




Política de Segurança da Informação



Política de Segurança da Informação
Versão Português


	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	1 / 29

HISTÓRICO DE REVISÕES/APROVAÇÕES

Versão	Revisado por	Data de Revisão	Aprovado por	Cargo do aprovador	Data aprovação
1.0	Rodrigo Periotto	07/08/2018	José Furtado	Gerente Geral de TI	08/08/2018
			Valdecir Botassini	Diretor de Desenvolvimento de Projetos & TI	08/08/2018

O documento é revisado minimamente uma vez ao ano ou sempre que ocorrerem mudanças significativas no ambiente.


Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	2 / 29

ÍNDICE


1. OBJETIVO	5
2. CONFORMIDADE COM A POLÍTICA	5
3. DEFINIÇÕES	6
3.1 Segurança da Informação.....	6
3.2 Ativo.....	6
3.3 Confidencialidade	6
3.4 Integridade.....	6
3.5 Disponibilidade.....	6
3.6 Incidente de Segurança.....	6
3.7 Empregado	6
3.8 Vulnerabilidade	7
3.9 Ameaça.....	7
3.10 Risco.....	7
3.11 Avaliação de Riscos.....	7
3.12 Terceiros e Contratados.....	7
4. PAPÉIS E RESPONSABILIDADES	7
5. DOCUMENTOS DE REFERÊNCIA	8
6. DIRETRIZES GERAIS	9
7. SEGURANÇA ORGANIZACIONAL	9
7.1 Sistema de Gestão de Segurança da Informação (SGSI)	9
7.2 Avaliação de Riscos	10
7.3 Segurança da Informação na Gestão De Projetos	10
7.4 Auditoria Interna	10
7.5 Contratação de Novos Empregados.....	10
7.6 Conscientização, Treinamento em Segurança da Informação.....	11

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	3 / 29


8. CONTROLE DE ACESSO	11
8.1 Controle de Acesso à Rede Corporativa	11
8.2 Controle de Acesso à Sistemas Aplicativos	12
8.3 Controle de Acesso em Sistema Operacional	12
8.4 Uso de Senhas	13
8.5 Reset de Senhas	14
8.6 Monitoramento de Acesso	14
8.7 Acesso Remoto	15
8.8 Desligamento ou Mudança de Função	15
9. RESPONSABILIDADES	15
9.1 Comitê de Segurança da Informação	15
9.2 Área de Tecnologia da Informação	16
9.3 Empregados	16
9.4 Demais Aspectos de Segurança da Informação	17
10. SEGURANÇA NO AMBIENTE DE TECNOLOGIA	17
10.1 Gerenciamento de Rede e Informações	17
10.2 Manipulação Segura de Mídias	18
10.3 Computadores e Dispositivos "Não Homologados"	18
10.4 Uso de Equipamentos Nexa	18
10.5 Manipulação e Reutilização de Equipamentos	19
10.8 Proteção Contra Vírus	20
10.9 Filtro de Conteúdo	20
10.10 Descarte e Transferência de Mídias	20
10.11 Proteção do Ambiente de Sistemas	21
10.12 Gestão de Ativos	21
10.14 Uso do Correio Eletrônico e Internet	21
11. SEGURANÇA FÍSICA	23

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	4 / 29

11.1	Segurança Física das Instalações	23
11.2	Segurança Física de Equipamentos	23
11.3	Segurança de Ambientes Críticos	24
11.4	Revisão e Revogação de Acesso.....	24
12.	MANUTENÇÃO E DESENVOLVIMENTO DE SISTEMAS	24
12.1	System Development Life Cycle – SDLC.....	25
12.2	Homologação de Sistemas e Aplicativos.....	27
13.	COMPLIANCE	27
13.1	Revisão e Aprovação do Documento.....	27
13.2	Exceções	27
13.3	Penalidades	28
14.	INFORMAÇÕES COMPLEMENTARES.....	28
15.	ANEXOS.....	28

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA		Código	PC-CTI-GTI-001-PT
	Política Corporativa		Revisão	1.0
	Título: Política de Segurança da Informação		Área	TI
			Páginas	5 / 29

1. OBJETIVO

Esse documento descreve as diretrizes necessárias à aplicação de práticas de Segurança da Informação, considerando pessoas, processos, tecnologia, requisitos do negócio, leis e regulamentações pertinentes da Nexa Resources S.A.

A companhia pretende proteger seus negócios, sua reputação e salvaguardar seus empregados e contratados, evitando interrupções no negócio da empresa e minimizando o impacto de qualquer incidente de segurança da informação, estabelecendo diretrizes para utilização de recursos de tecnologia e apoiando a implantação das iniciativas e controles relativos à segurança da informação.

Este objetivo pode ser alcançado através de garantia da confidencialidade, integridade e disponibilidade dos Ativos e informações da empresa, juntamente com a segurança dos empregados e contratados dentro dos escritórios. Este documento estabelece o quadro de gerenciamento de segurança da informação necessário para alcançar esse objetivo.

2. CONFORMIDADE COM A POLÍTICA


A adesão a esta política é obrigatória para todos os conselheiros, diretores, executivos, empregados, terceiros, contratados e usuários de informações da Nexa Resources S.A., doravante denominada Nexa, assim como de suas subsidiárias servindo de base para a definição de normas específicas, procedimentos, responsabilidades e conceitos.

Todos têm a responsabilidade individual de garantir sua conformidade pessoal com esta política e devem procurar orientação da área de Segurança da Informação para esclarecimentos, caso necessário.

