Política: Corporativa de Segurança da Informação

INDICE

DISTRIBUIÇÃO:

Esse documento é disponibilizado a todos os colaboradores da **New Voice Telecom** através da equipe de Segurança da Informação. Em caso de dúvida entre em contato através do e-mail: seguranca.informacao@nvtelecom.com.br

Histórico da Última Revisão:		
Revisão nº:	**Data:**	**Itens Atualizados:**
1.0	31/05/2023	Versão inicial
2.0	31/05/2024	Revisão Periódica

Aprovações Internas:			
Revisão nº:	**Data:**	**Autor:**	**Aprovador:**
1.0	31/05/2023	Marcos A Cabral	Comitê GRC
2.0	31/05/2024	Marcos A Cabral	Comitê GRC

1. Objetivo

A **New Voice Telecom** reconhece que os sistemas de informação e as informações são parte integrante do negócio, tornando os ativos críticos e importantes. O objetivo dessa Política de Segurança da Informação é garantir a integridade, confidencialidade e disponibilidade de todos os recursos de informação.

Dessa forma, as diretrizes aqui contidas asseguram:

- Que os sistemas estejam disponíveis sempre na medida em que haja necessidade de acessá-los;
- Que somente pessoas designadas pelos gestores tenham acesso à informação requerida, garantindo sua confidencialidade;
- Que as informações estejam íntegras e invioláveis quando acessadas pelos usuários;

Normas adicionais são desenvolvidas, a fim de atender:

- Diretrizes contidas nesse documento;
- Objetivos de negócio da **New Voice Telecom**;
- Requisitos de segurança da informação de nossos clientes;
- Melhores práticas do mercado ou regulamentações

Adicionalmente um documento chamado "**Cartilha de Conscientização para Usuários**" contempla de forma resumida os requisitos mais críticos e que merecem atenção devida dos nossos colaboradores.

1.1 1.1 Direito autorais e copyright

Os ativos desenvolvidos e utilizados internamente são de uso exclusivo da **New Voice Telecom** e estão de acordo com nossos objetivos de negócio e em linha com o serviço contratado pelos nossos clientes.

Qualquer uso sem o consentimento e ciência da empresa será considerado quebra de direitos autorais de acordo com a lei número: **9.610** de 19 de fevereiro de 1998.

2. Aplicação

Esta política se aplica a todos os recursos de informação utilizados pela **New Voice Telecom**, incluindo os dados internos e/ou externos, sistemas, servidores, softwares, aplicações, infraestrutura de rede e seus colaboradores internos e prestadores de serviço.

A Política Corporativa de Segurança da Informação define os requisitos que todos os colaboradores da **New Voice Telecom** necessitam atender para assegurar o gerenciamento de risco adequado dos sistemas da informação e tecnologias que suportam os nossos negócios.

Esse procedimento é divulgado a todos os colaboradores das operações, administrativo e tecnologia da informação através da Intranet corporativa da **New Voice Telecom.**

Todos os colaboradores da matriz e filiais devem seguir as diretrizes contidas neste documento. Adicionalmente prestadores de serviço, fornecedores e demais parceiros de negócio da **New Voice Telecom** também devem seguir essas diretrizes.

No caso de alguma demanda ser estritamente necessária ao ambiente de negócios da organização, porém fora do contexto de conformidade e sem as recomendações da Gerência de Segurança da Informação, cartas de risco podem ser adotadas de forma a mitigar e proteger a organização de vulnerabilidades e exposições desnecessárias.

Essa Política de Segurança da Informação está disponível na intranet corporativa da **New Voice Telecom** e uma cópia original impressa está disponível junto a área de Segurança da Informação. Dúvida de utilização entre em contato com a área através do e-mail: seguranca.informacao@nvtelecom.com.br

3. Documentos Referenciados

- Cartilha de Conscientização para Usuários
- Termo - Aceite da Política Corporativa de Segurança da Informação
- Lista de requisitos legais, regulatórios, contratuais e outros

4. Definições

AD – Active Directory

É um serviço de diretório que armazena informações sobre objetos em rede e disponibiliza essas informações a usuários e administradores de rede.

CSIRT

É o acrônimo de Computer Security Incident Response Team – Time de Resposta a Incidentes de Segurança da Informação. Responsável por receber, identificar, analisar e tratar incidentes críticos de segurança da informação dentro do ambiente corporativo.

Hardening

É um processo utilizado para diminuir o nível de vulnerabilidades em software e hardware através da desabilitação de serviços e processos desnecessários nesses dispositivos computacionais.

Logs

É uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

Perfil de administrador

É perfil que dá direito a funções administrativas ao computador ou a um sistema específico, sendo possível alterar configurações críticas, mudar padrão adotado pela empresa, alterar regras de segurança, etc.

Proxy

É o termo utilizado para definir os intermediários entre o usuário e seu servidor. E por isso desempenha a função de conexão do computador (local) à rede externa (Internet). Como os endereços locais do computador não são válidos para acessos externos, cabe ao proxy enviar a solicitação do endereço local para o servidor, traduzindo e repassando-a para o seu computador.

Softwares proprietários e de terceiros

Softwares proprietários são os softwares desenvolvidos internamente para as necessidades de negócio da **New Voice Telecom** ou adquiridos legalmente através de processos de compras. Já os softwares de terceiros são os pertencentes aos nossos clientes utilizados em suas respectivas.

Scan

Realizar um "scan" significa executar uma varredura, vasculhar, averiguar um objeto, nesse caso um ativo (hardware, software, sistema, aplicativo etc.). Fazer um "scan "com um antivírus, por exemplo, é usar uma ferramenta que realiza uma varredura em busca de vulnerabilidades e fragilidades.

