

Política Pública de Segurança da Informação

Sumário

1 Objetivo	3
2 Campo Aplicação	3
3 Glossário	3
4 Introdução	5
5 Diretrizes	5
5.1 Diretrizes Gerais	5
5.2 Segurança da Informação no Negócio	6
5.2.1 Gestão de Riscos de Tecnologia e Segurança da Informação	6
5.2.2 Gestão de Segurança em Fornecedores	6
5.2.3 Conscientização de Segurança da Informação para Recursos Humanos	7
5.2.4 Gestão de Classificação da Informação	7
5.2.5 Gestão de Aquisição, Desenvolvimento e Manutenção de Sistemas	7
5.2.6 Gestão de Controle de Acesso Lógico e Físico	7
5.2.7 Gestão de Incidentes de Segurança da Informação	8
5.2.8 Gestão de Uso de Recursos Tecnológicos	8
5.2.9 Gestão de Vulnerabilidade e Patches	8
5.2.10 Gestão de Teste de Intrusão	9
5.2.11 Gerenciamento de Crise	9
5.2.12 Continuidade de Negócios	9
6 Penalidades	10
7 Responsabilidades	10
8 Referências	14
9 Canal de Comunicação de Segurança da Informação	14

1 Objetivo

Para que a Segurança da Informação seja completamente eficaz, a Rede Américas implementou uma série de controles compostos por políticas, práticas, procedimentos, estruturas organizacionais e tecnologia.

Este documento lista os principais controles utilizados pela Rede Américas para atender às necessidades de segurança da informação e cibernética, mitigando as vulnerabilidades e incidentes.

2 Campo Aplicação

É aplicável a todos os colaboradores, prestadores de serviço e parceiros da Rede Américas.

3 Glossário

Termo	Definição
Ambiente de Produção	Ambiente operacional voltado para implementar um sistema e ser utilizado por usuários finais para executar suas tarefas do dia a dia.
Ameaça	Qualquer circunstância ou evento com potencial de impactar negativamente as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais ou indivíduos através de um sistema de informação por meio de acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço.
Análise de Impacto no negócio (Business Impact Analysis)	Processo de análise das funções operacionais e do efeito que uma perturbação pode ter sobre elas.
Ativos Tecnológicos	Um item de valor para as partes interessadas. Um ativo pode ser (por exemplo, um item físico, como hardware, firmware, plataforma de computação, dispositivo de rede ou outro componente tecnológico).
Backup	Cópia de Segurança de Dados, de um dispositivo de armazenamento para outro, para que possa ser restaurado em caso da perda dos dados originais.
Baseline	Controles de segurança mínimas necessários para proteger um sistema de TI com base nas necessidades identificadas de proteção de confidencialidade, integridade e/ou disponibilidade.
Centro de Defesa e Operações Cibernéticas	Equipe Rede Américas responsável por monitorar e tratar os incidentes e eventos relacionados ao tema de Segurança da Informação.
Colaborador	Pessoa que compõe o quadro de funcionários da Rede Américas.

Concessão de Acessos	Processo de atribuir acesso a um novo e/ou existente colaborador da empresa.
Continuidade de Negócios	Capacidade da empresa de continuar a entrega de produtos ou serviços em um nível aceitável previamente definido após incidentes de interrupção.
Credencial de Acesso	Um objeto ou estrutura de dados que vincula com autoridade uma identidade (e opcionalmente, atributos adicionais) a um token processado e controlado por um Assinante.
Crise	Qualquer evento que ameaça a integridade das pessoas, que gere alto impacto para o negócio e/ou reputação da empresa.
Desastre	Eventos adversos que causam grandes impactos nas operações, reputação e imagem da empresa.
Eventos	Qualquer ocorrência observável em uma rede ou sistema de informação.
Fornecedor	Fornecedor, também chamado de Provedor, consiste na organização e/ou empresa que provê um produto ou serviço.
Incidente	Situação que pode representar ou levar à interrupção de negócios, perdas, emergências e crises.
Infraestrutura	Sistema de instalações, equipamentos e serviços necessários para a operação de uma organização.
Log	Expressão utilizada para descrever o processo de registro de eventos em um sistema computacional.
Matriz de Acesso	Uma tabela na qual cada linha representa um assunto, cada coluna representa um objeto e cada entrada é o conjunto de direitos de acesso desse sujeito a esse objeto.
Mitre Attack	Estrutura de framework através de uma matriz de táticas e técnicas usadas para diagnosticar e lidar com ameaças à segurança cibernética.
NIST	Agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos;
Patch	Um componente de software que, quando instalado, modifica diretamente arquivos ou configurações de dispositivo relacionados a um componente de software diferente, sem alterar o número da versão ou os detalhes da versão do componente de software relacionado.
PDCA	PDCA (Plan, Do, Check, Act, ou em português, Planejar, Fazer, Verificar e Agir) é uma ferramenta de qualidade de quatro fases, amplamente utilizada para a solução de problemas, controle e melhoria contínua de processos e produtos.
Prestador de Serviço	Pessoa representante de um fornecedor, responsável por realizar atividades para auxiliar a empresa que fez a contratação de um fornecedor para atuar no ambiente da Rede Américas.