A violação desta política estará sujeita a ações disciplinares de acordo com as condições de trabalho, conforme aplicável. Podendo incluir o término do vínculo empregatício.

A área de Segurança da Informação é responsável por estabelecer mecanismos apropriados para alcançar o cumprimento desta política. O cumprimento desta política pode ser monitorado através de inspeções, análise de dados, e uso de outros registros, bem como auditorias e/ou pedidos de acompanhamento de conformidade por escrito.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	6 / 29

3. DEFINIÇÕES

Para os efeitos desta Política de Segurança da Informação, aplicam-se as seguintes definições.

3.1 Segurança da Informação

Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas.

3.2 Ativo

Qualquer coisa que tenha valor para a organização, incluindo, mas não limitando a informações, softwares, pessoas, instalações e equipamentos.

3.3 Confidencialidade

Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

3.4 Integridade

Propriedade de salvaguarda da exatidão e completeza de Ativos.

3.5 Disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.


3.6 Incidente de Segurança

Um único ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

3.7 Empregado

Pessoas contratadas no regime empregatício da legislação local vigente.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	7 / 29

3.8 Vulnerabilidade

Fraqueza de um Ativo ou grupo de Ativos que pode ser explorada por uma ou mais ameaças. (Ex: Antivírus Desatualizado, porta aberta no firewall, etc.).

3.9 Ameaça

Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

3.10 Risco

Combinação da probabilidade de um evento e de suas consequências.

3.11 Avaliação de Riscos

Uso sistemático de informações para identificar fontes de riscos e estima-las qualitativamente ou quantitativamente.

3.12 Terceiros e Contratados

Prestadores de serviços contratados diretamente ou através de outras empresas que realizam atividades para execução das rotinas de operacionais e de negócio da Nexa.


4. PAPÉIS E RESPONSABILIDADES

Para ser efetiva, a segurança da informação deve ser orientada para envolver a participação de cada usuário que lida com informações e/ou sistemas de informação. Como reconhecimento da necessidade do trabalho em equipe, esta política esclarece as responsabilidades dos usuários assim como os passos que eles devem seguir para auxiliar na proteção dos Ativos de informação e também os sistemas de informação.

Este documento descreve maneiras de prevenir e responder a uma variedade de ameaças às informações e sistemas, incluindo acesso não autorizado, divulgação, duplicação, modificação, apropriação, destruição, perda, mau uso e negação de uso.

O escopo de atuação da área de Segurança da Informação da Nexa está estabelecido em conjunto com a equipe CCTI da VSA (Votorantim S.A.), para a

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	8 / 29

manutenção do SGSI - Sistema de Gestão de Segurança da Informação compartilhados entre empresas. As atividades e objetivos gerais, em sua maioria, são semelhantes diferenciando-se acerca do escopo, definido pelas seguintes características:


- Ambiente físico das instalações da Nexa;
- Controles, normas e políticas de segurança específicas de sistemas ou ambientes não administrados ou abrangidos pela Votorantim (VSA);
- Iniciativas, treinamentos e programas de conscientização voltados ao público alvo da Nexa;
- Avaliação de fornecedores e contratações relevantes a segurança da informação realizadas através da Nexa;

As funções e responsabilidades incompatíveis devem ser identificadas e separadas dos respectivos papéis que tenham funções conflitantes, que poderiam resultar em comprometimento acidental ou deliberado de informações, sistemas ou processos, de forma a minimizar a possibilidade de acesso ou uso indevido e não autorizado de informação ou Ativos relacionados à informação da Nexa. Os papéis e responsabilidades estão definidos na Matriz RACI de Segurança da Informação disponível na Intranet.

5. DOCUMENTOS DE REFERÊNCIA

- PG-CTI-GTI-001-PT – Controle de Acesso Lógico
- PG-CTI-GTI-002-PT – Processo de Classificação da Informação
- PG-CTI-GTI-003-PT – Processo de Backup
- PG-CTI-GTI-004-PT – Processo de Gestão de Mudanças
- PG-CTI-GTI-005-PT – Processo de Gestão de Incidentes
- PG-CTI-GTI-006-PT – Controle de Segurança Física do Ambiente
- PG-CTI-GTI-007-PT – Controle de Acesso de Terceiros
- VIDE DOL – Política de Segurança da Informação VSA
- Norma ABNT NBR ISO/IEC 27001:2013 e ISO/IEC 27002:2013
- Lei Sarbanes-Oxley (SOX)

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA		Código	PC-CTI-GTI-001-PT
	Política Corporativa		Revisão	1.0
	Título: Política de Segurança da Informação		Área	TI
			Páginas	9 / 29

6. DIRETRIZES GERAIS

Todas as informações criadas, adquiridas ou custodiadas pela Nexa são consideradas como patrimônio da Nexa e estão sujeitas as suas normas e definições.

As informações manipuladas por todas as áreas da Nexa devem ser catalogadas e classificadas de acordo com seu nível de confidencialidade.

A concessão de acesso à informação deve ser realizada de forma controlada e limitada ao mínimo necessário para o desempenho da atividade em questão do profissional.

O uso dos recursos computacionais e informações da Nexa pode ser monitorado para fins de auditoria.

A extração ou envio de informações de propriedade da Nexa de forma não autorizada é proibida.

7. SEGURANÇA ORGANIZACIONAL

As definições desta seção estabelecem controles para manutenção da Política da Segurança das Informações, a fim de garantir alinhamento com os requisitos de negócios e iniciativas da Nexa.

