Política de Segurança Cibernética

Grupo Rede Tendência

Segurança da Informação – DTI

1. Introdução

Este documento institui a Política de Segurança Cibernética do Grupo Rede Tendência.

A presente política é composta por um conjunto de medidas necessárias à preservação da Segurança Cibernética e das Informações do Grupo Rede Tendência, clientes, fornecedores e colaboradores. Todos os conceitos e recomendações são pautados pelas melhores práticas de segurança da informação e requisitos regulatórios vigentes.

Em qualquer negócio, os ativos de informação são considerados os bens mais importantes, portanto, tratá-los com responsabilidade é uma premissa do Grupo. Diante do exposto, buscamos nossos fundamentados em princípios mandatórios de segurança da informação, o qual objetiva a preservação da propriedade da informação, sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, assim como o tratamento e monitoramento dos incidentes oriundos de ataques cibernéticos.

- Confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas a terem tal acesso;
- Integridade: salvaguarda da exatidão e completude da informação e dos métodos de processamento;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. Objetivo e Aplicação

O objetivo desta política é garantir a proteção, integridade, privacidade, disponibilidade e confidencialidade das informações de propriedade do Grupo Rede Tendência e/ou sob sua guarda, além de prevenir, dectectar e reduzir a vulnerabilidade inerente ao ambiente cibernético a através de processos e controles robusto, os quais constituem

regras que representam os princípios e fundamentos para o alcance dos objetivos da segurança da informação do Grupo Rede Tendência.

Essa Política expressa o zelo e o compromisso do Grupo Rede Tendência com a informação de seus clientes, colaboradores e fornecedores proporcionando satisfação quanto a segurança e privacidade de suas informações, além de demonstrar compromisso com os apectos regulatórios e de negócio, portanto, encontrando-se sempre em conformidade com as regulamentações vigentes.

Esta política se destina a todos os colaboradores do Grupo Rede Tendência, incluindo, mas não se limitando a: funcionários, estagiários, contratados, parceiros e fornecedores.

As diretrizes desta política devem ser aplicadas em todas as unidades do Grupo Rede Tendência.

3. Vigência

Esta passa a vigorar a partir da data de sua aprovação e publicação e deve ser revisada anualmente ou, quando necessário, em caso de mudanças nas diretrizes/objetivos do Grupo ou de segurança da informação, ou ainda, se requerido pelo órgão regulador.

O documento foi elaborado pela área de Segurança da Informação e aprovado por um grupo de executivos da empresa, identificados no quadro de “Histórico de alterações do documento”.

4. Controles e Procedimentos Para Garantir os Objetivos da Segurança Cibernética

A disseminação da cultura de segurança cibernética é de fundamental importância para garantir a integridade, confiabilidade e disponibilidade das informações. Com objetivo de garantir o cumprimento dos objetivos propostos, o Grupo Rede Tendência utiliza meios como políticas internas, comunicados corporativos, instruções normativas, realização de treinamentos periódicos sobre *compliance* e segurança da informação.

5. Controles Adotados Para a Segurança das Informações Sensíveis

O Grupo Rede Tendência possui vários procedimentos e controles objetivando garantir a segurança das informações sensíveis, conforme descrito nos tópicos abaixo:

5.1 Gestão de acesso às informações

O controle de acesso previne o acesso de indivíduos não autorizados aos sistemas e ambientes, com isso garante a confidencialidade das informações.

A política de gestão de acessos aborda os direitos de acesso como, perfis, concessão, revisão, monitoramento e revogação. As atividades citadas obedecem ao princípio de perfil mínimos e a concessão ou alteração necessitam de aprovação pelo gestor direto.

As instalações e equipamentos que processam informação crítica ou sensível são mantidos em áreas seguras, com acesso controlado, incluindo proteção contra ameaças físicas e ambientais.

Os colaboradores do Grupo recebem treinamentos periódicos sobre os conceitos de segurança da informação, através do programa de conscientização disseminação cultural de segurança cibernética.

O Grupo realiza revisões periódicas dos acessos, conforme política, a qual tem objetivo de atualizar os acessos e permissões. Este procedimento é coordenado pela área de segurança da informação com anuência da final da Diretoria.

5.2 Proteção de Ambiente Crítico do Grupo

Os recursos de processamento de informações do Grupo possuem controles e responsabilidades, visando garantir a segurança na infraestrutura tecnológica do Grupo por meio de um gerenciamento efetivo no monitoramento, tratamento e na resposta aos incidentes, visando minimizar o risco de falhas e a administração segura de redes de comunicações.

5.2.1 Autenticação

O acesso às informações e ambientes de tecnologia do Grupo deverá ser permitido somente às pessoas autorizadas pelos proprietários da informação, considerando a premissa do menor privilégio, a classificação da informação e a segregação das funções.

