Política de Segurança da Informação

Netbr

Política de Segurança da Informação

ÍNDICE

OBJETIVO

Estabelecer as diretrizes e orientações necessárias para proteção dos ativos de informação da NetBr em suas diversas formas, de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes, visando preservar o valor e a integridade da organização bem como salvaguardar a confidencialidade, integridade e disponibilidade das informações da companhia e de seus clientes e parceiros.

1. ABRANGÊNCIA

Aplica-se, independentemente de suas atribuições e responsabilidades, a todos os colaboradores da NetBr.

2. DOCUMENTAÇÃO COMPLEMENTAR

ABNT NBR ISO 22301 – Sistema de Gestão de Continuidade de Negócios
ABNT NBR ISO 27001 – Sistema de Gestão da Segurança da Informação
ABNT NBR ISO 27002 – Código de Prática para Controles de Segurança da Informação

3. CONCEITOS E SIGLAS

Ativo: Qualquer coisa, tangível ou intangível, que tenha valor para a organização.

Ativos de Informação: É o recurso físico ou lógico utilizado no armazenamento e manuseio da informação, por exemplo: documentos em papel, computadores, base de dados, dentre outros.

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

Continuidade de Negócios: Processo que visa garantir que os serviços essenciais de uma empresa sejam devidamente identificados, priorizados e documentados, para manter a empresa operacional, com o menor impacto possível aos clientes, mesmo após um desastre, até o retorno à situação normal.

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

Informação: É qualquer conteúdo ou dado que tenha valor para a organização.

Integridade: Neste contexto, trata-se da propriedade de salvaguarda da exatidão e completeza de ativos.

Mesa de Crise: Grupo de pessoas que são acionadas para analisar e tomar decisões em situações de crises.

Rede Corporativa: Ambiente de tecnologia local (infraestrutura e sistemas), acessível nos escritórios e remotamente via VPN - *Virtual Private Network* (Rede Privada Virtual), para uso dos colaboradores NetBr.

Rede *Guest*: Ambiente de infraestrutura tecnológica local com acesso somente a *Internet*, destinado a visitantes e colaboradores para uso de equipamentos pessoais.

Segurança física: Trata-se da proteção do ambiente tangível, composta por equipamentos biométricos, câmeras e portas.

Segurança lógica: Trata-se da proteção do ambiente intangível, composta por *softwares*, sistemas ou aplicações.

SI: Sigla que designa Segurança da Informação.

TI: Sigla que designa Tecnologia da Informação.

4. DISPOSIÇÕES GERAIS

A informação é um dos ativos fundamentais aos negócios da NetBr e a companhia tem a responsabilidade de mantê-los protegidos contra quaisquer ameaças que possam colocar em risco a integridade, disponibilidade e confidencialidade desses ativos.

Os ativos devem ser protegidos de acordo com sua sensibilidade, valor e criticidade conforme disposições de documento específico. Todas as medidas viáveis de segurança da informação devem ser aplicadas independentemente dos meios em que a informação seja armazenada, processada ou transmitida. Toda informação colocada à disposição dos colaboradores deve ser utilizada apenas para as finalidades de trabalho para a NetBr.

Os colaboradores devem fazer a proteção adequada da informação, realizar periodicamente avaliações de riscos das informações que manuseiam conforme disposições desta Política, atuar prontamente para reduzir a exposição de seus ativos na ocorrência de incidentes de segurança, monitorar a violação da Política de Segurança da Informação e a

confidencialidade, integridade e disponibilidade das informações para nossos clientes, colaboradores e demais partes relacionadas.

Os colaboradores devem ser conscientizados e ter disponível material de referência que possibilite identificar qual a proteção apropriada para os ativos da informação sob sua responsabilidade.

Os treinamentos e documentações sobre a segurança da informação são de responsabilidade da área de Segurança da Informação e seu conteúdo deve expressar que a segurança da informação é parte importante dos objetivos de negócios da NetBr.

Os colaboradores devem ter conhecimento desta Política e participar de todas as iniciativas de conscientização em relação às boas práticas de Segurança da Informação.

Todas as informações geradas e desenvolvidas são consideradas ativos de informação e intelectual da NetBr.