7.1 Sistema de Gestão de Segurança da Informação (SGSI)


A Nexa deve determinar todas as questões externas e internas ao SGSI, relevantes para a finalidade e que afetam a capacidade de alcançar os resultados pretendidos.

Um SGSI deve ser estabelecido, mantido e melhorado para apoiar a capacidade da Nexa em proteger informações confidenciais.

A companhia deve alocar orçamento e recursos para a implementação, manutenção e melhoria contínua do SGSI, levando em consideração a categorização dos serviços para alocar efetivamente os recursos, conforme detalhado no plano de tratamento de risco.

O SGSI deve ser gerenciado de acordo com as políticas e monitorado conforme o plano de tratamento de risco. Também deve ser revisado em intervalos planejados

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	10 / 29

pelo Comitê de Segurança da Informação, definido pela companhia para assegurar sua eficácia e melhoria contínua.

7.2 Avaliação de Riscos

Uma avaliação periódica de riscos de segurança da informação e revisão dos controles implementados deve ser realizada a fim de garantir a conformidade do ambiente com as Políticas de Segurança existentes.

Todo empregado deve informar a área de segurança da informação eventuais riscos de segurança identificados em processos, sistemas ou operações.

Os riscos identificados como significativos para o negócio e que afetem um dos pilares de segurança (Disponibilidade, integridade e confidencialidade) deverão ser documentados e revistos dentro do prazo de validade estipulado pela área de Gestão de Riscos.

7.3 Segurança da Informação na Gestão De Projetos

A Tecnologia da Informação deverá ser acionada em demandas de projetos de alta complexidade, onde, por meio de reuniões participam ativamente da definição de risco e impacto atrelados ao projeto com o foco em Segurança da Informação.

7.4 Auditoria Interna


A Nexa deverá utilizar sua estrutura de Auditoria Interna para avaliar periodicamente a conformidade com as Políticas de Segurança da Informação vigentes.

Os sistemas de informação devem ser periodicamente revisados contra os requerimentos de segurança da informação identificados.

7.5 Contratação de Novos Empregados

Será solicitado ao empregado que assine termos relacionados à segurança, confidencialidade e proteção das informações, os quais devem ser fornecidos e retidos pela área do DHO assim que o candidato for contratado.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA		Código	PC-CTI-GTI-001-PT
	Política Corporativa		Revisão	1.0
	Título:		Área	TI
	Política de Segurança da Informação		Páginas	11 / 29

O empregado deverá ler, entender e atuar de acordo com os termos descritos, além de participar de treinamentos de segurança da informação quando for indicado pela área do DHO e/ou de Tecnologia de Informação.

Para terceiros devem ser observadas as diretrizes do Controle de Acesso de Terceiros - PG-CTI-GTI-007-PT.

7.6 Conscientização, Treinamento em Segurança da Informação

Todos os empregados e terceiros devem receber treinamento e conscientização apropriados com atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

O programa de conscientização é obrigatório para novos empregados, terceiros, transferidos que ocupam novas posições ou atribuições com requisitos de segurança da informação. Este treinamento deve contemplar os seguintes aspectos:


- Declaração do comprometimento da direção com a segurança da informação em toda a companhia;
- Estar em conformidade com as regras de segurança da informação, conforme definido nas políticas e contratos;
- Procedimentos e controles básicos de segurança da informação;
- Pontos de contato e recursos para informações adicionais e orientações sobre questões de segurança da informação, incluindo materiais de treinamento e educação em segurança da informação.

8. CONTROLE DE ACESSO

8.1 Controle de Acesso à Rede Corporativa

Acesso à serviços das redes internas e externas da Nexa são controlados por firewall e VLAN, segregando todos os seus ambientes (Desenvolvimento, teste e produção). Os acessos externos a Ativos de informação exigem mecanismos de autenticação que devem ser autorizados pelo área de Segurança da Informação,

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	12 / 29

incluindo o uso obrigatório de tecnologias de VPN (Virtual Private Network), a fim de proteger as informações trafegadas em meios externos.

Todas as conexões realizadas na rede corporativa (Incluindo via rede sem fio), devem ser realizadas por meio de identificação única de usuário, e passar obrigatoriamente pelas regras de firewall. Adicionalmente, tais conexões devem ser registradas, a fim de possibilitar análises e investigações posteriores, quando necessário.

Tecnologias do tipo SIEM (Security Incident and Event Monitoring) devem ser aplicadas na arquitetura de rede corporativa, a fim de permitir o monitoramento periódico de eventos de segurança e, desta forma, sua investigação e correção.

Avaliações de vulnerabilidades são realizadas mensalmente e os testes de invasão realizados anualmente na rede corporativa, incluindo rede sem fio por especialistas independentes, com o objetivo de identificar eventuais ameaças à segurança das informações do ambiente tecnológico da companhia.

8.2 Controle de Acesso à Sistemas Aplicativos

Mecanismos de segurança devem ser implementados na camada da aplicação, em um grau prático e viável, para proteger Ativos de informação contra danos decorrentes de mau uso. Os controles mínimos a serem considerados incluem mecanismos de autenticação, perfis de acesso e registro de trilhas de auditoria.


Todas as tecnologias em uso no ambiente devem atender as recomendações de seus fabricantes no que tange a atualizações e correções de falhas técnicas de segurança em seus códigos.