Privacy/Security by Design	Framework que tem como objetivo incorporar a Privacidade, Proteção de Dados e Segurança da Informação em todos os projetos de uma organização.
Recertificação de Acessos	Processo de revalidar um acesso, realizando a renovação das credenciais de acesso.
Revisão de Acessos	Processo de revisar os acessos atuais dos colaboradores com o objetivo de garantir apenas os acessos corretos aos colaboradores que necessitam do acesso.
Risco	Combinação da probabilidade de ocorrer um evento e suas consequências. Em negócios, risco é o potencial de uma ameaça explorar as vulnerabilidades de um recurso para causar perda e/ou prejuízos, usualmente medido por uma combinação de impacto e probabilidade de ocorrência.
Teste de Intrusão	Avaliação para detectar e explorar vulnerabilidades de um sistema ou ambiente.
Teste de Contingência	Política e procedimentos de gestão usados para orientar a resposta de uma empresa a uma perda percebida de capacidade de missão. O Plano de Contingência é o primeiro plano utilizado pelos gerentes de risco corporativo para determinar o que aconteceu, por que e o que fazer. Pode apontar para o plano de continuidade de operações (COOP) ou plano de recuperação de desastres (DRP) para grandes interrupções.
Topologia de Rede	Uma representação das topologias e componentes da rede interna até o nível do host/dispositivo para incluir, mas não se limitando a: informações de conexão, sub-rede, enclave e host.
Vulnerabilidade	Fragilidade de um ativo ou grupo de ativos que podem ser explorados por uma ou mais ameaças.

4 Introdução

A Rede Américas, através de seu departamento de Segurança da Informação e de forma alinhada com os objetivos e requisitos do negócio, estabelece regras e direcionamentos baseados nas normas NBR ISO 27001, 27002 e no NIST National Institute of Standards and Technology a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações da Rede Américas e suas marcas, de seus clientes, fornecedores e parceiros de negócios.

5 Diretrizes

5.1 Diretrizes Gerais

Com propósito de auxiliar seus funcionários e partes interessadas a entenderem as suas responsabilidades e garantindo a conformidade com as diretrizes previamente definidas e com a legislação, foram desenvolvidos alguns documentos para disseminar o conhecimento dos processos de segurança da informação. Estes documentos estão em ambiente protegido contra alterações e estão disponíveis em local acessível aos colaboradores, prestadores de serviço e fornecedores da Rede Américas.

5.2 Segurança da Informação no Negócio

A seguir estão relacionados os principais controles utilizados pela Rede Américas para proteger as informações, atender às necessidades da segurança cibernética e reduzir a vulnerabilidade a incidentes de acordo com sua Política de Segurança da Informação. Todas as diretrizes descritas abaixo são aplicáveis aos colaboradores, prestadores de serviços e fornecedores da Rede Américas.

5.2.1 Gestão de Riscos de Tecnologia e Segurança da Informação

A Rede Américas deve conduzir a identificação, análise, medição e tratativas de riscos relacionados ao contexto de Segurança da Informação e Tecnologia da Informação de acordo com as diretrizes estabelecidas através dos documentos internos.