Os ativos de informação podem estar presentes em diversas formas, tais como: arquivos em diretórios de rede, equipamentos, mídias externas, documentos impressos, sistemas, dispositivos móveis, banco de dados e diálogos.

Independentemente da forma apresentada, compartilhada e/ou armazenada, a informação deve ser utilizada apenas para a sua finalidade, tendo sido devidamente autorizada e estando sujeita a monitoração e auditoria.
Todo o ativo de informação de propriedade da NetBr deve ter um responsável, ser devidamente classificado e adequadamente protegido de qualquer risco e/ou ameaças que possam comprometer o negócio.

4.1. **Papéis e Responsabilidades**

4.1.1. **Segurança da Informação**

- Definir o plano de estratégia geral da Segurança da Informação;
- Gerenciar a Mesa de Crise em caso de incidentes de segurança da informação;
- Definir as diretrizes de Segurança da Informação física, lógica e de Continuidade de Negócios;
- Planejar e participar das atividades do Comitê de Segurança da Informação, intermediando as interações com entidades internas ou externas em assuntos relacionados à Segurança da Informação;
- Viabilizar e nortear o colaborador nas boas práticas de Segurança da Informação;
- Definir as principais responsabilidades quanto à Segurança da Informação;

- Acompanhar a evolução do plano de ação para tratamento das vulnerabilidades e ameaças digitais sob responsabilidade das demais áreas;
- Promover campanhas de conscientização para os colaboradores em relação às boas práticas de Segurança da Informação, treinamento obrigatório de Segurança da Informação para os novos colaboradores e treinamentos contínuos referentes ao tema;
- Divulgar semestralmente a lista atualizada de proprietários de informações e sistemas;
- Gerenciar os indicadores de segurança da informação, crises, incidentes e continuidade de negócios;
- Realizar a análise de conformidade de segurança da informação e de Continuidade de Negócios nas instalações da NetBr.

4.1.2. **Comitê de Segurança da Informação**

As responsabilidades do Comitê de Segurança da Informação incluem, mas não se limitam a:

- Estabelecer o plano estratégico de Segurança da Informação alinhado a necessidade do negócio;
- Entender e aplicar as atribuições definidas pela área de Segurança da Informação;
- Garantir que a Segurança da Informação seja parte dos processos e da cultura da empresa;
- Apoiar e viabilizar orçamento para as iniciativas de Segurança da Informação, visando à melhoria contínua das medidas de proteção e redução dos riscos;
- Apresentar os principais indicadores de segurança, crises, incidentes e continuidade de negócios.
- Coordenar a gestão dos incidentes relacionados à Segurança da Informação ou Incidentes Críticos.

O Comitê é composto pelos representantes das diretorias da empresa.

4.1.3. **Mesa de Crise**

O processo de gestão de crises deve tratar todas as crises da empresa. Caracteriza-se a crise quando a ocorrência de um evento afeta, no mínimo, duas áreas com impacto na disponibilidade dos serviços, financeiro ou imagem da empresa.

A responsabilidade da Segurança da Informação em Mesa de Crise inclui, mas não se limita a:

- Gerenciar todos os incidentes críticos e crises da empresa com impactos de confidencialidade, integridade, disponibilidade, danos à reputação da marca e possibilidade de perdas financeiras.

A mesa de crise é composta pelos representantes das diretorias da empresa.

4.2. **Propriedade Intelectual**

A propriedade intelectual é composta por bens imateriais de propriedade da NetBr, dentre as quais se incluem informações, patentes, direitos autorais, segredos comerciais, marcas registradas, especificações, desenhos, modelos, cronogramas, exemplos, ferramentas, programas de computador, base de dados, todas as informações produzidas, invenções, códigos de *software* ou melhorias decorrentes das atividades associadas ao trabalho durante o contrato do colaborador ou mesmo após seu término, por prazo indeterminado e outros direitos de propriedade intelectual da NetBr.

Os inventos, desenvolvimento ou aperfeiçoamento de *softwares*, sistemas ou outras melhorias feitas pelo colaborador, no exercício de suas atribuições, mesmo que fora do horário de trabalho e fora das dependências da NetBr, desde que relacionados com as atividades da empresa, devem ser comunicados à respectiva liderança.