8.3 Controle de Acesso em Sistema Operacional

O acesso de usuários às configurações de sistema operacional e ferramentas administrativas deve ser restrito, de forma que somente usuários administradores da rede corporativa possam realizar essas alterações.

Somente usuários administradores da rede corporativa podem instalar, remover ou desativar softwares nas estações de trabalho ou notebooks.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---


	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	13 / 29

Configurações mínimas de segurança (baselines) devem ser definidas para os Ativos tecnológicos da rede corporativa, e um processo de *hardening* deve ser estabelecido para avaliar de forma periódica a conformidade dos Ativos com estes baselines.

8.4 Uso de Senhas

- Todas as contas de usuário devem possuir uma senha forte e secreta, conhecida apenas pelo proprietário da conta;
- Os usuários devem manter seguras suas senhas e não compartilha-las ou divulga-las;
- Os usuários não devem manter um registro em papel ou documento não criptografado (Documento do Microsoft Word, por exemplo) com lista de senhas;
- A companhia manterá os usuários cientes de suas responsabilidades em preservar a confidencialidade de suas senhas;
- Os sistemas devem ser definidos para exigir senhas para todas as contas;
- As senhas armazenadas em um sistema devem ser protegidas através de controles de criptografia e de acesso;
- As senhas devem ser alteradas sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
- A criação de senha deve observar as seguintes diretrizes:
 - a) Não serem baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações;
 - b) Não serem relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;
 - c) Não serem vulneráveis a ataques de dicionário (Por exemplo, não consistir em palavras inclusas no dicionário);
 - d) Serem isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;
 - e) Modificar senhas regularmente ou com base no número de acessos (Convém que senhas de acesso a contas privilegiadas

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	14 / 29

sejam modificadas mais frequentemente que senhas normais) e evitar a reutilização de senhas antigas;

f) Modificar senhas temporárias no primeiro acesso ao sistema.

- Não incluir senhas em nenhum processo automático de acesso ao sistema, por exemplo, armazenadas em uma macro ou funções-chave;
- Não utilizar a mesma senha para uso com finalidades profissionais e pessoais;
- Devem ser permitidas cinco tentativas de login antes do bloqueio do acesso e caso o bloqueio ocorra, a conta será desbloqueada automaticamente após 30 minutos;
- Os sistemas devem ser configurados para tomar ações corretivas quando os limites de tentativas inválidas consecutivas de login foram excedidos. As ações de correção devem incluir o registro do evento, o bloqueio da conta por um período mínimo de 30 minutos e envio de um alerta para um sistema de gerenciamento de sistemas disponíveis.
- A senha deve conter os seguintes requerimentos de complexidade:
 - a) Números (0, 1, 2, ...);
 - b) Caracteres especiais (#, %, !, %, @, ?, -, *);
 - c) Letras maiúsculas (A, B, C, ...); Letras minúsculas (a, b, c, ...).
 - d) Mínimo de 8 caracteres;
 - e) Não deve contar palavras do cotidiano como nome da empresa, nome de clubes de futebol, data de aniversário, nome ou sobrenome do usuário.


8.5 Reset de Senhas

A redefinição de senhas é restrita apenas a pessoas autorizadas e/ou ferramenta automatizada para tal fim.

8.6 Monitoramento de Acesso

O acesso aos Ativos de informação deve ser monitorado para detectar desvios e para registrar eventos ou incidentes relacionados à segurança, bem como registro de

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	15 / 29

trilhas de auditoria e relatórios. Os resultados do monitoramento destas atividades devem ser mantidos por tempo suficiente para permitir e apoiar qualquer análise de segurança da informação, incluindo o gerenciamento de capacidade para garantir que os serviços de infraestrutura de TI atendam aos requisitos relacionados ao desempenho.

8.7 Acesso Remoto

O acesso remoto a Ativos de informação deve possuir controles de autenticação e criptografia (Ex. Acesso através de VPN *client-to-site*)

8.8 Desligamento ou Mudança de Função

A área do DHO realiza a revogação dos acessos às informações no sistema de RH após a notificação de desligamento. A área do DHO deve notificar a área de TI, Facilities, Jurídico e GRC sobre mudanças de função ou desligamentos.

Deve ser realizado um checklist de ações que devem ser tomadas durante o desligamento, tais como: coleta dos Ativos, revogação dos acessos (Rede e sistemas), para depois seguir o fluxo padrão do DHO.

Os empregados devem assinar o Termo de Devolução (Retido pela área de Tecnologia da Informação) para comprovar a entrega dos Ativos sob sua responsabilidade (Ex.: notebook e celular), no momento do desligamento.


9. RESPONSABILIDADES

A área de Risco possui responsabilidade geral sobre a definição e manutenção das diretrizes para gestão dos riscos corporativos na companhia, incluindo aquelas específicas para segurança da informação.

9.1 Comitê de Segurança da Informação

É de responsabilidade de todos os integrantes do Comitê de Segurança da Informação o apoio e aplicação integral da Política de Segurança da Informação, bem como a validação e aprovação dos procedimentos definidos no presente documento, para que os conceitos de segurança da informação sejam disseminados aos empregados, garantindo a sua implantação e direcionamento eficaz da estrutura

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA		Código	PC-CTI-GTI-001-PT
	Política Corporativa		Revisão	1.0
	Título: Política de Segurança da Informação		Área	TI
			Páginas	16 / 29

organizacional para o cumprimento e adequação aos controles. Além disso, o Gerente Geral de TI, juntamente com o Comitê de Segurança da Informação, deverá analisar e propor alterações (Se necessário) na Política de Segurança da Informação, após as revisões periódicas realizadas (Anualmente ou sempre que for necessário).