5. Desenvolvimento

5.1 Introdução

A segurança da informação faz parte de todas as organizações como medida de proteção aos seus negócios. Um dos pontos fundamentais no contexto dessa segurança, dessa proteção é o estabelecimento de diretrizes e regras de uso dos ativos que suportam os objetivos de negócio.

Esses ativos podem ser recursos tecnológicos, como computadores, servidores, links de comunicação, e-mails, bancos de dados e recursos humanos que farão uso desses recursos.

A Política de Segurança da Informação da **New Voice Telecom** tem como objetivo, estabelecer as regras mínimas e aceitáveis para a proteção dos nossos negócios e as informações dos nossos clientes.

Essa política é estabelecida pela Gerência de Segurança da Informação e periodicamente atualizada, monitorada e em linhas com os objetivos de negócio, requisitos de nossos clientes e refletindo melhores práticas e compliance do mercado.

Adicionalmente, a Política de Segurança da Informação da **New Voice Telecom** é discutida mensalmente através de reunião realizada junto ao Comitê de Segurança da Informação.

Esse comitê é constituído por representantes com cadeira cativa: CEO, sócios, representante de infraestrutura, sistemas, segurança da informação e Recursos Humanos e quando necessários representantes rotativos.

Os representantes rotativos são convidados quando haja impactos significativos nas operações e áreas administrativas. Dessa forma, poderão ser convidados: Jurídico, Financeiro, Comercial, etc.

5.2 Diretrizes Básicas de Segurança da Informação:

Todos os recursos de informação são ativos corporativos de propriedade da **New Voice Telecom**. Como exemplo de ativos corporativos:

- Computadores (desktops/notebooks), monitores, head sets e demais hardwares que auxiliam na execução das atividades de negócio;
- Softwares proprietários e de terceiros (nossos clientes) que auxiliam e suportam os objetivos de negócio;
- Cadeiras, mobiliário, telefones, celulares;
- Informações impressas e em formato digital.

Cada usuário é responsável pela utilização de todos os ativos citados, seja preservando e fazendo bom uso dos mesmos. Cada usuário necessita ter em mente que é responsável pela proteção das informações e que faz parte do contexto da segurança da informação e dos controles internos da organização.

Gestores (Coordenadores, supervisores, gerentes, superintendentes e diretores) são responsáveis em utilizar princípios básicos para concessão e uso da informação. São eles:

- **Necessita saber/conhecer (Need to know basis):**

Consideração: Qual a real necessidade de se usar esse aplicativo? Tem como princípio, objetivos de negócio? Auxiliará nas atividades do usuário? Conseguirá o usuário realizar suas atividades sem esse aplicativo? Acesso?

- **Privilégio mínimo (Least privilege):**

Consideração: Utilizar o princípio de autorizar o mínimo de acesso necessário ao usuário e quando justificado liberar o acesso; ao contrário de liberar o máximo de acesso possível e bloquear quando identificado que o acesso não é necessário.

5.3 Administração da Política de Segurança da Informação

O Comitê de Governança, Riscos e Compliance é responsável pelo desenvolvimento e pela manutenção da Política de Segurança da Informação, normas e procedimentos de segurança de forma compatível com a governança e práticas da **New Voice Telecom.**

À medida que os negócios da empresa evoluam, estejam mais suscetíveis a riscos e o uso da tecnologia da informação se torne mais abrangente, essa Política de Segurança da Informação precisa refletir esses elementos e inserida no contexto da educação contínua dos usuários e sua conscientização.

A **New Voice Telecom** se reserva no direito de tomar as medidas adequadas para assegurar que os padrões e procedimentos sejam cumpridos. Qualquer falha com o respeito a essa política é suscetível a medidas disciplinares.

5.4 Definições e Papéis e Responsabilidades

Responsabilidades dos Usuários:

Cada usuário da **New Voice Telecom** tem a responsabilidade de usar os recursos do computador e da rede de forma adequada para facilitar as atividades empresariais. Somos todos responsáveis pela salvaguarda destes ativos da empresa. Todos os usuários destes ativos da empresa são obrigados a aceitar as seguintes responsabilidades:

I - Salvaguardar todos os dados e informações pessoais, senhas, códigos de autorização, e dados confidenciais.

II - Seguir as políticas, normas e procedimentos de segurança estabelecidos para controlar o acesso e uso de todos os dados.

III - Respeitar a integridade dos ativos de informação (rede/computadores). Alterações de qualquer sistema ou componente de software de rede ou os dados só podem ser realizadas por pessoal autorizado.

IV - O uso de qualquer recurso de computação da empresa para fins comerciais não relacionados com os negócios da **New Voice Telecom** ou atividades não relacionadas ao trabalho ou que sejam ilegais ou antiéticas constituem uma violação desta política.

V - Usuários de computador e/ou ativos de rede estão sujeitos a todas as leis aplicáveis à Política de Segurança da Informação. Software não comercial e pessoal não pode ser instalado em computadores disponibilizados pela empresa. Além disso, os usuários não podem realizar downloads de softwares a partir da Internet sem a concordância da área de TI. Usuários são responsáveis pelo software e a sua legalidade nos computadores sob sua responsabilidade.

VI - Reportar a área de Gerência de Segurança da Informação e Gerência de Recursos Humanos, caso ocorram as seguintes situações:

a) Política de Segurança da Informação foi ou está sendo violada.

b) A informação sensível da **New Voice Telecom** foi perdida, divulgada a terceiros não autorizados, ou suspeita de serem perdidas ou divulgadas a terceiros não autorizados.

c) Uso não autorizado de sistemas de informação da **New Voice Telecom** ocorreu, ou é suspeito de ter ocorrido.

d) Senhas ou outros controles de acesso do sistema são perdidas, roubadas, ou divulgadas ou são suspeitas de terem sido perdidas, roubadas ou divulgadas.

e) Há qualquer comportamento incomum nos sistemas, tais como arquivos ausentes, frequentes falhas no sistema ou mensagens perdidas.

