POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

INORPEL
cybersecurity

INORPEL cybersecurity	**POLÍTICA INORPEL CYBERSECURITY**				**Data de Criação: 15/10/2024**
	Número: POL-SI-0001	**Localizador: POL-SI**	**Revisão:** 2.0	**Folhas: 10**	**Data para Revisão: 01/11/2024**
Título: Política de Segurança da Informação				**Área Emitente: White Team**	
Elaborador: João Pimentel			**Aprovadores: Rodrigo Brito**		
Data da Publicação: 01/11/2024			**Auditor: Auditoria**		
Classificação da Informação: PÚBLICA					

Sumário

1. LISTA DE SIGLAS E ABREVIATURAS

- ABNT – Associação Brasileira de Normas Técnicas;
- CLT – Consolidação das Leis do Trabalho
- ISO – *International Organization for Standardization*;
- NIST – *National Institute of Standards and Technology*
- PSI – Política de Segurança da Informação;
- SGSI – Sistema Gestor de Compliance, Privacidade e Segurança;
- RH – Recursos Humanos;
- TIC – Tecnologia da Informação e Comunicação
- LGPD – Lei Geral de Proteção de Dados Pessoais
- GDPR – *General Data Protection Regulation*
- CGCSP – Comitê de Gestor de Compliance, Segurança e Privacidade

2. OBJETIVOS E ABRANGÊNCIA

A presente Política de Segurança da Informação tem por objetivo estabelecer e difundir as diretrizes básicas de PSI no âmbito da INORPEL CYBERSECURITY, visando orientar à todos quanto ao uso adequado de informações e recursos de TIC, visando a preservação dos Pilares de Confidencialidade, Integridade e Disponibilidade da Segurança da Informação bem como a conformidade com as normas, atendendo às disposições legais, regulamentares e as melhores práticas previstas em Padrões Normativos tais como ISO/IEC e NIST.

A presente Política da Segurança da Informação tem aplica-se à todos os administradores, funcionários, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executado externamente ou por terceiros que utilizem os ambientes físicos ou virtuais da INORPEL CYBERSECURITY ou com acesso à informações e uso de sistemas que pertençam à INORPEL CYBERSECURITY ou seus clientes.

3. PRINCÍPIOS

São Princípios norteadores das ações de Segurança da Informação na INORPEL CYBERSECURITY:

Visão Abrangente e Sistêmica da Segurança da Informação: questões relacionadas à Segurança da Informação é de respeito obrigatório por todos que compõem a INORPEL CYBERSECURITY e devem ser sempre analisados de forma integrada com os objetivos do negócio.
Uso Responsável dos ativos e recursos de TIC: os ativos de TIC devem ser usados de forma responsável visando o melhor atendimento aos interesses do negócio e dos clientes da INORPEL CYBERSECURITY.
Garantia da Confidencialidade, Disponibilidade, Integridade e Autenticidade: a presente PSI busca dar suporte e orientação para ações que visem a garantia da Confidencialidade, Disponibilidade e Integridade de informações e ativos da INORPEL CYBERSECURITY e seus clientes.

4. REFERÊNCIAS NORMATIVAS E LEGISLATIVAS

A presente PSI possui referenciado em seu escopo o cumprimento ou seguimento das seguintes normas, leis e regulamentos:

a) Decreto-Lei 5452/1943 – Consolidação das Leis do Trabalho;
b) Decreto n° 9637/2018 – Política Nacional de Segurança da Informação
c) Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;
d) ABNT NBR ISSO/IEC 27001:2022
e) ABNT NBR ISO/IEC 27002:2022
f) ABNT NBR ISO/IEC 27701:2019
g) ABNT NBR ISO/IEC 29100:2020

5. RESPONSABILIDADES

Todos os usuários são responsáveis pelo cumprimento das disposições da presente PSI. Por usuários entende-se todos os administradores, diretores, supervisores, funcionários, estagiários, prestadores de serviço que usem, em ambientes físicos ou virtuais da INORPEL CYBERSECURITY ou seus clientes, bem como tenham acesso a informações da INORPEL e seus clientes, sob pena de responsabilização de seu mau uso.