9.2 Área de Tecnologia da Informação


A área de Tecnologia da Informação possui a responsabilidade pela operacionalização tecnológica desta política e pela sustentação dos termos definidos neste documento, a fim de satisfazer as obrigações da alta administração da companhia. Suas responsabilidades incluem:

- Revisar as questões descritas neste documento, no mínimo uma vez ao ano;
- Participar do Comitê de Segurança da Informação, a fim de discutir interesses especializados de segurança da informação, esse Comitê se reúne trimestralmente e é integrado por membros das diversas áreas de negócio da Nexa;
- Desenvolver, manter e implantar políticas, normas, procedimentos e manuais de segurança da informação de TI, fornecendo diretrizes para o desenvolvimento de uma infraestrutura de TI segura;
- Analisar e agir em casos de incidentes de segurança da informação e investigações que necessitem de apoio;
- O Gerente Geral de Tecnologia da Informação terá a responsabilidade de, juntamente com sua equipe, garantir que todas as políticas de segurança estejam devidamente elaboradas e aprovadas pelas diretorias responsáveis, a fim de garantir a sua plena aplicabilidade;
- Responder às questões de interpretação e exceções a essa política, sujeito à aprovação do Comitê de Segurança da Informação.

9.3 Empregados

Todos os empregados são responsáveis por comunicar a área de Segurança da Informação sobre qualquer situação que possa representar ameaças à

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA		Código	PC-CTI-GTI-001-PT
	Política Corporativa		Revisão	1.0
	Título: Política de Segurança da Informação		Área	TI
			Páginas	17 / 29

confidencialidade, integridade e disponibilidade das informações. É de responsabilidade dos empregados e/ou terceiros o adequado uso e sigilo das informações da Nexa e de seus clientes. Todos os empregados devem ler e assinar formalmente o Termo de Compromisso, o qual é retido pela área do DHO.

9.4 Demais Aspectos de Segurança da Informação

Os papéis e responsabilidades de segurança da informação relacionados à empregados, fornecedores e terceiros devem ser definidos e documentados de acordo com os seguintes critérios:

- Implementar e agir de acordo com as Políticas de Segurança da Informação da Nexa;
- Proteger Ativos contra acesso não autorizado, divulgação, modificação, destruição ou interferência de acordo com o Processo de Classificação da Informação e Lei Sarbanes–Oxley (SOX);
- Executar processos ou atividades particulares de segurança da informação;
- Assegurar que a responsabilidade é atribuída a pessoa para tomada de ações;
- Relatar eventos potenciais ou reais de segurança da informação ou outros riscos de segurança para a Nexa.

10. SEGURANÇA NO AMBIENTE DE TECNOLOGIA


O objetivo desta seção é estabelecer os requisitos necessários para assegurar a transmissão e armazenamento seguro dos Ativos de informação da Nexa.

10.1 Gerenciamento de Rede e Informações

As informações compartilhadas dentro da rede devem ser seguras em todos os estágios do transporte. A instalação de novas conexões para a rede não deve ser realizada sem a ciência e aprovação da área de Segurança da Informação.

Em situações em que os empregados estiverem trabalhando fora da rede corporativa e necessitarem transmitir informações confidenciais, é obrigatório o uso de senhas para proteção do conteúdo transmitido, além do uso de VPN.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	18 / 29

As configurações padrão dos servidores e demais Ativos tecnológicos que armazenam ou processam informações sensíveis não devem permitir que estes se conectem a mais de uma rede (ou sub-rede) ao mesmo tempo.

A arquitetura das aplicações deve observar o não armazenamento de informações sensíveis em redes do tipo Demilitarized Zone (DMZ).

10.2 Manipulação Segura de Mídias

Procedimentos operacionais apropriados devem ser estabelecidos a fim de proteger documentos, mídias, entrada e saída de dados e documentação contra danos, roubos e acessos não autorizados, incluindo também proteger portas sistêmicas, tanto logicamente como fisicamente contra o uso não autorizado.

10.3 Computadores e Dispositivos “Não Homologados”

Não é permitido a conexão de computadores na rede corporativa, bem como armazenamento de informações sensíveis que não aqueles adquiridos e homologados pela área de Tecnologia da Informação da Nexa.

10.4 Uso de Equipamentos Nexa


Os empregados que, por conta de suas atribuições receberem um notebook e celular, deverão no ato do recebimento, assinar o Termo de Responsabilidade Geral para Uso e Guarda de Notebook.

É obrigatória a utilização de senha para inicializar os Ativos tecnológicos (Desktops e notebooks).

Protetores de tela devem estar Ativos, com senha, em todos os computadores (Desktops e notebooks) em uso, com período para ativação que não deve exceder 15 (quinze) minutos. Quando em trânsito, os notebooks devem estar desligados (Opção shutdown).

O acesso ao e-mail por meio de telefones celulares deverá seguir mecanismos de segurança, como criptografia e configuração de senha avançada, objetivando proteger as informações contidas no aparelho. O uso de criptografia e configuração de senha é obrigatório, caso contrário não será possível o acesso.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	19 / 29

Controles apropriados de segurança devem ser aplicados na transmissão de informações confidenciais a partir de dispositivos

Os computadores da companhia devem:

- a) Possuir backups regulares;
- b) Estar protegidos contra vírus e softwares maliciosos.