VII - Ler e adotar a sensibilização para a segurança da informação.

Responsabilidades dos gestores:

I – É necessário que gestores garantam que suas equipes compreendam e possuam acesso à Política de Segurança da Informação e entendam onde podem obter ajuda.

II – É necessário que gestores garantam que qualquer acesso não mais necessário, seja desativado ou excluído entrando em contato com a área de TI. Adicionalmente requisito obrigatório que uma vez solicitado pela Gerência de Segurança da Informação realizem revisões de acessos e de perfis periodicamente.

III – Gestores devem ter ciência, monitorar e informar a Gerência de Segurança da Informação sobre qualquer acesso de terceiros (Fornecedores, prestadores de serviço, parceiros de negócio e empresas do grupo) ao ambiente da **New Voice Telecom.**

IV - Gestores não podem divulgar em hipótese alguma, senhas, direta ou indiretamente, para qualquer um.

Responsabilidades específicas dos Proprietários de Dados (data owners):

I - Garantir a precisão e a qualidade dos dados constantes nas aplicações.

II - Estabelecer níveis de acesso com base em segregação de funções e com princípio de menor privilégio (**Least Privilege**) e necessidade de saber/conhecer (**Need to Know**).

III - Revisar e validar periodicamente quem tem acesso aos dados.

IV - Revisar e autorizar mudanças nos sistemas e componentes relacionados.

V - Classificar dados proprietários e determinar o nível adequado de proteção (sob a delegação do proprietário do sistema).

Responsabilidades específicas dos Proprietários de Sistemas:

I - Um proprietário de sistema é o indivíduo a quem foi atribuída a responsabilidade final para:

a) Funcionalidades sistêmicas,

b) Integridade dos dados,

c) Classificação adequada dos dados,

d) Requisitos de retenção de dados,

e) Tipos e níveis de acesso,

f) Alterações nos sistemas.

II - Proprietários dos sistemas poderão delegar certas tarefas para outros grupos, mas permanecem em última instância, responsáveis por eles.

Exemplos:

a) Administração de segurança para provedores de serviços,

b) Classificação de dados para os proprietários de dados,

c) Aprovação de acesso padrão ao sistema de Gerenciamento de Usuários e / ou serviço de fornecedores.

Responsabilidades específicas dos Provedores e Prestadores de Serviço:

I - Provedores e Prestadores de Serviço podem ser internos ou terceirizados. Os provedores de serviços exercem suas responsabilidades com base na delegação de proprietários do sistema. Eles fornecem serviços, incluindo:

a) Infraestrutura,

b) Operações de TI,

c) Monitoramento de acessos,

d) Conceder / ajustar / cancelar o acesso (com base nos proprietários de dados/ sistemas e instruções do Gerenciamento de Usuários).

e) Assegurar controles de operação adequados sobre as aplicações a fim de manter um ambiente seguro de processamento (sob a delegação do proprietário do sistema).

II - A política em relação à segregação de função é que as equipes e áreas necessitam estar alinhadas com limites funcionais claros que cumprem com os princípios de segregação de funções.

III – É mandatório que os acessos aos sistemas sejam controlados para permitir que os colaboradores trabalhem apenas dentro de suas áreas funcionais.

5.5 Gestão de Ativos da Informação

5.5.1 Utilização de Equipamentos Eletrônicos

I - Não é permitido o uso de aparelhos celulares, computadores de mão, agendas eletrônicas, smartphones entre outros equipamentos eletrônicos no ambiente de operação.

a) A utilização destes equipamentos necessita ser previamente aprovada pela Gerência de Segurança da Informação, durante a realização e acompanhamento de auditorias;

b) A utilização de equipamentos móveis está autorizada no ambiente de operação, somente para os gestores que possuam equipamento corporativo e que seja de uso para fins de negócio.

II - A produção de vídeos e fotografias é proibida nos ambientes corporativos.

a) As áreas de Comunicação Interna e Segurança do Trabalho, bem como a Gerência de Segurança da Informação, durante a realização e acompanhamento de auditorias, possuem autorização prévia para esta ação.

III - Os equipamentos móveis de clientes, fornecedores e prestadores de serviço somente podem ser conectados à rede corporativa após:

- Abertura de chamado junto ao Service Desk com justificativa de uso;
- Aprovação pelo gestor responsável;
- Análise e aprovação pela Gerência de Segurança da Informação.

a) Após o uso; término do serviço prestado, o acesso será retirado.

b) O Gestor é responsável pelo uso correto, responsável e em linha com as diretrizes de negócios e segurança da informação.

IV - Não é permitida a utilização de equipamentos eletrônicos pessoais na empresa Center. O uso do mesmo está sujeito a penalidades previstas de acordo com o **Código de Ética e Conduta** assinado pelo colaborador (a).

5.5.2 Computadores

I – É mandatório que os colaboradores encerrem ou bloqueiem a sessão da estação de trabalho sempre que se ausentarem do posto de trabalho.

II - Os colaboradores não poderão, em hipótese alguma, alterar os padrões definidos ou desativar os mecanismos de segurança disponibilizados pela **New Voice Telecom.**

a) Auditorias periódicas são realizadas e reincidências serão passíveis de penalidades.

III - Apenas as equipes de suporte poderão adicionar, alterar ou remover equipamentos e softwares em estações de trabalho, servidores e outros ativos da empresa.

