOSSA ORGANIZAÇÃO** ao Colaborador no ato de sua contratação, referente ao modo de tratamento de informações identificáveis e (ou) sensíveis, e aplica-se, a base legal do tipo “Consentimento” por parte do colaborador, para o tratamento específico destas informações para a execução de políticas públicas e cumprimento das normativas e legislações vigentes no território Nacional (Brasil), conforme as determinações legais estabelecidas em cada Estado e município do nosso país, sendo considerada a (LGPD – Lei 13.709/2018) como a lei de tratamento de informações identificáveis e (ou) sensíveis de titulares.
- II. Fica estabelecido que as medidas necessárias para reduzir os riscos até os níveis aceitáveis de tratamento são promovidas em consonância com os requisitos da ISO/IEC 27001 e 27701, para promover o nível máximo de proteção conforme a capacidade da organização, o que não enfatiza a declaração de “total garantia de proteção de informações” por parte da **NOSSA ORGANIZAÇÃO**. Desde já, toma-se como norteamto, a última declaração de aplicabilidade assinada pela alta direção, para ratificar o compromisso de salvaguarda, proteção e controles aplicados para garantir a confidencialidade, a integridade e a disponibilidade das informações coletadas, processadas, e armazenadas pelo tempo

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.



PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 28/30

estabelecido pelas normativas e leis associadas ao ciclo de vida de informações dos setores de Recursos Humanos, Departamento Pessoal, e Desenvolvimento Humano.

III. Estão associadas a este modelo de tratamento, informações dos tipos:

- banco de currículos (Observar Processo específico indicando tempo de armazenamento e modo de descarte);
- dados fornecidos à seguradora do plano de saúde (Observar contrato e cláusulas de tratamento de informações pela Seguradora) – A **NOSSA ORGANIZAÇÃO** torna-se OPERADORA DE DADOS, e assume corresponsabilidade no modo de tratamento, fazendo-se necessário apontar precisamente qual é a empresa operadora parceira e disponibilizar sua política de privacidade e segurança;
- dados compartilhados com a empresa responsável por fechar a folha de pagamento (Observar responsabilidade solidária e mecanismos seguros de tratamento – faz-se necessário apontar precisamente quais são as empresas que operam dados em nome do controlador e para qual atividade específica). Da mesma forma, faz-se necessário disponibilizar sua política de privacidade e segurança;
- envio de dados para o sindicato, associações de classe e órgãos públicos. (Observar responsabilidade solidária e mecanismos seguros de tratamento - faz-se necessário apontar precisamente quais são as empresas que operam dados em nome do controlador e para qual atividade específica, incluindo o número para contato). Da mesma forma, faz-se necessário disponibilizar sua política de privacidade e segurança;
- exames admissionais - – faz-se necessário apontar precisamente quais são as empresas que operam dados em nome do controlador e para qual atividade específica, incluindo o número de contato). Da mesma forma, faz-se necessário disponibilizar sua política de privacidade e segurança;

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.

**PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
SISTEMA DE GESTÃO DE SEGURANÇA E
PRIVACIDADE DAS INFORMAÇÕES.**

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 29/30

18. POLÍTICA BYOD – BRING YOUR OWN DEVICE – PARA COLABORADORES INTERNOS/EXTERNOS:

- I. A **NOSSA ORGANIZAÇÃO**, estabelece as diretrizes a serem cumpridas mediante a utilização de dispositivos corporativos e (ou) particulares para a realização de tarefas subordinadas às funções que exijam comunicação e (ou) transferência de arquivos digitais através de Dispositivos Informáticos (Notebooks, Smartphones, Tables etc.).

- II. Fica estabelecido que é terminantemente proibida a veiculação de imagens e (ou) documentos que contenham dados identificáveis e (ou) sensíveis, através de grupos de comunicação interna/externa, que não tenham sido expressamente autorizados e (evidenciados) pelos titulares dos dados previamente. Fotos a partir de celulares ou outros dispositivos de captura de imagens, poderão ser promovidas apenas nos seguintes casos:
 - a) Tenham sido coletados os termos específicos de autorização para utilização e (ou) veiculação de dados (sensíveis) onde o titular dos dados, seja parte integrante da ação;
 - b) Os canais de utilização estejam expostos no documento de autorização de forma explícita ex: whatsApp, redes sociais etc.;
 - c) Não existam outras possibilidades de utilização e (ou) veiculação de conteúdo sensível, que não tenham sido previamente declaradas, autorizadas, e evidenciadas pelo agente coletor.

- III. Torna-se necessário que mediante a utilização de dispositivos de comunicação digital particulares pelos colaboradores internos, que estes sejam acordados e apontados no termo de contratação e estejam sob a gerência da área jurídica observando as questões trabalhistas relacionadas ao desempenho das funções e jornadas de trabalho. É altamente recomendável, que mediante a aceitação deste cenário, a organização providencie soluções

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.

PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO SISTEMA DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES.

TIPO DE DOCUMENTO: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI SGPI – SISTEMAS DE GESTÃO DE SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES PARA COLABORADORES INTERNOS E EXTERNOS.	CLASSIFICAÇÃO: RESTRITA	VERSÃO: 002
IDENTIFICADOR ÚNICO: PSI_NOVAXS_05_2023.	DATA: 12/06/2023	PÁGINA: 30/30

que garantam a privacidade e a segurança das informações tanto do colaborador quanto da organização, como por exemplo, soluções que providenciem containers gerenciados pela área de tecnologia, e da mesma forma, possam inibir a utilização de recursos associados á organização, fora do horário acordado entre a contratante e o contratado.

19. DISPOSIÇÕES FINAIS.

- I. Assim como a ética, a segurança da Informação deve ser entendida como parte fundamental da cultura interna da **NOSSA ORGANIZAÇÃO**. Ou seja, qualquer incidente de segurança subentende-se como algum agente que explora uma vulnerabilidade para agir contra a ética e os bons costumes regidos pela instituição.

Diretoria executiva

RESTRITO

As informações contidas neste documento são destinadas ao uso Restrito da nossa Organização.