10.5 Manipulação e Reutilização de Equipamentos

Todos os Ativos da Nexa devem receber manutenções preventivas de acordo com a periodicidade definida nas especificações do fabricante para assegurar sua disponibilidade e integridade permanente. Todas as manutenções devem ser executadas por equipe qualificada e as manutenções corretivas e preventivas devem ser documentadas.

A área de Tecnologia da Informação é responsável pelas atividades de instalação, manutenção, desinstalação e remoção dos Ativos tecnológicos e sistemas.

Todos os Ativos tecnológicos que contenham informações críticas devem ser destruídos fisicamente ou sobrescritos antes de serem reutilizados para outras finalidades.

10.6 Compartilhamento das Informações


As informações da Nexa em posse dos empregados deverão ser sempre criptografadas, estejam estas em computadores ou dispositivos de compartilhamento (Ex.: flash drives)

10.7 Backup de Dados Sensíveis

Todos os sistemas da Nexa que contenham informação sensíveis requeridas para conduzir operações de negócios devem ter backups realizados regularmente e armazenados em um ambiente seguro (Ex.: salas trancadas ou gabinetes com acesso limitado, de acordo com as necessidades de negócio).

Dados mantidos por longos períodos (De acordo com a legislação associada) devem ser armazenados em localidade externa, sempre observando os controles físicos mínimos descritos em seção específica desta política. Testes periódicos devem ser

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	20 / 29

realizados a fim de verificar a integridade dos dados armazenados de acordo com o Processo de Backup.

As informações poderão ser criptografadas nos servidores da companhia dependendo da natureza do projeto.

10.8 Proteção Contra Vírus

Todos os sistemas e computadores utilizados pelos empregados da Nexa devem possuir software antivírus instalado e atualizado.

10.9 Filtro de Conteúdo

Todo o acesso à internet por meio da rede corporativa deve ser verificado por uma solução de filtragem de conteúdo. Desta forma, fica expressamente proibido o uso de:

- Compartilhamento de arquivos em nuvem, tais como: One Drive, iCloud, Google Drive, Dropbox, entre outros não autorizados pela companhia (**Exceto OneDrive for Business** – *solução de armazenamento nuvem padronizada pela Nexa*);
- Compartilhamento de arquivos via P2P;
- Software de games e de recreação;
- Softwares não autorizados;
- Softwares não licenciados e não homologados;
- Acesso à conteúdos Web: pornográfico, malicioso, obsceno, violência, drogas ilícitas, chat e discriminação.


10.10 Descarte e Transferência de Mídias

A área de Tecnologia da Informação deverá definir procedimentos para garantir a execução de uma forma segura de transferência e de envio para descarte das mídias não mais utilizadas pelos empregados da Nexa, contra acesso não autorizado, uso impróprio ou corrompida, durante o transporte.

Procedimentos de descarte:

- Destruição física: incineração ou trituração;

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA		Código	PC-CTI-GTI-001-PT
	Política Corporativa		Revisão	1.0
	Título: Política de Segurança da Informação		Área	TI
			Páginas	21 / 29

- Apagar ou excluir, de forma que as informações originais sejam irrecuperáveis, utilizando softwares de exclusão (Técnica de sobrescrita).

10.11 Proteção do Ambiente de Sistemas

A área de Tecnologia da Informação utiliza a solução “Anti-Malware” que oferece proteção abrangente contra spyware, conteúdos inadequados da Web, phishing, vírus, worms e outras ameaças.

10.12 Gestão de Ativos

Todo empregado da Nexa é responsável por zelar pela integridade de qualquer recurso provido pela empresa para realização de suas atividades, e quando aplicável deve assinar o “Termo de Compromisso de Uso de Recurso”.

O transporte dos Ativos da Nexa, caso seja necessário, devem ser devidamente autorizados pelo Gerente Geral da área do empregado e da área de TI, de forma que o transporte seja feito de forma segura, garantindo assim a integridade física e lógica;

A perda, ou furto de equipamentos da Nexa devem ser reportados de forma tempestiva e o mais detalhado possível, para a área de TI Local da unidade, bem como a apresentação do Boletim de Ocorrência (BO).


10.13 Gestão de Patches

A área de Tecnologia da Informação deve atualizar mensalmente os patches críticos para as tecnologias prioritárias. A atualização de *patches* deve ser homologada a cada atualização para identificar possíveis impactos com a instalação.

10.14 Uso do Correio Eletrônico e Internet


O sistema de correio eletrônico é de utilização exclusivamente profissional, destinando-se apenas a assuntos profissionais. A Internet é um recurso de informação fornecido pela Nexa com o objetivo de aumentar a produtividade nos processos de trabalho. Seu uso deve ser direcionado para atividades profissionais, de interesse da companhia e de caráter informativo. São expressamente proibidos (as):

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Política Corporativa	Área	TI
		Páginas	22 / 29
	Título: Política de Segurança da Informação		