IV - Apenas softwares homologados e licenciados podem ser instalados nas estações de trabalho, notebooks e servidores da empresa.

a) É mandatório que softwares exigidos pelos nossos clientes e necessários a operação de negócios dos mesmos passem por processo de análise de vulnerabilidades e somente serão aceitos em nosso ambiente se as mesmas forem corrigidas e estiver dentro de padrões de segurança.

V - A cópia de softwares, adquiridos ou desenvolvidos pela **New Voice Telecom**, é vedada, salvo em casos de autorização da área responsável pelo controle de ativos.

VI - Não é permitida a utilização simultânea de mais de uma interface de rede (placas de rede, modens, conexões moveis, celular, entre outras) em segmentos diferentes, na rede corporativa.

5.5.3 Notebooks e Celulares Corporativos

I – É mandatório que colaboradores que possuem direito a notebook e celular corporativo assinem o termo de uso desses ativos.

II – É obrigatório que todos os equipamentos sejam entregues sem perfil de "Administrador" aos usuários e somente com os softwares homologados pela empresa. Para isso, uma lista com os softwares permitidos e homologados será divulgada periodicamente para fins de ciência e conformidade.

III - Os colaboradores são obrigados a utilizar cabos de segurança fornecidos pela empresa sempre que se ausentarem da frente dos mesmos quando estiverem alocados presencialmente seja nas dependências da empresa, seja nos clientes onde prestam o serviço.

a) Auditorias periódicas são realizadas e os equipamentos encontrados sem a trava de segurança serão recolhidos e um comunicado da Gerência de Segurança da Informação será deixado na mesa do usuário para que o mesmo retire o equipamento junto ao seu gestor imediato. Reincidências serão passíveis de penalidades.

IV - Informações pessoais são proibidas de serem utilizadas nos dispositivos. Tanto notebook, quanto em celulares corporativos.

V – É mandatório que o backup de informações corporativas nos notebooks disponibilizados e nos celulares corporativos seja armazenado periodicamente em local apropriado e protegido de acordo com diretrizes contidas na norma de backup corporativo.

VI - Não é permitida a utilização de notebooks e celulares pessoais para os objetivos de negócio da **New Voice Telecom**. Na hipótese de o equipamento corporativo estar danificado, a área de Tecnologia da Informação providenciará outro equipamento dentro dos prazos estipulados.

5.5.4 Uso Aceitável de Ativos de Informação

I - Toda informação sensível ao negócio necessita ser classificada seguindo os critérios pré-estabelecidos na norma intitulada "**Classificação da Informação**".

II – É mandatório que sejam disponibilizados aos setores críticos da organização fragmentadores de materiais a fim de evitar que documentos sensíveis descritos na Política "**Classificação da Informação**" sejam furtados e desviados da organização.

III - Os proprietários (owners) dos ativos críticos da organização necessitam ser identificados e as responsabilidades dos mesmos identificadas.

5.5.5 Segurança e Manuseio de Mídias

I - É vedada a utilização de mídias removíveis graváveis, tais como pendrives, HDs externos e gravador de CD/DVD. Limitada a Diretoria executiva da **New Voice Telecom** e a equipe de suporte desde que justificado e com formalização de chamado.

II – É mandatório que o descarte das mídias que contenham as informações da **New Voice Telecom** seja realizado em conformidade com a Política de "**Classificação da Informação**".

5.5.7 Internet

I - O uso da internet não será permitido, entre outros, para:

a) Download de softwares, músicas, vídeos, entre outros documentos que não façam parte da rotina de trabalho do colaborador.

b) Violar leis e acessar conteúdos incompatíveis com os valores da **New Voice Telecom**, tais como: pornografia, incitação à violência, pedofilia, preconceitos em geral, entre outros.

c) Acessar sites de relacionamento, chat, ferramentas de mensagem instantânea, skype e outras ferramentas que permitam o envio de informações para fora da empresa sem prévia autorização.

d) Comprometer a privacidade ou o sigilo das informações de terceiros e internas da **New Voice Telecom** através das redes sociais. Nenhuma informação sobre a empresa e seus clientes pode ser divulgada sem a autorização da área de Comunicação Interna da empresa.

e) Praticar qualquer tipo de hostilidade eletrônica, tais como: alterar ou destruir a integridade de informações armazenadas em computadores sem a devida autorização.

II – É mandatório que os colaboradores que atendam às operações possuam acesso apenas às páginas necessárias às suas respectivas funções.

III - Será vedado o acesso a sites que não sejam considerados de interesse da empresa ou que possam comprometer sua imagem ou a segurança das informações.

IV – O acesso à Internet necessita ser realizado através de Proxy, ou de outro mecanismo de filtragem, sendo os serviços HTTP e HTTPS previamente autorizados, desde que não infrinjam o artigo acima. A liberação dos demais serviços necessitam ser aprovados pela Gerência de Segurança da Informação e pela gerência responsável pelo ambiente de Produção.

V – A **New Voice Telecom** monitora regularmente o uso da Internet na empresa, a fim de preservar a integridade das informações, identificar vulnerabilidades e falhas de segurança, bem como verificar o uso adequado desta ferramenta.

VI – Os serviços disponibilizados através da Internet podem ser desativados temporariamente caso haja indício de tentativas de quebra de segurança, ou outras ações que ponham em risco a imagem ou os negócios da **New Voice Telecom** ou de seus clientes.

5.5.8 Correio Eletrônico

I – É mandatório que os colaboradores adotem uma linguagem e postura condizentes com os valores da **New Voice Telecom**, evitando gírias e palavras de baixo calão. É vedado, entre outros, o envio de:

a) Spam.

b) Conteúdo pornográfico, incitação à violência, pedofilia, preconceitos em geral, hacker, entre outros.

c) Informações classificadas como confidenciais e restritas (internas), sem autorização previa do responsável pela informação.