Conforme estabelecido no Código de Conduta e Ética, todo colaborador é responsável pela preservação da propriedade intelectual da organização, bem como pela observância e respeito à propriedade intelectual de terceiros, nos termos da legislação vigente, cabendo à responsabilização em casos de omissão, dolo ou culpa.

Todas as informações e propriedade intelectual que pertençam à NetBr, ou por ela disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

Devem ser adotadas, pelas respectivas lideranças, todas as medidas cabíveis e legais para proteger a propriedade intelectual, por meio de controles internos e de registro nos órgãos competentes.

4.3. **Recursos Corporativos**

Todas as informações contidas ou criadas em dispositivos da NetBr ou autorizados para uso dos colaboradores são de propriedade da NetBr e constituem bens da empresa. Dispositivos que podem ser, mas não se limitam a computadores, *notebooks*, celulares, *tablets, pendrive* ou recursos na “nuvem” abrangendo *Internet* e *Intranet*, e-mails, repositórios de arquivos, dentre outros.

Não é permitido instalar e/ou executar produtos e/ou *softwares* considerados "piratas" ou gratuitos ("*freeware* e/ou *shareware*") e softwares não homologados nos computadores corporativos. A aquisição, instalação e execução de novos programas devem ser homologadas pela área de Tecnologia da Informação e aprovada pela área de Segurança da Informação. O produto deve estar acompanhado de licença legalmente adquirida, cedida ou autorizada para uso corporativo seguindo suas políticas de uso e privacidade. Caso seja efetuado o uso sem a devida avaliação, a NetBr poderá estar exposta a riscos de pirataria de *software* e sujeita às sanções e punições legais associadas ao uso indevido.
Se o colaborador vier a utilizar equipamento próprio deverá submeter-se às mesmas regras e políticas aqui definidas a fim de proteger os direitos da NetBr.
Os recursos corporativos devem ser utilizados com responsabilidade e exclusivamente para as atribuições relativas à NetBr, não sendo permitidos os acessos impróprios na *Internet,* incluindo, mas não se limitando a: jogos de azar, mensagens de corrente, troca ou armazenamento de conteúdo obsceno, pornográfico, violento, discriminatório, racista, político, religioso, difamatório ou que desrespeite qualquer indivíduo ou entidades), de acordo com as Leis nº 8.069 (Estatuto da Criança e do Adolescente) e nº 12.965 (Marco Civil da *Internet*).

Os colaboradores devem ter zelo pelos recursos corporativos, como computadores, impressoras, celulares e demais equipamentos que ele tenha acesso, podendo sofrer sanções administrativas conforme previsto no Código de Conduta e Ética.

A manutenção e configuração dos recursos físicos (computadores, *notebooks*, impressoras e celulares) e recursos eletrônicos (*softwares*) da NetBr são responsabilidade da área de Suporte em TI, sendo vedado aos demais colaboradores alterarem sua configuração, abrir o equipamento ou alterar componentes.

A NetBr se reserva o direito de monitorar e de inspecionar o uso dos recursos da empresa e/ou conectado à rede corporativa, que se utilize de informações corporativas – por exemplo: computadores, e-mails, acesso à *Internet*, conteúdos da marca na *Internet*, telefones corporativos e informações proprietárias – de acordo com a legislação aplicável e procedimentos internos definidos pela área de Segurança da Informação.

Ao se ausentar da estação de trabalho, sala de reunião ou outros ambientes, mesmo que por breve período, o colaborador deve proteger as informações contra acessos indevidos bloqueando seu computador utilizando a senha de bloqueio. Material impresso deve ser protegido e guardado em local seguro. Material impresso não utilizado deve ser destruído após o seu uso. Cuidados semelhantes se aplicam ao material impresso deixado nos escaninhos de impressoras.

É vedado utilizar qualquer tipo de conexão remota (telefônica, cabo, rede *wireless*, dentre outras) nos equipamentos que estejam ao mesmo tempo conectados nas redes locais da empresa.