- A utilização do sistema de correio eletrônico corporativo para obtenção de lucro pessoal de qualquer espécie;
- O envio de mensagens de caráter geral como alerta de vírus, correntes e informativos (Exceto as enviadas ou autorizadas pela área de Tecnologia da Informação);
- A participação em salas de bate-papo, jogos pela Internet, descarregar arquivos (Download) de entretenimento, encaminhamento de correntes de e-mail e sites com conteúdo erótico ou discriminatório;
- A utilização do correio eletrônico de outras pessoas sem autorização prévia;
- O envio de mensagens com conteúdo difamatório, ofensivo ou discriminatório, que importune ou cause constrangimento às pessoas;
- As mensagens do correio eletrônico devem ser escritas em linguagem profissional e que não comprometa a imagem da Nexa, não vá de encontro a legislação vigente e nem aos princípios éticos da empresa;
- O conteúdo do correio eletrônico de cada usuário pode ser acessado pela área de TI, quando em situações que ponham em risco a sua imagem, o seu negócio e/ou a segurança. Este acesso será feito a critério da área de TI, mediante comunicação ao superior imediato do usuário, à área de Segurança e deve ser registrado formalmente permitindo uma auditoria desse procedimento. Procedimentos desse tipo são para evitar ataques de phishing, spam's, DDOS, ataques em massa e similares;
- Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão excluídas automaticamente, caracterizando assim como uma conta "inativa". As exceções como licença maternidade ou licenças por doença, vão seguir o seguinte período:
 - Licença maternidade: De acordo com o prazo legal.
 - Licenças por doença: De acordo com o tempo do laudo médico.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	23 / 29

11. SEGURANÇA FÍSICA

A presente seção define controles a fim de obter proteção para as informações da Nexa contra riscos associados à distribuição inadequada, má gestão e uso indevido dos dados. Os locais de trabalho que armazenam informações críticas, tais como salas de servidores, devem seguir os procedimentos abaixo:

11.1 Segurança Física das Instalações

As instalações da Nexa devem ser utilizadas apenas para atividades relacionadas aos negócios da companhia. O acesso às instalações é restrito aos usuários que possuem autorização para realização dos negócios.

Todos os visitantes devem ser apropriadamente identificados, designados e monitorados durante suas visitas. Os registros dos visitantes devem ser mantidos e auditados regularmente.

Todos os pontos de entrada e saída das áreas seguras de TI devem ser registrados e revisados. O acesso físico por pessoas externas devem ser restritos, supervisionados e revogados imediatamente quando não mais requerido.


11.2 Segurança Física de Equipamentos

O acesso físico às áreas nas quais estão localizados os Ativos contendo informações sigilosas e sensíveis deve ser restrito somente aos empregados explicitamente autorizados para operar ou manter os sistemas, softwares ou equipamentos tecnológicos.

Ativos tecnológicos devem ser posicionados em salas fisicamente protegidas e com acesso restrito por meio de senhas, crachás ou biometria, ou uma combinação de dois destes fatores. O uso de racks em datacenters e salas restritas de TI é imprescindível para Ativos contendo informações sensíveis. Deve ser observado, ainda, o uso de Circuito Fechado de TV (CFTV), com retenção das informações por período definido, de acordo com as necessidades do negócio a fim de possibilitar eventuais investigações.

O acesso a estes Ativos deve ser formalmente aprovado pela área de OGS-TI e controlado pela área de Facilities da unidade.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	24 / 29

11.3 Segurança de Ambientes Críticos

O Datacenter ou a sala dos servidores deverão possuir:

- Porta corta-fogo, resistente a arrombamento;
- Acesso controlado (Ex.: automático, biometria);
- CFTV posicionados de forma panorâmica (Sem registrar telas de Monitores ou teclados)
- Energia elétrica estabilizada;
- Fontes de energia alternativa (Ex.: geradores, nobreaks);
- Interruptores elétricos de emergência próximos à saída para desligar todos os Ativos em caso de incêndio;
- Detectores de incêndio baseados em fumaça ou combustão de gases;
- Extintores de incêndio (Ex.: CO2);
- Sistema de ar-condicionado exclusivo;
- Contrato de seguro.

A sala dos servidores deverá estar em perfeitas condições de limpeza e não deverá possuir material que possibilite a propagação de incêndio, como caixas de papelão, plásticos, mesas de madeira, etc.

O cabeamento da rede deverá ser protegido por conduítes e separado dos cabos elétricos.

Para casos específicos em que as informações forem processadas ou armazenadas em instalações de terceiros, estas devem seguir os mesmos parâmetros estabelecidos nas políticas internas da companhia.


11.4 Revisão e Revogação de Acesso

Os acessos físicos às áreas protegidas devem ser revisados no mínimo a cada 6 meses e revogados imediatamente quando não mais necessários.

12. MANUTENÇÃO E DESENVOLVIMENTO DE SISTEMAS

As definições desta seção foram estabelecidas para garantir que todos os membros da companhia envolvidos nos processos de desenvolvimento e manutenção

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	25 / 29

de sistemas possuam conhecimento adequado dentro dos padrões e boas práticas de mercado.


12.1 System Development Life Cycle – SDLC

A metodologia de desenvolvimento de softwares utilizada pela companhia baseia-se no modelo “Systems Development Life Cycle – SDLC”, composta por uma série de fases de trabalho claramente definidas e distintas, considerando, dentre outros itens, as etapas de planejamento, criação, testes e implantação de um sistema de informação.