Processos, pessoas e tecnologias devem ser continuamente avaliados pelos times responsáveis, para identificar possíveis riscos que possam impactar o negócio.

Os fornecedores também devem passar pelo processo de gerenciamento de riscos da Rede Américas, assim como devem garantir que exista um processo de gestão de riscos interno para mitigar potenciais riscos que possam impactar na prestação de serviços para a organização

Eventuais riscos que não puderem ser tratados através do processo dos planos de correção, serão encaminhados ao Comitê de Riscos e serão identificados como riscos para serem endereçados controles compensatórios para a mitigação.

5.2.2 Gestão de Segurança em Fornecedores

Os prestadores de serviços contratados pela Rede Américas devem ser avaliados através do processo interno de avaliação de fornecedores, conforme descrito nos documentos internos.

Todo o processo de seleção, avaliação e reavaliação deve seguir os critérios definidos em documentos internos, garantindo que seja realizada a avaliação de desempenho de segurança da informação para assegurar a confidencialidade, integridade, disponibilidade e privacidade das informações para os Fornecedores, garantindo que estejam em conformidade com as leis e regulamentações.

Os fornecedores devem realizar a comunicação em caso de incidentes relevantes relacionados às informações armazenadas e processadas por eles, em cumprimento às determinações legais, regulamentares e de acordo com as diretrizes da Rede Américas.

5.2.3 Conscientização de Segurança da Informação para Recursos Humanos

A Rede Américas estabelece um programa de conscientização de diretrizes de Segurança da Informação através de treinamentos e campanhas informativas de maneira periódica com o intuito de fortalecer o conhecimento a respeito do tema de Segurança.

5.2.4 Gestão de Classificação da Informação

Todas as informações sob domínio da Rede Américas devem seguir as diretrizes para que os dados da empresa sejam gerenciados de maneira uniforme em todo o conglomerado, garantindo que estejam os dados classificados como confidenciais e de uso restrito não sejam compartilhados de maneira equívoca, tendenciosa e/ou maliciosa para usuários não autorizados.

Todos os colaboradores, terceiros e prestadores de serviço são responsáveis por garantir a proteção dos dados, sejam impressos ou digitais, garantindo o sigilo necessário das informações.

5.2.5 Gestão de Aquisição, Desenvolvimento e Manutenção de Sistemas

Toda atividade relacionada ao processo de aquisição, manutenção e desenvolvimento de sistemas da informação deve seguir as diretrizes estabelecidas pelos documentos internos da Rede Américas.

Devem ser estabelecidos requisitos mínimos para a aquisição, desenvolvimento e manutenção segura de aplicações e aplicativos visando a redução dos riscos associados à segurança dos dados utilizados pelas aplicações ou à infraestrutura utilizada.

O desenvolvimento de softwares deve seguir critérios e práticas para desenvolvimento seguro de aplicações, com objetivo de reduzir os riscos e impactos nas áreas de negócios, além de propiciar segurança e confiabilidade ao processo de desenvolvimento / implantação de mudanças e/ou novas versões de sistemas no ambiente de produção.

Devem garantir a realização de avaliações e testes de segurança de aplicações desenvolvidas no ambiente de homologação da Rede Américas.

5.2.6 Gestão de Controle de Acesso Lógico e Físico

Através de um processo estruturado de solicitação e aprovação, a área de Gestão de Identidade e Acessos busca assegurar que o acesso lógico seja concedido apenas a usuários autorizados, contribuindo para a proteção e segurança dos ativos de informação da Rede Américas.

A Rede Américas conta com processos definidos de concessão, revisão, recertificação dos acessos, além de realizar a construção de matrizes de acessos baseadas para incorporar o menor privilégio aos colaboradores. São estabelecidos padrões para os tipos de credenciais, privilégios e nomenclatura das contas dos usuários para acesso aos sistemas informatizados.

Para o controle de acessos físicos, a Rede Américas possui um processo estabelecido de segurança patrimonial contando com controles de segurança técnicos (Leitores Biométricos, Controles de Acessos em Unidades, Sistemas de CFTV) para garantir a incolumidade da segurança física das pessoas, ativos e da imagem da empresa.