Um equipamento conectado na rede corporativa da NetBr não pode se conectar à outra rede simultaneamente. Esta prática pode expor as informações da NetBr e/ou contaminar o ambiente corporativo com vírus.

Todos os incidentes corporativos que envolvam ameaças digitais, incluindo, mas não se limitando a vulnerabilidades, vírus de computador e ataques digitais diretos ou indiretos, devem ser reportados para a Segurança da Informação.

4.4. **Redes Sociais**

Todos os colaboradores devem ser conscientes com as informações publicadas. O colaborador que infringir alguma diretriz mencionada poderá sofrer punições ou sanções previstas no Código de Conduta e Ética e nesta Política de Segurança da Informação.

- Não fale em nome da NetBr, exceto se você possuir aprovação formal da área de Marketing, bem como da sua respectiva diretoria;
- Nunca publique informações internas ou confidenciais da NetBr;
- Nunca comente sobre assuntos relacionados à sua função na NetBr;
- Não critique ou faça comentários negativos da concorrência, clientes e parceiros da NetBr;
- Toda e qualquer opinião expressa em mídias sociais é de sua inteira responsabilidade;

4.5. **Continuidade do Negócio**

A gestão dos planos de continuidade deve garantir que os serviços essenciais da empresa sejam devidamente identificados, priorizados e documentados para manter a empresa operacional, sem grandes impactos aos clientes, mesmo após um desastre, até o retorno à situação normal, sempre alinhado às necessidades do negócio.

Para tanto, a área de Segurança da Informação é responsável por definir as diretrizes, estratégias e os planos de Continuidade de Negócios, conforme as melhores práticas requeridas pela ISO 22301 – Sistema de Gestão de Continuidade de Negócios.

4.6. **Gestão de Acesso e Senhas**

A gestão de usuários e acessos à rede corporativa, sistemas e equipamentos de infraestrutura é de responsabilidade da área de Segurança da Informação.

Usuários

As credenciais de acesso físico e lógico de colaboradores deverão ser revogadas imediatamente ao término do contrato de trabalho ou prestação de serviços.

Os usuários e senhas de acesso aos sistemas são pessoais e intransferíveis. O colaborador deverá zelar pelas suas credenciais e acessos, trocando a senha a cada 90 (noventa) dias ou quando suspeitar que possa ter sido comprometida, utilizando Múltiplo Fator de Autenticação sempre que o sistema possibilitar.

É de responsabilidade do usuário qualquer ação executada através de sua conta de acesso.

Os usuários e perfis de acessos aos sistemas NetBr e terceirizados deverão ser revisados semestralmente pelos gestores ou pontualmente por iniciativa da área de Segurança da Informação.

Contas impessoais devem ter o mesmo tratamento de contas pessoais e definição de responsável.

Acessos

As solicitações de acessos devem ser formalizadas e serão atendidas após validação dos gestores, que devem verificar se os acessos são compatíveis com as funções e responsabilidades do colaborador.

O colaborador e demais usuários autorizados devem ter acesso somente às informações e recursos que se façam necessários para a realização de suas atividades na NetBr, devendo ser respeitada a segregação de funções.

Na revisão de acessos, todos os acessos concedidos que não sejam necessários para o colaborador desempenhar suas atividades na NetBr, conforme determinação do Gestor do Sistema, devem ser removidos e comunicados à Segurança da Informação.

Acessos privilegiados e/ou administrativos devem ter sua concessão autorizada pelo Gestor do Sistema em conjunto

com o Gestor Imediato do colaborador solicitante.

Constitui-se grave violação da Política de Segurança da Informação ter acesso às informações não autorizadas, tentar ou conseguir acesso a qualquer serviço ou informação sem a devida autorização, tentar ou burlar as restrições de segurança, tentar ou prejudicar serviços da NetBr, tentar ou interceptar comunicação de forma não autorizada ou utilizar os recursos da NetBr para atividades não condizentes com as suas atribuições profissionais.

Senhas

A senha é pessoal e intransferível, devendo obedecer aos padrões da NetBr.

É responsabilidade do usuário qualquer ação executada com o seu usuário e senha, constituindo-se grave violação da Política de Segurança da Informação, realizar o compartilhamento.