II – É mandatório que a concessão de contas de correio eletrônico aos colaboradores seja realizada de acordo com os interesses da **New Voice Telecom**. A Gerência de Segurança da Informação se reserva ao direito de revogar qualquer acesso em caso de suspeita de má utilização.

III - Toda informação transmitida por meio de correio eletrônico é de responsabilidade de seu remetente, sendo observado, especialmente, o conteúdo daquelas endereçadas ao ambiente externo. É vedado o uso de correio eletrônico particular dentro dos ambientes da **New Voice Telecom**.

IV - É obrigatória a utilização do termo de confidencialidade de e-mail abaixo da assinatura de cada indivíduo.

5.5.9 Sistemas e Utilização de Ferramentas Corporativas

I – É mandatório que os sistemas sejam utilizados de acordo com os interesses da **New Voice Telecom**, sendo vedada a utilização deste em benefício próprio ou de terceiros.

II - As ferramentas corporativas disponibilizadas aos colaboradores são de uso exclusivo profissional e de acordo com os interesses da **New Voice Telecom**.

III - A Gerência de Segurança da Informação se reserva ao direito de poder acessar registros, e-mails, sistemas e qualquer informação existente no ambiente da **New Voice Telecom**, a qualquer momento, sempre que julgar necessário, podendo solicitar o recolhimento do equipamento, para inspeção física e lógica do mesmo.

IV - A Gerência de Segurança da Informação poderá bloquear o acesso a estas ferramentas em caso de suspeita de má utilização.

V – Não é permitido o perfil de "administrador" para sistemas, ferramentas, utilitários e demais recursos que suportem os objetivos de negócio. É necessário o mapeamento e estabelecidos os perfis necessários que terão acessos a esses recursos.

5.6 Segurança em Recursos Humanos

I – Todo colaborador deve passar por processo de verificações de histórico profissional e de antecedentes a fim de verificar perfis que não estejam aderentes aos processos de negócio e em linha com compliance no que tange a valões éticos, morais e íntegros. É necessário que todo colaborador receba instruções sobre Segurança da Informação ao ser contratado pela **New Voice Telecom**. Esse treinamento será realizado no momento de integração do mesmo a empresa, onde este assinará os devidos termos de uso e responsabilidade.

II - Tanto os colaboradores que trabalharão na operação, quanto os colaboradores administrativos e de Tecnologia Informação são obrigados a passar por tal treinamento em todos os níveis (operadores, auxiliares, assistentes, analistas, especialistas, gestores, supervisores, superintendentes, gerentes, diretores).

III - Antes de exercer qualquer função na empresa, todo funcionário necessita receber treinamento adequado sobre como realizar suas atividades, exceto em casos em que o funcionário tenha seu conhecimento atestado. Isto tem como objetivo minimizar risco de falhas nos procedimentos operacionais.

IV - Treinamentos específicos em Segurança da Informação necessitam ocorrer em até 21 dias após a contratação. É obrigatório que o treinamento ministrado seja evidenciado e armazenado até o encerramento do vínculo empregatício do colaborador.

V - Treinamentos e campanhas regulares de segurança da informação são realizados a cada 6 (seis) meses e necessitam obrigatoriamente ser evidenciados para fins de auditorias internas e externas dos nossos clientes.

VI - A educação contínua em segurança da informação utiliza dos seguintes mecanismos:

a) Intranet Corporativa da **New Voice Telecom**.

b) Campanhas periódicas através de palestras proferidas pela Gerência de Segurança da Informação.

c) Distribuição de kits com material educativo (mouse pads, bottons, vídeos educativos).

d) Utilização de comunicação interna com mensagens educativas.

e) Utilização de papel de parede e protetor de tela com temas sobre segurança da informação.

5.7 Segurança da Informação para Terceiros

I – Todos os colaboradores denominados "terceiros", onde se enquadram: fornecedores, prestadores de serviço, parceiros de negócio e empresas do grupo **New Voice Telecom** devem seguir as diretrizes dessa política de segurança da informação.

II – Toda demanda envolvendo "terceiros" deve previamente ser abordada através do respectivo Acordo de Não Divulgação (**NDA – Non Disclosure Agreement**) a fim de salvaguardar as informações tratadas entre ambas as partes. Para efeitos de alinhamento e diretriz, os NDAs devem ser firmados quando e não restrito a:

- reuniões comerciais
- apresentação de produtos
- reuniões com fornecedores
- provas de conceito (POCs), etc.

III – Os respectivos Acordos de Não Divulgação devem ser atualizados a cada 6 (seis) meses, devendo os envolvidos colher novas assinaturas e enviar tanto o arquivo digital como o arquivo impresso a Gerência de Segurança da Informação.

IV – Os terceiros devem ser registrados e identificados de maneira diferenciada em nossa rede corporativa, sistemas e demais ativos da organização.

V – Esse registro é mandatório através de chamado formalizado junto ao Service Desk corporativo onde as seguintes informações são necessárias:

- Nome completo do colaborador, CPF e empresa que faz parte
- De Acordo do gestor da gerência que trabalhará diretamente com o terceiro e aprovação da área de Segurança da Informação.
- Uma vez aprovado o chamado, o seguinte padrão de criação deverá ser seguido: CPF.ext (CPF sem o dígito. ext).

VI – É mandatório que os acessos sejam concedidos por um período inicial de 3 meses, renováveis por mais 3 meses através dos processos de aprovação citado no item anterior.

Adicionalmente qualquer usuário denominado "terceiro" não pode ter a opção nos sistemas de controle como "Nunca expirar senha".