Desta forma, cumpre à TODOS:

a) Cumprir fielmente a presente PSI;
b) Proteger as Informações contra acessos, modificações, destruição ou divulgação não autorizadas pela INORPEL CYBERSECURITY.
c) Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição seja utilizado apenas para as finalidades aprovadas pela INORPEL CYBERSECURITY
d) Cumprir as leis e normas que regem a propriedade intelectual, proibido assim o uso de softwares e equipamentos não licenciados e aprovados pela INORPEL CYBERSECURITY;
e) Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas, incluindo a emissão de comentários e opiniões em redes sociais, blogs, sites e correlatos, sob pena de responsabilização;
f) Não compartilhar informações confidenciais de qualquer tipo;
g) Comunicar imediatamente à equipe do SGSI qualquer descumprimento ou violação desta PSI e/ou de suas Normas e Procedimentos.

É um DEVER de todos que integram a INORPEL CYBERSECURITY, independentemente do vínculo, considerar a informação como sendo um ativo da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para organização deve ser sempre tratado de forma profissional.

É de responsabilidade do Gestor de cada setor, operacional ou de apoio, classificar a informação (relatórios, documentos, modelos, procedimentos, planilhas, e-mails, dentre outros) gerada por sua área, de acordo com o nível de confidencialidade estabelecido em Política de Classificação da Informação próprio.

A adoção de políticas de “mesa limpa” e “tela limpa” configuram boas práticas, devendo todos manter suas mesas organizadas com seus respectivos documentos que contenham informações confidenciais arquivados em locais trancados, quando não estiverem sendo utilizados, bem como bloquear o acesso ao computador sempre que sair da estação de trabalho, mesmo que momentaneamente.

Por fim, fica vedado o armazenamento de arquivos da INORPEL em dispositivos de *endpoint*, tais como computadores, celulares, tablets, ou outros dispositivos eletrônicos, mesmo que de propriedade da INORPEL, devendo os arquivos serem armazenados única e exclusivamente em pasta própria no File-Server da INORPEL, podendo os arquivos armazenados fora desse padrão, serem excluídos, sem prévia comunicação, pelo setor de suporte da empresa à qualquer momento.

6. DIRETRIZES GERAIS

6.1 Sistema Gestor de Compliance, Privacidade e Segurança

O SGCPS é um conjunto de políticas, processos e procedimentos que ajudam uma organização a proteger seus ativos de informação bem como garantir que ela esteja em conformidade com as normas e regulamentos. O objetivo principal é assegurar que os parâmetros legais e éticos, estejam em constante operação dentro da INORPEL, protegendo informações, garantido a privacidade, reforçando a conformidade e a segurança. Além das políticas, procedimentos e processos, será composto por um Comitê Gestor de Compliance, Segurança e Privacidade.

a) Composição do Comitê Gestor de Compliance, Segurança e Privacidade

-

O CGCSP deverá ser gerido pelos membros do Comitê Gestor de Compliance, Segurança e Privacidade, visando garantir que as práticas de segurança da informação, a proteção de dados pessoais e compliance sejam eficientes e estejam em conformidade com a legislação prevista, o grupo será formado por:

1. 01 (um) membro da diretoria;
2. 01 (um) membro do White Team;
3. 01 (um) membro do *Blue, Orange, Red ou Purple* Team;
4. 01 (um) membro do Comercial;
5. 01 (um) membro do Administrativo;

b) Mandato dos Membros e Nomeação

Os membros do CGCSP terão mandatos de 02 (dois) anos, podendo ser reconduzidos sempre que do interesse da organização. Serão nomeados pelo CSO/CTO da INORPEL CYBERSECURITY e serão escolhidos em respeito aos seguintes critérios:

a) Tempo de senioridade na INORPEL CYBERSECURITY;
b) Tempo de senioridade na função;
c) Nível na hierarquia da organização;

Em caso de saída de algum dos membros, será escolhido novo para completar o tempo de mandato restante, levando-se em conta os mesmos critérios.