Algumas orientações devem ser observadas para elaboração e manutenção da senha:

- O usuário não deve armazenar senha em arquivos digitais sem criptografia, e-mails, papéis ou outras mídias. É recomendado memorizar sua senha;
- Não se deve utilizar senhas consideradas “fracas”, como as baseadas em nomes próprios ou dados pessoais, tais como: nomes, datas, RG, CPF, dentre outras.
- A senha deve ser composta por, no mínimo, 12 caracteres respeitando as quatro regras abaixo:
  - Letra maiúscula;
  - Letra minúscula;
  - Um número;
  - Um carácter especial (!@#$%&*()”).

4.7. **Proprietário da Informação**

As informações devem possuir um proprietário, que é responsável por efetuar a classificação, aprovação e revisão das informações periodicamente.

O proprietário é responsável pela definição formal do seu substituto para efetuar as atividades na sua ausência.

Caso haja alguma informação que não tenha um proprietário formal, o gestor da área que gera a informação será designado como proprietário da informação.

É de sua responsabilidade, também, definir os prazos de cópia de segurança e descarte das informações, observando os prazos legais.

4.8. **Gestor do Sistema**

É responsável por demandar e controlar as melhorias nos sistemas, bem como prover os investimentos necessários.

Garantir que os acessos ao sistema seja atribuído apenas para usuários necessários.

4.9. **Classificação da Informação**

É um processo importante que visa proteger a informação estabelecendo uma classificação mediante a relevância da informação, relacionada ao manuseio, criação, rotulagem, armazenamento, transporte e descarte da informação.

Neste contexto, é importante ter ciência que documentos como contratos, registros financeiros, comerciais, relatórios internos de qualquer natureza, planos e projetos, dentre outros, contém informações que são de propriedade da NetBr.

Documentos produzidos pela e para a NetBr não devem ser publicados, a não ser que devidamente autorizados para este fim.

A Norma de Classificação da Informação estabelece como as informações da NetBr são classificadas.

A tabela a seguir deve ser utilizada como base para classificar a informação:

	PÚBLICA	**INTERNA**	**CONFIDENCIAL**
A QUEM se destina?	Todos dentro e fora da empresa podem ter acesso às informações.	Somente colaboradores e terceiros de empresas prestadoras autorizadas podem ter acesso.	Somente os destinatários do conteúdo podem acessá-las.
O QUE é?	Tipo de informação em que não há problema em levar ou chegar ao mercado ou ao concorrente.	Toda informação obtida por/com resultado do desempenho de atividades na empresa é no mínimo informação interna.	Em geral, se trata de informação utilizada por grupos restritos, caso contrário a confidencialidade fica comprometida, qualquer dados referente a clientes.
QUEM pode Classificar?	Diretorias da Netbr	Qualquer colaborador.	Qualquer colaborador.

Informações Confidenciais

Informações confidenciais devem ser armazenadas com controle de acessos somente aos colaboradores autorizados e somente durante o tempo em que valer a confidencialidade.

Após o prazo da confidencialidade a informação deve ser corretamente descartada.

Toda informação não classificada deve ser tratada como interna.

É considerada grave violação da Política de Segurança da Informação a troca de informações confidenciais com áreas distintas, empresas e membros das áreas que não devem ter o conhecimento da informação confidencial e ou privilegiada.

Os colaboradores que observarem atitudes suspeitas ou desvios desta Política devem reportar à área de Segurança da Informação.

4.9.1. **Integridade das Informações**

As informações da NetBr devem ser corretas, completas, mantidas e descartadas de acordo com os prazos legais e internos.

É de responsabilidade da área de Tecnologia da Informação efetuar as cópias de segurança conforme os prazos definidos pelo proprietário da informação.

4.9.2. **Manutenção da Informação**

Todas as informações da NetBr devem ser armazenadas na nuvem privada oficial da empresa.

É vedado armazenar e transferir informações ou dados para dispositivos e ou meios de armazenamento externos, incluindo, mas não se limitando a: Unidades USB (*Pendrivers*, *Flashdrivers,* dentre outros), HDs externos, *chats* e ambientes de armazenamento em nuvem (*Dropbox*, *OneDrive*, *iCloud*, *Google Drive.* dentre outros).