VII – Todo acesso de terceiros à internet através da rede corporativa da **New Voice Telecom** é concedido através de abertura de chamado junto ao Service Desk, com as devidas aprovações citadas no item V, onde os mesmos serão inseridos no grupo de acesso padrão com funcionalidades básicas de navegação.

VIII – Todo acesso de terceiro requer o Termo de Responsabilidade preenchido e assinado pelo solicitante e do Gestor responsável pelo terceiro, além do termo de uso de VPN quando se fizer necessário.

5.8 Segurança Física e do Ambiente

5.8.1 Utilização de Crachás

I - É obrigatório o uso de crachá em todas as dependências da **New Voice Telecom** (quando em regime presencial) de modo que seja possível visualizar a identidade do colaborador (a).

II - É expressamente proibido utilizar o crachá fora das dependências da empresa, a fim de evitar que o colaborador seja identificado em qual empresa trabalha, seu nome, matrícula e sujeito a "engenharia social" utilizada por pessoas com má intenção.

III - É expressamente proibido utilizar o crachá para auxiliar outro colaborador ter acesso à determinada dependência dentro da empresa.

IV – É mandatório que em caso de perda ou roubo, o colaborador (a), avise imediatamente a área de Recursos Humanos da **New Voice Telecom** para que bloqueie imediatamente o ID desse crachá a fim de evitar que a pessoa de posse do mesmo obtenha acesso às dependências da empresa.

5.9 Gerenciamento de Operações e Comunicações

5.9.1 Gestão de Incidentes e Solicitações

I - Todas as demandas envolvendo incidentes e solicitações da **New Voice Telecom** necessitam ser registradas, categorizadas e direcionadas através de ferramenta de controle de chamados apropriada.

II – É obrigatória a existência de um catálogo de serviços apropriado contendo as demandas mais comuns envolvendo os incidentes e solicitações. Esse catálogo necessita possuir categorias de sistemas e recursos utilizados na operação, administrativo e TI (Exemplo: Nice, CMS, Protheus, AD, etc).

III – É necessário um ponto único de contato (Help Desk ou Service Desk) estabelecido para receber as demandas (incidentes/solicitações) de toda a empresa, através de ramal único, 0800 ou e-mail.

IV - Não são permitidos atendimentos realizados através de e-mail ou telefone sem que os mesmos não tenham sido registrados e gerenciados de forma apropriada.

V – É mandatório que níveis de serviço e os grupos de suporte designados sejam identificados, bem como período de cobertura do grupo de suporte (Exemplo: segunda a sexta – 8X5 ou domingo a domingo – 24X7).

VI – É necessário que seja estabelecida árvore de escalonamento e notificações para cada item do catálogo de serviços, incluindo processo de aprovação quando esse exigir.

VII – Os incidentes de segurança críticos que impactam consideravelmente o ambiente de negócios dos clientes deve ser informados através de seus respectivos CSIRTs (Computer Security Incident Response Team – Time de Resposta a Incidentes de Segurança da Informação) ou outro canal de report e formalização descrito em contrato ou através de requisitos de segurança da informação.

5.9.2 Gestão de Mudanças

I - Qualquer alteração no ambiente de produção necessita obrigatoriamente ser formalizada através de registro na ferramenta de controle de chamado. Isso inclui alterações em sistemas, infraestrutura de TI e infraestrutura física.

II – É mandatório que o processo de gestão de mudanças possua critérios de separar/segregar mudanças tendo como origem: novos projetos e incidentes/problemas identificados.

III – É obrigatório que qualquer mudança passe pela aprovação das seguintes áreas: Tecnologia da Informação, Segurança da Informação e Desenvolvimento de Sistemas.

IV - Mudanças emergências necessitam ser formalizadas, ainda que após a efetivação da mudança efetuada.

V – É mandatório que toda mudança seja realizada com os seguintes requisitos:

- Número, ID da mudança
- Dono da mudança (owner)
- Descrição da mudança a ser efetuada em detalhe
- Riscos envolvidos
- Plano de retorno (rollback) em caso de falha
- Áreas ou sistemas afetados
- Telefone de contato dos envolvidos e áreas impactadas

5.9.3 Controle de Acessos

I – É obrigatório que todos os acessos necessários a sistemas, servidores, VPN e acessos físicos sejam controlados e o seguinte fluxo executado:

- Abertura de chamado
- Aprovação do gestor imediato
- Aprovação do "owner", dono aplicação
- Aprovação da Gerência de Segurança da Informação (Dependendo da criticidade)

II – Os acessos são concedidos com base nos critérios de necessidade e privilégio mínimo, sendo utilizada a matriz de acessos x perfis para efeitos de referência e diretriz básica,

III – Os sistemas, aplicações, utilitários disponibilizados pela **New Voice Telecom** devem ser parametrizados para que não haja login simultâneo dos usuários, ou seja, controle de cessão vinculada apenas a um usuário.

IV - É mandatório que revisões de acessos sejam realizadas a cada (2) meses em todos os sistemas, aplicações que sirvam de apoio às necessidades de negócio da **New Voice Telecom**. Os gestores (owners) são responsáveis pela revisão e a área de Segurança da Informação direcionará as atividades necessárias para esse processo.

V - Independente da área que conceder acesso, é obrigatório que as diretrizes contidas nessa Política de Segurança da Informação sejam seguidas.

VI - Todos os acessos, sejam eles lógicos ou físicos, necessitam prover logs, de modo a verificar acessos realizados e identificar possíveis falhas de segurança ocorridas.

5.9.4 Mesa Limpa

I - Toda informação sensível ao negócio necessita ser armazenada em local apropriado e compatível seguindo os critérios pré-estabelecidos na política intitulada "**Classificação da Informação**".