A alteração da versão 1.0 para a presente versão da Política de Segurança da Informação com o aumento do escopo do antigo Sistema Gestor de Segurança da Informação e seu consequente Comitê Gestor de Segurança da Informação não alterará a composição atual do comitê, que consistirá apenas em mudança de nomenclatura e escopo.

c) Missão

O gestor do CGCSP tem como missão a proteção das informações da organização e manutenção dos processos de segurança estabelecidos, bem como, realizar a supervisão de compliance e analisar se a organização está operando em conformidade com as normas, catalisando, coordenando, desenvolvendo e/ou implementando ações para esse fim, além de atuar como um agente facilitador que promoverá um ambiente seguro dentro da organização.

d) Atribuições do Comitê Gestor de Compliance, Segurança e Privacidade

O CGCSP tem como atribuições principais, não excluindo outras porventura previstas em políticas temáticas complementares e outras normas internas da organização:

- Revisar e aprovar as Políticas, Processos e Procedimentos que impactem na Segurança de informações, Privacidade e no Compliance;

- Acompanhar e avaliar o desempenho do SGCPS;
- Garantir conformidade com leis e regulamentos relevantes;
- Aprovar metodologias para avaliações de riscos;
- Analisar e aprovar planos de tratamento de riscos;
- Monitorar e revisar *KPI's*;
- Promover a cultura da Segurança da informação, compliance e privacidade na organização;
- Aprovar o plano de treinamento em Segurança da informação, Compliance e Privacidade;
- Monitorar e avaliar a efetividade do treinamento;
- Aprovar planos de respostas à incidentes de segurança e privacidade;
- Ser notificado de incidentes de segurança e/ou privacidade;
- Avaliar a gravidade dos incidentes de segurança reportados;
- Acompanhar investigações sobre incidentes de segurança;
- Acompanhar a resolução de incidentes;
- Gerenciar o acesso às informações confidenciais;
- Julgar responsabilidades em questão de violações e incidentes de segurança, emitindo recomendações quanto aos casos analisados;
- Conduzir auditorias regulares e elaborar relatórios sobre a situação de compliance, segurança e privacidade para a Direção;
- Implementar melhorias contínuas a partir de feedbacks dos colaboradores e lições aprendidas com eventos/incidentes ocorridos;
- Acompanhar as mudanças em legislações, normas e regulamentos;
- Outras que porventura sejam estabelecidas em políticas temáticas próprias.

6.2 Classificação das Informações

As informações na INORPEL CYBERSECURITY são classificadas quanto ao seu nível de confidencialidade, nível de criticidade e nível de valor.

Quanto ao seu nível de confidencialidade ela pode ser:

- Público: Acessível a qualquer pessoa.
- Interno: Acessível apenas aos colaboradores da organização.
- Confidencial: Acessível apenas a colaboradores com autorização específica.
- Secreto: Acessível apenas a um grupo restrito de colaboradores com autorização específica.

Quanto ao seu nível de Criticidade ela pode ser:

- Alta: Informação crítica para o funcionamento da organização.
- Média: Informação importante para a organização, mas não crítica.
- Baixa: Informação útil, mas não essencial para a organização.

Quanto ao seu nível de Valor, ela pode ser:

- Alto: Informação com alto valor legal, comercial ou estratégico.
- Médio: Informação com valor moderado legal, comercial ou estratégico.
- Baixo: Informação com baixo valor legal, comercial ou estratégico.

A classificação deverá ser feita com base em tais critérios pelos proprietários dos ativos e informações, podendo ser revisada pelo gestor direto do setor detentor da informação ou pelo CGCSP.