Processo de expurgo: O processo de expurgo consistente na eliminação dos dados relativos a clientes e projetos ao final da implementação de uma solução interna ou externa. Isso pode incluir o uso de ferramentas de software para automatizar o processo, essa atribuição é de responsabilidade da área de TI.

4.10. **Mesa Limpa**

O programa de mesa limpa visa evitar a exposição desnecessária de informações da empresa, seguindo as seguintes orientações:

- Não devem ser deixados documentos impressos sobre a mesa, nem lembretes (principalmente com senhas) nos monitores e teclados;
- Os documentos impressos e dispositivos externos devem ser guardados em local seguro;
- As informações dos quadros sempre devem ser apagadas antes de deixar a sala de reunião. Se houver informações em papel, o descarte deve ser realizado utilizando as picotadoras de papel.

4.11. **Uso de *Internet* e Correio Eletrônico**

É vedado o acesso de conteúdo de entretenimento que porventura não seja relacionado às atividades do colaborador.

É vedado utilizar o correio eletrônico corporativo (e-mail) para fins pessoais como, por exemplo: cadastro em sites de compras, mídias sociais, dentre outros.

Os acessos são monitorados e poderão ser bloqueados sem aviso prévio.

Aviso Legal e Assinatura do Correio Eletrônico

Deve ser utilizado o aviso legal oficial da empresa (*disclaimer*) de e-mail ao enviar mensagens, além disso:

- Todos os colaboradores devem configurar sua assinatura no e-mail corporativo conforme o padrão mais atual da empresa;
- Todas as mensagens de e-mail devem ser classificadas como confidencial, interna ou Pública, seguindo as regras de classificação da informação.

4.12. **Uso de dispositivos móveis**

Os dispositivos móveis com acesso a dados da organização devem seguir, além das demais diretrizes desse documento, as abaixo:

- Utilizar o sistema anti-malware corporativo.
- Informar TI em casos de perda, roubo ou extravio do dispositivo móvel. Nessas situações, a equipe de Tecnologia da Informação irá proceder imediatamente com o *reset* do dispositivo móvel.
- Não armazenar dados corporativos ou de clientes no dispositivo móvel.

4.13. **Terceiros e Prestadores de Serviço**

Ao realizar a contratação de terceiros ou prestadores de serviços, a área contratante deverá ser responsável por definir previamente, em conjunto com o Gestor do Contrato e do Sistema, qual o nível de acesso necessário às informações para desempenho das atividades, bem como os controles a serem adotados para monitoramento da utilização.

Os controles de acesso devem ser concedidos mantidos e revogados da mesma maneira que é realizada para um colaborador Netbr e revisados periodicamente.

4.14. **Segurança Física**

Escritórios

É vedado fotografar ou filmar as instalações da NetBr, exceto o espaço reservado para convivência, salvo no caso de exceções previamente autorizadas.

Todo e qualquer acesso deve ser feito por portas com controle de acesso eletrônico. As portas de combate a incêndio devem ser mantidas fechadas.

A abertura das portas de incêndio só pode ser realizada em situação de emergência ou devidamente autorizada pela Brigada de Incêndio.

Câmeras de Segurança

Os ambientes da NetBr são monitorados por câmeras de segurança e as gravações devem ser armazenadas por 30 (trinta) dias para fins de consulta e manter cópias de segurança.

Nota: As consultas somente poderão ser realizadas mediante a aprovação da área de Segurança da Informação.

Uso de Crachá

O crachá é a identificação do colaborador no ambiente corporativo, portanto, é necessário que cumpra as seguintes regras:

- Cuide do seu crachá e nunca o deixe exposto em locais públicos;
- Em caso de esquecimento, perda ou extravio, comunique imediatamente a equipe de Recursos Humanos;

Estações de Trabalho

Para computadores, em casos de locomoção para outros locais, o computador deve ser transportado de forma discreta, em mochila apropriada e sempre no porta-malas dos veículos, além disso:

- Ao se ausentar da sua estação de trabalho, faça o bloqueio de seu computador utilizando Ctrl + Alt + Del ou ⊞ + L;
- Equipamentos da NetBr devem ser utilizados exclusivamente para assuntos profissionais relacionados à NetBr;

- Exceções somente serão permitidas mediante liberação realizada pela área de *Suporte* de TI.