Todos os acessos físicos e/ou lógicos realizados no ambiente da Rede Américas devem ser devidamente aprovados de maneira prévia e revisados periodicamente.

5.2.7 Gestão de Incidentes de Segurança da Informação

A Rede Américas conta com uma equipe de Centro de Defesa e Operações Cibernéticas definida para realizar o monitoramento da segurança, estabelecendo um processo para identificar, notificar e gerenciar os incidentes de segurança da informação e determinar as regras para apurar, responsabilizar e aplicar as medidas corretivas e disciplinares em decorrência de violações da política de segurança da informação.

A equipe responsável pelo monitoramento deve gerenciar as atividades ou eventos através da análise de logs, detectando atividades não autorizadas ou inadequadas de processamento da informação e atende requisitos legais relevantes aplicáveis às suas atividades de registro e monitoramento.

5.2.8 Gestão de Uso de Recursos Tecnológicos

Os ativos tecnológicos são quaisquer recursos de informação que tenham valor, podendo ser software e hardware, que devem ser identificados, inventariados e atualizados para garantir a disponibilidade dos ativos tecnológicos para a empresa.

As diretrizes determinam que a organização deve conduzir e garantir o backup das informações dos ativos e informações (arquivos corporativos, sistemas de produção, programas, aplicativos, sistemas operacionais, banco de dados), realizando testes periódicos de restauração de arquivos armazenados em servidores.

Todos os colaboradores devem utilizar os ativos e recursos de Tecnologia da Informação de maneira correta de acordo com as definições descritas em procedimentos internos.

5.2.9 Gestão de Vulnerabilidade e Patches

Todos os ativos, sistemas, plataformas, redes e/ou sistemas da companhia devem passar por análises de vulnerabilidades e aplicações de patches para identificar possíveis vulnerabilidades que possam causar impacto na operação da companhia ou riscos que possam causar impacto financeiro, operacional e/ou reputacional.

A equipe de Tecnologia da Informação deverá identificar, corrigir e atualizar todos os patches que estejam aplicáveis aos seus ativos tecnológicos, garantindo também que todos os ativos possuam baselines de segurança da informação estabelecidos para garantir a segurança destes dispositivos.

A organização conta com um processo estruturado para garantir a priorização, tratamento e validação das vulnerabilidades da empresa, buscando tratar as vulnerabilidades críticas de maneira rápida e efetiva (através da realização de testes das ações de correção). Em caso de vulnerabilidades críticas não tratadas dentro do prazo estipulado, a equipe conta com um processo de gestão de riscos estabelecido para tratar as vulnerabilidades e realizar o acompanhamento em conjunto com os responsáveis.

5.2.10 Gestão de Teste de Intrusão

O teste de intrusão estabelece a análise de atividades e de vulnerabilidade de sistemas, com o objetivo de identificar possíveis fragilidades no sistema. A organização estabelece um ciclo de testes através das seguintes etapas: Planejamento, Preparação, Execução e Encerramento. Todas as etapas e processos relacionados aos testes estão correlacionados com frameworks existentes na atualidade (como NIST e Mitre Att&ck).

A organização estabelece que testes internos ou externos podem ser realizados, com o intuito de avaliar a infraestrutura, topologia de rede, estrutura de sistemas e demais pontos tecnológicos que podem ser avaliados através do teste.

5.2.11 Gerenciamento de Crise

A organização estabelece um processo de gerenciamento de crise para realizar atividades de recuperação em caso de um cenário de crise e/ou desastre.

O processo estabelece diretrizes para realizar a identificação, gerenciamento, comunicação interna e externa, tratativas de contenção e de correção e encerramento da crise. Através destas etapas, as equipes são mobilizadas para garantir que todas as ações sejam realizadas de maneira rápida e efetiva, para estabelecer a recuperação das atividades e garantir a redução de prejuízo para a empresa.

5.2.12 Continuidade de Negócios

A Rede Américas conta com um processo estabelecido de gestão de continuidade de negócios com o objetivo de minimizar os impactos negativos causados por qualquer evento que ofereça risco à continuidade dos negócios da empresa.