Quando da classificação como secreto, deverá o documento indicar as pessoas e/ou cargos que poderão ter acesso ao citado documento.

Será criada Política de Classificação de Informações e Ativos em documento próprio com normais mais específicas.

6.3 Tratamento de Incidentes

É dever de TODOS a comunicação de todo e qualquer evento, incidente, brecha ou violação deste código, não devendo o usuário realizar qualquer teste para checar possíveis falhas de Segurança.
Ao perceber qualquer brecha, incidente ou violação à presente PSI o usuário deverá comunicar de imediato ao seu superior imediato, que irá realizar as devidas comunicações aos setores competentes bem como ao CGCSP.

Os incidentes, brechas ou violações ao presente PSI deverão ser registrados e gerenciados, bem como deve ser definida equipe para tratamento e resposta para incidentes.

6.4 Gestão de Riscos e Continuidade de Negócios

Deverá ser realizada análise dos riscos que podem afetar a operação, para ciência das vulnerabilidades e identificação e implementação de medidas de proteção visando a mitigação ou eliminação dos riscos.

6.5 Compliance e Revisão Contínua

A INORPEL CYBERSECURITY preza pelo cumprimento das normas legais, regulamentares e padrões de melhores práticas existentes no mercado. É dever de TODOS a observância dessas normas, bem como das políticas, processos e procedimentos emitidos pela INORPEL CYBERSECURITY e diretrizes estabelecidas por sua direção.

6.6 Controle de Acesso

O controle de acesso compreende tanto o acesso físico quanto o acesso lógico às instalações, equipamentos e sistemas da INORPEL CYBERSECURITY. Todo o acesso à informação confidencial se dará através de mecanismos de identificação e controle de acesso e qualquer mudança funcional implicará em obrigatória revisão dos direitos de acesso à informação, sempre respeitando o princípio do menor privilégio, onde o usuário deve ter acesso apenas ao necessário para o cumprimento de suas atribuições.

Deverá o Gestor de Recursos Humanos criar processo para revisão periódica e/ou por mudança funcional nos direitos de acesso.

O controle de acesso será baseado no princípio do "menor acesso necessário", onde o colaborador apenas terá acesso, físico ou lógico, ao que necessita ao cumprimento de suas atribuições.

6.7 Comunicação

A comunicação interna, para transferências de informações e dados, deverá ser centralizada nos sistemas disponibilizados pela INORPEL para esse fim, mediante política e procedimento próprio, visando com isso a mitigação de riscos relacionados à confidencialidade e autenticidade das informações e dados, ficando vedado o envio de dados e informações para e-mails pessoais de TODOS.

A comunicação fora dos meios homologados pela organização implicará em responsabilização do colaborador, em caso de incidente decorrente desse uso fora dos padrões.

6.8 Recursos Humanos

Todos devem ter pleno conhecimento das diretrizes, responsabilidades, limitações e penalidades relacionadas à utilização dos recursos de TIC, inclusive por ocasião da mudança de atividades.

Cumpre ao Gestor de Recursos Humanos implementar processos que tenham como base o respeito a presente PSI, atentando para a preservação das informações em processos de contratação e desligamento de funcionários, estagiários e prestadores de serviço, atentando para criações e revogações de acesso à ambientes físicos e virtuais em prazos e momentos críticos que busquem evitar a má utilização desses acessos.

6.9 Gestão de Fornecedores

Aplicam-se à terceirizados, prestadores de serviço, fornecedores de serviços e/ou produtos, os
quais tenham acesso às informações da INORPEL CYBERSECURITY e/ou seus clientes, as disposições da presente PSI e demais normas de Segurança, Privacidade e Compliance, que porventura sejam editadas.

Caberá à INORPEL CYBERSECURITY realizar treinamento e divulgação da presente PSI, e outras normas temáticas que sejam editadas aos fornecedores, terceirizados e prestadores de serviço.