4.15. **Segurança em Tecnologia da Informação**

A área de Tecnologia da Informação deve cumprir as diretrizes desta Política visando proteger os ambientes digitais da NetBr, sendo responsável pela implantação de soluções tecnológicas e de segurança.

Gestão de Acessos

- Pela Gestão de Acessos de usuários;
  - Os acessos de colaboradores desligados devem ser bloqueados imediatamente e os dados armazenados no correio eletrônico e servidor de arquivos serão mantidos em cópia de segurança por 5 anos, durante este período o gestor imediato pode solicitar acesso a estes dados com a aprovação do responsável pela área de Segurança da Informação.
- Pela Gestão de Acessos a usuários de bancos de dados e sistemas.

Nota: Os acessos devem ser revisados semestralmente, sempre que houver alterações significativas ou por solicitação pontual da área de Segurança da Informação.

Segurança de Perímetro

O Suporte de TI da NetBr deve manter o ambiente tecnológico protegido e monitorado.

A topologia de redes deve estar sempre atualizada e disponível para a área de Segurança da Informação.

Testes de Segurança

Todos os sistemas devem ser submetidos a testes de segurança antes de sua implantação, quando houver alterações significativas ou por demanda. Estes testes de segurança devem englobar varredura de vulnerabilidades, tentativas de intrusão, análise de código e outras técnicas.

Gestão de Vulnerabilidades e Correções (*Patches*)

Deve ser contemplado um procedimento de atualização periódica, preferencialmente mensal, e sempre que houver vulnerabilidades críticas nos servidores, estações de trabalho e infraestrutura.

Proteção de Máquinas

O sistema operacional dos equipamentos destinados ao uso dos colaboradores deve ser atualizado, e podem ser monitorados por TI, mantendo sempre as atualizações de segurança mais recentes.

Hardening

Hardening é a configuração para reforçar a segurança tecnológica evitando a exploração de vulnerabilidades. Deve haver um processo de *hardening* para servidores e demais equipamentos de infraestrutura.

Monitoramento

O ambiente tecnológico NetBr deve ser monitorado a fim de salvaguardar seus colaboradores e a própria empresa.

A NetBr se reserva ao direito de monitorar e interceptar o tráfego de redes comum e criptografado oriundos de quaisquer conexões pertencentes à empresa.

Proteção contra ameaças digitais

Todos os servidores, estações de trabalho e *gateways* de e-mail devem possuir mecanismos de segurança, sempre ativos e atualizados, como por exemplo antivírus e outros.

Criptografia

A área de TI é responsável por gerenciar os certificados digitais, chaves e algoritmos criptográficos, criptografias de disco e de conexão.

Estação de trabalho

Deve haver um processo de criptografia de disco em todos os *computadores*, para proteger a confidencialidade e integridade das informações da NetBr em todos os sistemas que armazenem informações.

Descarte de equipamentos e mídias

Deve haver um processo para destruir definitivamente as informações dos equipamentos e mídias após o mesmo deixar

de ser utilizado, houver alteração de uso e responsáveis ou antes de ser descartado.

Redes

As informações confidenciais armazenadas em repositórios e todos os dados trafegados nas redes da empresa devem ser criptografadas, bem como todas as conexões de *Internet* de parceiros e fornecedores.

Repositório de Informações

A área de TI deve disponibilizar infraestrutura e espaço adequado para que todos os colaboradores armazenem as informações da NetBr nos repositórios com as devidas proteções e segregações de acesso.

Plano de *Backup* – Cópias de Segurança

Deve haver plano de *backup* para efetuar a cópia de segurança de todas as informações armazenadas nos servidores NetBr. O plano deve ser validado pelos proprietários da informação com base legal e regulatória, contemplando no mínimo:

- Periodicidade dos b*ackups*;
- Prazo de retenção;
- Informações contempladas na cópia de segurança;
- Testes aleatórios de recuperação dos *backups*;
- Guarda em local externo;
- Tipo de *backup*: completo, incremental, dentre outros.