II - As credenciais de acesso aos sistemas corporativos ou de clientes não podem ficar expostas em locais de fácil acesso. Não é permitido que os colaboradores as escrevam em papéis ou em documentos eletrônicos.

III – É mandatório que impressões e cópias sejam recolhidas imediatamente e guardados em locais apropriados.

IV - Não será permitido o manuseio de alimentos, bebidas ou fumo em ambientes nos quais existam estações de trabalho, servidores ou documentos classificados como críticos para a empresa.

V - Informações que não sejam mais necessárias aos colaboradores necessitam ser descartadas de modo adequado

5.9.5 Política de Senhas

I - Os logins e senhas fornecidas são de uso pessoal e intransferível.

a) É vedado ao titular compartilhamento ou fornecimento desta a terceiros;
b) É vedada a utilização destas por colaboradores que não sejam seu titular;

II - As senhas de acesso são classificadas como informação confidencial e, como tal, precisam possuir os controles definidos na política "**Classificação da Informação**".

III - Os colaboradores são responsabilizados por todas as ações realizadas mediante os logins e senhas que lhes são atribuídos.

IV - As senhas de acesso são alteradas em intervalos:

a) Inferiores trinta dias, não sendo permitida a utilização das últimas cinco senhas válidas, no caso de senhas da operação
b) Inferiores a trinta dias, não sendo permitida a utilização das últimas dez senhas válidas no caso de usuários de áreas administrativas (recursos humanos, ti, terceiros, etc) e super. usuários (administradores de rede)

V – É mandatório que as senhas de acesso sejam compostas da seguinte forma:

a) Tenham um comprimento mínimo de 12 caracteres
b) Pelo menos uma letra maiúscula;
c) Pelo menos um número;
d) Um caractere especial (!@#$%¨&*()"+)

VI - Não é permitido na composição de senhas padrão do tipo: nvtelecom2024, nvtelecom1234, nvtelecomteste. Essas senhas somente são permitidas no acesso inicial do colaborador (a), obrigatoriamente sendo trocadas imediatamente no primeiro acesso (TODOS os sistemas necessitam exibir mensagens para que a senha seja obrigatoriamente trocada).

VII – Não é recomendado na composição de senhas: placas de carro, datas de nascimento, aniversário, parte do seu nome, RG, CPF, rua etc.

VIII - Os parâmetros de senhas para servidores e ambiente críticos seguem as mesmas premissas com exceção do item 1, onde o comprimento da senha passa a ser de 20 caracteres no mínimo.

5.9.6 Computação Móvel e Trabalho Remoto (VPN)

I - O acesso remoto às informações da **New Voice Telecom** traz um risco significativo ao ambiente corporativo. Para mitigar tais riscos com viés preventivo e não corretivo, são mandatórios os seguintes controles:

a) Autenticação por 2 fatores (2FA)
b) Controle de logs da VPN,
c) Canal de comunicação seguro através de criptografia,
d) Acesso restrito a pastas e ambientes específicos,
e) Revisão de acesso periódico (três meses) aos colaboradores da área de TI que possuem acesso permanente.

II - O acesso remoto através de VPN deverá ser formalizado e justificado através de:

- Abertura de chamado.
- Aprovação do diretor da área.
- Aprovação pela Gerência de Segurança da Informação.

III - Acesso remoto de fornecedores, prestadores de serviço somente são permitidos quando justificados e formalizados através dos passos descritos no item **II**. Para efeitos de justificativa de acesso são considerados:

- Configurações, parametrizações, customizações necessárias,
- Testes e homologações de produtos,
- Participação em procedimentos inseridos em alguma mudança previamente aberta.

IV - Fornecedores e prestadores de serviço não podem ter acesso permanente ao ambiente interno da **New Voice Telecom**. Acessos ao ambiente por conta das atividades citadas no item **III** serão concedidos e revogados depois de concluídas as atividades.

5.9.7 Sincronização dos Relógios

Os relógios de todos os ativos críticos da **New Voice Telecom** que suportam os processos de negócios são sincronizados com fontes de tempo precisas. Dessa forma essa sincronização, com fontes de tempo confiáveis dos relógios dos computadores e outros equipamentos interligados à Internet, é essencial para:

- o correto funcionamento de sistemas e redes;
- o apoio a processos de detecção de incidentes de segurança e seu tratamento adequado, permitindo a correlação de eventos;

- a documentação e preservação de evidências que possam vir a ser utilizadas em investigações de crimes de informática.

Adicionalmente, de acordo com o **Comitê Gestor da Internet no Brasil (CGI.BR)** recomenda-se:

- Sincronizar, com a Hora Legal Brasileira, todos os dispositivos de rede e servidores conectados à Internet no Brasil, de forma continuada, utilizando-se de programas de computador apropriados e fontes de tempo confiáveis;
- Sempre que possível e apropriado, sincronizar, com a Hora legal Brasileira, estações de trabalho conectadas à Internet no Brasil, de forma continuada, utilizando-se de programas de computador apropriados e fontes de tempo confiáveis;
- Estabelecer procedimentos de ajuste do tempo ao fuso horário local e ao horário de verão, quando necessários;
- Gerar registro de eventos (logs) pertinentes, de forma a manter informações inequívocas sobre o fuso horário em que se deu um evento;
- Utilizar, preferencialmente, o protocolo NTP (Network Time Protocol), conforme padrões de referência e instruções presentes na página Web do Projeto NTP do NIC.br - http://ntp.br;
- Utilizar, preferencialmente, os servidores de tempo implantados pelo NIC.br, através do projeto NTP.br, como referências de tempo, conforme instruções e recomendações presentes em sua página Web - http://ntp.br

Tabela de Servidores NTP.br:

Servidor:	**Endereço:**
a.st1.ntp.br	200.160.7.186 e 2001:12ff:0:7::186
b.st1.ntp.br	201.49.148.135
c.st1.ntp.br	200.186.125.195
d.st1.ntp.br	200.20.186.76
a.ntp.br	200.160.0.8 e 2001:12ff::8
b.ntp.br	200.189.40.8
c.ntp.br	200.192.232.8
gps.ntp.br	200.160.7.193 e 2001:12ff:0:7::193

6. Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação

6.1 Processo de Hardening (Estações. Servidores e Dispositivos)

I – É necessário que um processo de hardening de estações e servidores seja adotado antes da entrada em produção desses ativos. Em relação às estações de trabalho, independente do "domínio" pertencer ao cliente, é mandatório que seja aplicado o check list: "**Processo de hardening das estações"** que contempla, mas não se limita as seguintes regras:

a) Desabilitar USB
b) Prompt do comando do DOS
c) Acesso a BIOS das estações
d) Acesso ao REGEDIT

II - Adicionalmente é obrigatório que seja adotado processo equivalente para servidores, demais dispositivos de redes e celular corporativo antes da entrada em produção ou disponibilização, onde serviços, processos, aplicativos e devices não necessários sejam desabilitados.

III - A área de suporte responsável por configurar esses dispositivos necessita também:

a) Alterar senha padrão de acordo com o estabelecido no item 5.9.5 – Política de Senhas

Após aplicar processo de hardening, será aberto chamado junto à ferramenta de controle de chamados para que seja aplicado o processo de gestão de vulnerabilidades nos servidores.

IV - Todos os servidores deverão forçar a desconexão das sessões de usuário, quando de sua inatividade, evitando o desperdício de recursos computacionais e garantindo a proteção dos servidores:

b) O período de inatividade pode variar de acordo com a necessidade fim do serviço acessado no servidor

6.2 Gestão de Vulnerabilidades

I - Dispositivos e aplicações que entrarem em produção necessitam obrigatoriamente passar por processo de scan de vulnerabilidades, seja de escopo infraestrutura ou sistêmico (DAST/SAST) formalizado através de:

a) RDM - Requisição de mudança
b) CAB - Comitê executivo de mudança
c) Aprovação da mudança
d) Aplicação das correções recomendadas

e) Retest

II – É necessário o estabelecimento de um cronograma mensal de correção das vulnerabilidades encontradas e adicionalmente a necessidade de haver alinhamento envolvendo as áreas de negócio afetadas e a área de TI.

III - Nenhum dispositivo ou aplicação pode entrar em produção antes de processo de hardening e gestão de vulnerabilidades. É mandatório que esse controle seja realizado através de termo de aceite das áreas envolvidas, além de chamado e requisição de mudança (RDM) formalizada.

IV – As vulnerabilidades críticas identificadas, deverão ser corrigidas com prioridade conforme definido no processo denominado Gestão de Vulnerabilidades, bem como planos de ação formalizados e documentados para as demais categorias de vulnerabilidades (Chamado aberto, Mudanças abertas, etc) a cada três meses.

7. Continuidade de Negócios e Recuperação de Desastres

I - É mandatório que todos os processos críticos de negócio da **New Voice Telecom** tenham contingência para que em caso de indisponibilidades sejam elas naturais, acidentais ou intencionais não haja impacto nos negócios da empresa e dos nossos clientes. Para contemplar esse requisito em sua totalidade, uma política específica denominada **Política de Continuidade de Negócios** contém as principais diretrizes a respeito.

II - São considerados críticos para a organização primeiramente as operações de nossos clientes, área de TI e administrativo. Dessa forma, torna-se necessária a documentadas em detalhe, opções de continuidade e recuperação de desastres, onde não haja impacto significativo no ambiente.

III – É necessário que seja estabelecida matriz de risco interativa onde seja possível identificar os processos críticos e os ativos de TI que suportam esses processos. Também é mandatório que sejam identificados os gestores de negócio responsáveis e equipe de TI, juntamente com árvore de escalonamento contendo: **Nome, endereço, telefone móvel, telefone celular, telefone de recado, e-mail corporativo e e-mail pessoal para efeitos de acionamento.**

IV - Testes dos planos de continuidade e recuperação necessitam ser estabelecidos periodicamente (A cada seis meses) a fim de verificar eventuais falhas, melhorias e em linha com requisitos de nossos clientes.

V - Auditorias serão realizadas a fim de verificar os resultados dos testes e dessa forma propor melhorias e ações de conformidade.

8. Sanções Previstas

I - O descumprimento das normas previstas neste instrumento é passível de sanções administrativas, conforme regimento interno do departamento de Recursos Humanos da **New Voice Telecom**, e legais, conforme legislação vigente.

9. Disposições Finais

I - A Gerência de Segurança da Informação divulgará este documento de forma a conscientizar os colaboradores sobre a importância do tema para o desempenho de suas atividades profissionais.

II - A Gerência de Segurança da Informação realizará avaliações periódicas, a fim de verificar a conformidade dos ambientes da empresa com a Política Corporativa de Segurança da Informação, objetivando adequar tais ambientes às normas estabelecidas pela empresa.

III - Todas as exceções às diretrizes apresentadas na Política de Segurança da Informação necessitam ser tratadas pela Gerência de Segurança da Informação em conjunto com o comitê de Segurança da Informação da **New Voice Telecom**.

10. Atualizações

A presente **Política Corporativa de Segurança da Informação** será revisada sempre que:

- Houver alguma alteração relevante nos processos de negócio dos nossos clientes
- Diretrizes regulatórias
- Ou a cada 12 meses

11. Dúvidas e Esclarecimentos

Enviar e-mail para: seguranca.informacao@nvtelecom.com.br