Poderá a INORPEL CYBERSECURITY requisitar adequação dos fornecedores, terceirizados e prestadores de serviço a disposições da presente PSI, políticas temáticas que porventura venha ser editada bem como Leis, Normativos e Regulamentos que afetem à relação contratual com a INORPEL CYBERSECURITY.

Novos fornecedores deverão responder à *checklist*, conforme Anexo, com declaração de conformidade dos mesmos, conforme Anexo, podendo, a INORPEL CYBERSECURITY requisitar prova dessa conformidade à qualquer tempo, sob pena de, não cumprindo, ser a relação contratual encerrada por culpa do fornecedor e sem qualquer aplicação de multa em desfavor da INORPEL CYBERSECURITY.
A INORPEL CYBERSECURITY realizará avaliação periódica de riscos decorrentes de relação contratual com fornecedores, prestadores de serviço e terceirizados que afetem à Segurança da Informação.

6.10 Segurança Física e do Ambiente

Deve ser garantida a segurança física dos locais onde estão armazenadas informações sensíveis, bem como a proteção contra ameaças ambientais.

6.11 Aquisição, Desenvolvimento e Manutenção de Sistemas

Quando da aquisição ou desenvolvimento de sistemas, a segurança da informação, a privacidade e compliance devem ser sempre observados, principalmente quanto aos princípios do "*Security By Design*" e "*Security By Default*", em todo o ciclo do Sistema, cabendo tal respeito também quando das manutenções e atualizações em tais sistemas.

6.12 Uso de Ativos, Equipamentos e Sistemas.

Os equipamentos, sistemas e demais ativos fornecidos pela INORPEL CYBERSECURTY devem ser protegidos contra acesso não autorizado e utilizados apenas para as atividades fins da INORPEL CYBERSECURITY.

O uso de equipamentos de informática pessoais, como tablets, notebooks, celulares, dentre outros ficam vedados dentro do perímetro da empresa, onde será permitido apenas com autorização expressa do diretor da área, ficando o uso da rede e sistemas restritos aos equipamentos fornecidos pela INORPEL CYBERSECURITY.

7. MEDIDAS DISCIPLINARES POR DESCUMPRIMENTOS DA PSI

A violação de um ou alguns dos preceitos da presente PSI, Políticas Temáticas, Procedimentos estabelecidos, ou processos indicados, ensejará a aplicação de medidas disciplinares, por meio de procedimento administrativo próprio, onde será apurada culpa ou dolo por parte de quem violou as normas, com as punições previstas na CLT como advertências, suspensões ou mesmo demissão.

Caberá ao Comitê Gestor apurar dolo ou culpa na conduta infratora realizando relatório demonstrando os elementos apurados encaminhado à diretoria de RH que tomará as medidas disciplinares que entender cabível de acordo com a situação em concreto.

9. DISPOSIÇÕES FINAIS

As previsões dispostas na presente PSI poderão ser alteradas a qualquer momento, devendo haver revisões anuais de tais disposições.
Em caso de conflito entre a presente PSI e uma política temática específica, tal como política de classificação de informações, ou políticas de uso de dispositivos móveis, prevalecerá o disposto na política temática.

Caberá à INORPEL CYBERSECURITY assegurar o conhecimento e divulgação da presente PSI, suas alterações, políticas temáticas, suas alterações, processos e procedimentos, por meio de treinamento e confirmação por escrito da ciência dos envolvidos das normas de SI previstas.

10. HISTORICO DE VERSÕES E APROVAÇÕES

Versão	Data	Assinatura	Responsável	Descrição
1.0	20/05/2024	Via D4Sign	Rodrigo Brito	Aprovação do documento
2.0	01/11/2024	Via D4Sign	Rodrigo Brito	Aprovação do documento com as alterações relacionadas ao Sistema e Comitê Gestor de Compliance, Privacidade e Segurança