O processo está baseado no modelo PDCA (Plan-Do-Check-Act) para estabelecer, implementar, operar, monitorar, analisar criticamente e melhorar continuamente a eficácia do sistema de gestão de continuidade de negócios garantindo as melhores práticas de acordo com os frameworks da atualidade.

São estabelecidos processos de análise de impacto e riscos para garantir o mapeamento e potenciais ameaças à continuidade de negócio da empresa, bem como garantir que os processos estão seguindo diretrizes através dos planos e testes de contingência.

6 Penalidades

O não cumprimento desta Política de Segurança da Informação pode gerar riscos de segurança da informação, financeiros, vazamento de informações, uso impróprio e negativo da imagem da empresa, bem como não garantir a confidencialidade, integridade, disponibilidade e privacidade da informação.

7 Responsabilidades

Alta Direção

- Estar alinhada e comprometida com a política de segurança da informação, bem como suas normas e procedimentos.
- Definir responsabilidades e alocar os recursos necessários para a implantação e manutenção dos diversos controles de segurança da informação.
- Assegurar que as metas de segurança da informação estejam identificadas, atendam aos requisitos da Rede Américas e estejam integradas nos processos relevantes.
- Aprovar as atribuições de tarefas e responsabilidades específicas para a segurança da informação.
- Assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeia a Rede Américas.

Segurança da Informação

- Monitorar os recursos e os ambientes sob sua responsabilidade com o objetivo de garantir a proteção contra possíveis ameaças e usos inadequados.
- Gerenciar os controles e as ferramentas de segurança da informação, assim como tratar os incidentes, problemas, mudanças e quaisquer requisições e/ou reportes relacionados à segurança da informação.
- Analisar de forma sistemática e periódica, os controles, incluindo a política, as normas e os procedimentos de segurança da informação, para que eles se mantenham efetivos, pertinentes e aderentes aos requisitos do negócio.
- Desenvolver e manter a políticas de segurança da informação.
- Interagir com as áreas de Infraestrutura de TI e sistemas na avaliação de impactos e riscos, no desenvolvimento, na homologação e na gestão de mudanças do ambiente de tecnologia da Rede Américas.
- Desenvolver em conjunto com a diretoria de Gestão de Pessoas, ações de disseminação da cultura de segurança da informação na Rede Américas.
- Realizar reuniões periódicas do Comitê de Segurança da Informação e Cibernética com as principais lideranças de tecnologias e negócios.
- Elaborar e propor iniciativas voltadas à manutenção e evolução do nível de segurança da Rede Américas, a serem validadas e patrocinadas pelo Comitê de Segurança da Informação.

- Avaliar os riscos associados à segurança da informação, identificando previamente os potenciais riscos à confidencialidade, integridade e disponibilidade.
- Coordenar a implantação das medidas preventivas e corretivas. Fiscalizar, analisar, reportar e coordenar a resposta de incidentes de segurança da informação.
- Elaborar relatórios periódicos contendo indicadores de segurança e progressos.
- Administrar o acesso lógico aos sistemas, respeitando as políticas aplicáveis.
- Garantir que os usuários tenham acesso, somente, às informações a que foram autorizados pelo respectivo líder.
- Adotar padrões de segurança, no desenvolvimento e na aquisição de novos produtos, desde sua concepção (privacy/security by design and default).
- Realizar exercícios cibernéticos com participação de múltiplos atores.

Privacidade de Dados

- Suportar e Apoiar em questões legais relacionadas ao tema de dados pessoais;
- Realizar a avaliação de riscos relacionadas ao contexto de privacidade e proteção dos dados pessoais;
- Prestar suporte em cenários de incidentes de violação de dados pessoais, bem como realizar diagnósticos de incidentes de privacidade.

Tecnologia da Informação

- Monitorar os recursos e os ambientes sob sua responsabilidade com o objetivo de garantir a proteção contra possíveis ameaças e usos inadequados, assim como mantê-los em dia com as atualizações e mudanças nas legislações e/ou nos requisitos do negócio.
- Garantir o armazenamento e retenção de logs quanto ao acesso a serviços de rede, aplicações, sistemas e ativos de informação para que exista visibilidade e análise de incidentes de segurança.
- Implementar ações das medidas preventivas e corretivas relacionadas ao tema de Tecnologia da Informação.
- Operacionalizar e fornecer apoio às atividades de segurança da informação no ambiente de TI da Rede Américas e nos demais processos, nas diversas áreas de negócio.
- Manter o inventário de recursos de tecnologia e as informações da Rede Américas atualizados, bem como os demais controles e procedimentos relacionados aos recursos de tecnologia.