Com relação aos aspectos de segurança da informação cobertos pelos controles de SDLC, foram considerados:

- Questões de segurança da informação deverão ser consideradas e analisadas criticamente a intervalos planejados, em todos os projetos;
- Todos os acessos dos desenvolvedores envolvidos deverão ser limitados de acordo com sua alçada, monitorados, registrados e revogados quando não mais necessária sua utilização;
- Os requisitos de negócio dos projetos realizados deverão considerar escopo, recursos, funções e responsabilidades, e serem suportados por um processo formal de gestão de mudanças;
- Os requisitos de negócio dos projetos realizados deverão medir o nível de esforço de desenvolvimento, bem como possuir aprovação da alta administração;
- Os requisitos de negócio deverão ser formalmente documentados e revisados sempre que necessário;
- As atualizações de software deverão ser testadas e aprovadas antes da implementação no ambiente de produção;
- As tarefas deverão ser segregadas nos ambientes de desenvolvimento, testes e produção, bem como atribuídas adequadamente entre os departamentos e/ou áreas envolvidas;
- Os requisitos de negócios dos projetos realizados deverão abordar atividades que descrevam as limitações do trabalho e proibições, bem


Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Política Corporativa	Área	TI
		Páginas	26 / 29
	Título: Política de Segurança da Informação		

como o uso adequado das informações manuseadas nos ambientes de produção e testes;

- Os requisitos de negócio dos projetos realizados deverão limitar o acesso ao código-fonte do programa ao departamento de desenvolvimento envolvido no projeto;
- Os requisitos de negócio dos projetos realizados deverão registrar todos os acessos realizados aos códigos-fonte desenvolvido;
- Os requisitos de negócio dos projetos realizados deverão especificar controles de entradas (Verificações de erro e máscaras de formulários), a fim de detectar caracteres inválidos e dados ausentes ou incompletos, dependendo da natureza dos projetos realizados;
- Os requisitos de negócio dos projetos realizados deverão avaliar os riscos envolvidos durante a aquisição de novas aplicações, análise do ambiente antes da implementação da solução, integração e compra de serviços de terceiros;
- Os requisitos de negócio dos projetos de terceiros realizados deverão possuir ambientes de desenvolvimento segregados após análise de viabilidade, bem como considerações relacionadas a natureza do trabalho;
- Os requisitos de negócio dos projetos realizados deverão especificar procedimentos de *rollback/backout plan* (Restauração de serviços ao seu estado anterior à mudança) necessários para promoção ao ambiente de produção;
- Os requisitos de negócio dos projetos realizados deverão possuir código-fonte do ambiente de produção segregado dos recursos de informação (Servidores, etc.);
- A fim de permitir segurança apropriada das informações, as aplicações devem fazer o uso do conceito de 3 (três) camadas em servidores dedicados, considerando: apresentação, lógica de negócio e de dados;
- Os requisitos relacionados à proteção de informações confidenciais da companhia devem ser avaliados previamente à aquisição de novas

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	27 / 29

aplicações, análise do ambiente antes da implementação da solução, integração e compra de serviços de terceiros;

- O uso de dados de produção para testes deve ser evitado, a fim de proteger informações sensíveis e confidenciais. Entretanto, em casos extremos, ferramentas de mascaramento de dados devem ser utilizadas antes destes serem disponibilizados às áreas de teste.

12.2 Homologação de Sistemas e Aplicativos

Apenas a área de Tecnologia da Informação está autorizada a efetuar e/ou orientar a instalação ou remoção de softwares homologados nas estações de trabalho e servidores. Nenhum software poderá ser desenvolvido, adquirido e/ou instalado sem que seja avaliado e homologado pela área de Tecnologia da Informação.

13. COMPLIANCE

As definições desta seção foram estabelecidas para garantir o cumprimento correto da Política de Segurança da Informação pelos empregados da companhia.


13.1 Revisão e Aprovação do Documento

A Nexa reserva o direito de revisar e reavaliar as Políticas de Segurança da Informação anualmente ou sempre que for necessário a fim de buscar alinhamento à legislação e melhores práticas de mercado. As revisões devem ser coordenadas pelo Gerente da Segurança da Informação e aprovadas pelo Comitê de Segurança da Informação e a Diretoria Executiva. É de responsabilidade de qualquer usuário que tenha conhecimento de um Ativo de informação que não esteja em conformidade com as diretrizes da política reportar o incidente para a alçada competente, de acordo com Processo de Gestão de Incidentes definido.

13.2 Exceções

Não são esperadas exceções à política. Eventuais exceções devem ser documentadas, analisadas e aprovadas pelo Comitê de Segurança da Informação e o Diretor Executivo.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---

	NEXA Política Corporativa	Código	PC-CTI-GTI-001-PT
		Revisão	1.0
	Título: Política de Segurança da Informação	Área	TI
		Páginas	28 / 29

13.3 Penalidades

Os empregados e terceiros que violarem as normas e regras da Nexa referentes à Política de Segurança da Informação são passíveis de punição:

- Perda de acesso a determinados recursos;
- Advertência formal e comunicação do ocorrido ao superior imediato;
- Aplicação de sanções trabalhistas previstas em legislação vigente, incluindo dispensa por justa causa ou afastamento (No caso de terceiros, aplicação de sanções de acordo com o contrato de prestação de serviços compactuado entre as partes);
- Processo civil ou criminal;
- Aplicação de ações disciplinares constantes na legislação do país;
- Ressarcimento dos prejuízos causados à companhia conforme previsto em contrato ou apurado pelo órgão competente;
- Reparação dos danos causados à companhia;
- Aplicações dos procedimentos definidos no Código de Conduta da Nexa.

14. INFORMAÇÕES COMPLEMENTARES

Não aplicável.

15. ANEXOS

Não aplicável.

Elaborador: Fabiano Alves	Classificação: Uso Interno	Aprovador: Valdecir Botassini
-------------------------------------	--------------------------------------	---