Desenvolvimento dos Sistemas

Todo sistema deve possuir Controle de Acesso de modo a assegurar o uso apenas por usuário autorizado. Os sistemas críticos devem permitir o registro de trilhas de auditoria, conforme a Lei N° 12.965/14 do Marco Civil da Internet, que possibilite o rastreamento e monitoramento das atividades executadas, com ressalvas para os sistemas legados onde deve ser aplicado um plano de mitigação a fim de garantir o controle sistêmico.

Os sistemas devem possuir autenticação, autorização e gestão de acessos e seguir as melhores práticas de mercado, como exemplo a NBR27001 e NBR27002.

O desenvolvimento de sistema seguro visa proteger a empresa de utilizar sistemas com códigos passíveis à exploração de vulnerabilidades e códigos maliciosos, podendo gerar riscos adicionais para a operação da NetBr.

Os ambientes de homologação de produção devem ser segregados. Os dados de produção utilizados para testes devem ser descaracterizados de forma que não identifique a informação original.

Confidencialidade do Monitoramento

Toda informação identificada no monitoramento é confidencial e só pode ser utilizada pelas pessoas autorizadas com o objetivo de tratamento de incidentes e erros, análise de desempenho e demais funcionalidades inerentes de TI, sendo vedado o uso para outras finalidades.

A identificação de informações pessoais de colaboradores no monitoramento não deve ser utilizada, exceto por solicitação das áreas de Segurança da Informação, Auditoria ou *Compliance*.

A violação deste item é passível de sanções administrativas e legais conforme previsto no Código de Conduta e Ética e legislação vigente.

Inventário para Ativos de TI

A área de Tecnologia da Informação é responsável por documentar e inventariar todos os *hardwares* e *softwares* de tecnologia da informação.

Indicadores de Segurança da Informação

A área de Tecnologia da Informação é responsável por disponibilizar todas as informações referentes aos indicadores de segurança dos sistemas e da infraestrutura para a área de Segurança da Informação.

Continuidade – Recuperação de Desastres em TI (*Disaster Recovery*)

A área de Tecnologia da Informação é responsável por elaborar, testar e manter os planos para recuperação do ambiente de tecnologia da NetBr atualizados, sempre alinhado às necessidades do negócio.

Ativos tecnológicos públicos

A área de Tecnologia da Informação é responsável por manter inventariado todos os ativos públicos de tecnologia, que contempla domínios e endereçamentos de servidores.

4.16. **Aderência a esta Política**

Todos os colaboradores e respectivas áreas devem se adequar a esta Política no prazo de até 180 (cento e oitenta) dias a partir da data de publicação.

5. **RESPONSABILIDADES**

RESPONSÁVEL	ATIVIDADE	PERIODICIDADE
Proprietário da Informação	Classificar a informação de acordo com a Política de Segurança da Informação.	Semestralmente
	Aprovar e revisar os acessos.	Semestralmente
Proprietário do Sistema	Responsável pelas demandas referentes aos sistemas em TI – Desenvolvimento e definição das rotinas de *backup* dos sistemas.	Não aplicável
	Aprovar e revisar os acessos.	Semestralmente
Segurança da Informação	Manter e revisar a Política de Segurança da Informação, bem como realizar atualizações.	Sempre que necessário
	Manter a Política de Gestão de Continuidade de Negócios atualizada.	De acordo com o prazo do normativo
	Manter os planos de Gestão de Continuidade de Negócios atualizados.	De acordo com o prazo dos planos
Tecnologia da Informação	Realizar testes periodicamente.	Anualmente
	Realizar a revisão da gestão de acessos tecnológicos.	Trimestralmente
	Elaborar, revisar e testar o Plano de Recuperação de Desastres de TI.	Anualmente

6. HISTÓRICO DAS REVISÕES

PÁGINA	VERSÃO	DATA DA EMISSÃO	MOTIVO DAS ALTERAÇÕES	SOLICITADA POR