Auditoria Interna

- Ser consultado em caso de necessidade para orientar e apoiar na elaboração e realização de reuniões periódicas do Comitê de Segurança da Informação e Cibernética para manter a evolução do nível de segurança com as demais áreas de tecnologia.
- Orientar e apoiar na análise e elaboração de indicadores de forma sistemática e periódica para os controles, incluindo políticas, normas e procedimentos de segurança da informação.
- Analisar e avaliar riscos e controles relacionados ao contexto de Segurança da Informação na organização.
- Elaborar anualmente um plano anual de auditoria, abrangendo áreas, processos e atividades dos riscos de maior relevância da empresa, endereçando preocupações ao Corpo Diretivo e Comitê de Auditoria.

Fornecedores

- Estar alinhado e comprometido com as diretrizes de Segurança da Informação da Rede Américas;
- Disponibilizar os recursos necessários para atender as diretrizes da Rede Américas;
- Respeitar os direitos de propriedade autoral, industrial ou intelectual sobre os serviços prestados, projetos e produtos desenvolvidos para Rede Américas;
- Notificar a Rede Américas imediatamente em quaisquer situações de violação ou que possibilite a violação dos controles de segurança da informação;
- Assegurar que a cultura de segurança da informação seja seguida na organização;
- Garantir a conformidade regulatória, a fim de atender as demandas previstas pela legislação local;
- Assegurar a integridade, a confidencialidade, disponibilidade e privacidade das informações da Rede Américas.

Colaboradores e Prestadores de Serviço

- Conhecer a política de segurança da informação da Rede Américas, bem como os demais controles e procedimentos relacionados à mesma, e aplicáveis às atividades desempenhadas.

- Observar estritamente as disposições contidas na política de segurança de informação e suas atualizações, as quais se encontram disponíveis no sistema de gestão da qualidade.
- Ler e assinar o termo de acordo de confidencialidade.
- Utilizar e ser responsável pelos recursos tecnológicos e pelas informações da Rede Américas em caráter estritamente profissional, limitado ao âmbito de suas atividades e observando sempre os requisitos de ética.
- Manter o sigilo das informações que você tem acesso ou conhecimento.
- Consultar a política de segurança da informação e as normas relacionadas, o líder da área ou a equipe de segurança da informação, sempre que tiver dúvidas de como agir.
- Proteger as informações às quais tenha acesso, garantindo que recebam o tratamento adequado, de acordo com sua classificação e seus procedimentos, em respeito ao compromisso de sigilo profissional assumido.
- Relatar, imediatamente, quaisquer situações de violação ou que possibilitem a violação dos controles de segurança da informação que venha a tomar conhecimento.
- Reportar qualquer suspeita de violação de segurança e comportamento, em não conformidade com as diretrizes contidas na Política de Segurança da Informação, bem como todos os incidentes de segurança ocorridos, à gerência de segurança da informação.
- Colaborar com os programas de conscientização promovidos pela diretoria de Gestão e Pessoas e gerência de Segurança da Informação.
- Observar e respeitar que os direitos de propriedade intelectual são da Rede Américas, sabendo que estes direitos recaem tanto sobre ativos tangíveis quanto intangíveis, incluindo as marcas, as patentes, os códigos-fonte, os contratos de licenciamento entre outros.
- Colaborador pode sofrer medidas legais e/ou profissionais caso acesse, transmita ou gere informações de conteúdo ilegal, malicioso, impróprio ou que conflite ou contrarie os valores e interesses da Rede Américas.

8 Referências

Política de Segurança da Informação

Política de Continuidade de Negócios

NIST – Information Technology Laboratory COMPUTER SECURITY RESOURCE CENTER

– Glossary

9 Canal de Comunicação de Segurança da Informação

Para comunicar algum incidente, envie um e-mail para:

- security@americasmed.com.br

*Vigência imediata a partir da aprovação.