O controle de acesso deve considerar, no mínimo, os seguintes requisitos:

- Identificadores únicos (credencial de acesso) e individualizados, com monitoramento e com possibilidade de bloqueio e restrições, os quais podem ser automatizados ou manuais;
- Revogação imediata das autorizações a usuários desligados ou afastados do Grupo, ou que tiveram sua função alterada; e
- Realização de revisões periódicas nas concessões de acesso.

5.2.2 Gestão de Incidentes de Segurança da Informação

O monitoramento de possíveis ataques devem ser realizados permanentemente através de controles de detecção de implementados no ambiente, como ferramentas de IDS/IPS, filtros de conteúdo, Antivírus, *Antispam.*

5.2.3 Gestão do uso dos recursos de tecnologia da informação

O Grupo controla os aplicativos instalados nos computadores verifica periodicamente o controle de acessos à internet. Nenhum usuário detém a permissão de administrador local, o que impossibilita a instalação de qualquer software não aprovado pela DTI. Somente podem ser instalados aplicativos previamente testados e autorizados por TI. A equipe de TI realiza o monitoramento da rede por meio de software específico.

5.2.4 Varredura de vulnerabilidades

As varreduras das redes internas e externas são executadas periodicamente em busca de vulnerabilidades e devem ser tratadas e priorizadas conforme seu nível de criticidade.

5.2.5 Teste de Intrusão

Devem ser executados, no mínimo anualmente, testes de intrusão nas camadas de rede interna e externa.

5.2.6 Gestão de ameaças e Vulnerabilidades de TI

O ambiente do Grupo possui *software* de antivírus para a proteção contra vírus, arquivos e *softwares* maliciosos, atualizados periodicamente. Todas as atualizações de segurança dos *softwares* e sistemas operacionais deves seguir a política de atualização de *patchs* e correções de segurança.

5.2.7 Rastreabilidade

Todos os componentes da infraestrutura e sistemas devem possuir logs que permitam reconstituir eventos como:

- Autenticação dos usuários;
- Acesso às informações;
- Ações de criação, remoção e alteração executadas pelos usuários do sistema.

5.2.8 Cópias de segurança

A execução das rotinas de *backup* devem ser realizadas periodicamente nos ativos de informação do Grupo Rede Tendência com objetivo de evitar e/ou mitigar a perda de dados após a ocorrência de um incidente importante.

5.2.9 Gestão e segurança de Senhas

Quando disponível, os sistemas de informação do Grupo são integrados ao *Active Directory*, o qual possui as suas especificidades de parâmetro de senha definidas em políticas. Para sistemas que não estão integrados com AD, existe um pré-requisito mínimo para as parametrizações de senhas definido em política. A gestão de parametrização de segurança de senhas são prerrogativas exclusivas da área de Segurança da Informação.

5.2.10 Segurança de Rede e Segmentação

Todos os ambientes (Desenvolvimento, Homologação e Produção) são segregados e devem possuir regras específicas de acesso aos mesmos.

Quando necessário, todo acesso de terceiros ao ambiente deve ser devidamente justificado e autorizado pela área de segurança da informação. O acesso deve ocorrer por VPN, ser monitorado, e ter regras de acesso específicas com tempo determinado.

Para solicitação de criação, exclusão e alteração de regras nos firewalls ou ativos de rede, o pedido deve ser encaminhado para a área de segurança da informação, o qual fará irá deferir ou não o pedido, e caso sim, enviar para a execução na área de TI e seguir o fluxo da gestão de mudanças.

5.2.11 Segurança física

As instalações e recursos de processamento de informações de negócio e críticas relativas as atividades do Grupo estão localizadas em áreas seguras, com barreiras físicas de segurança apropriadas e conta com recursos para o controle do acesso. Os equipamentos críticos possuem redundância ativa e proteção contra desastre físico e recursos para combate a incêndio. Todas as instalações possuem sistema de controle do acesso dos colaboradores, prestadores de serviços ou fornecedores aos locais restritos, além de monitoramento por câmeras.

6. Registro, análise da causa de incidentes relevantes e vulnerabilidades

O registro e análise dos incidentes relevantes são tratados com a urgência adequada com objetivo de minimizar os impactos negativos para o Grupo Rede Tendência, em nível operacional e de imagem.

O Grupo entende a importância da existência de um procedimento de tratamento de incidentes e que possibilite a detecção oportuna e a imediata comunicação de incidentes e vulnerabilidades, e que, em consequência, assegure a eficácia das medidas de tratamento seguintes. Diante da importância do assunto, o Grupo possui um processo de incidentes que contempla os controles que permitem detectar e identificar os incidentes e vulnerabilidades que afetam o ambiente de Segurança Cibernética. As responsabilidades referentes ao registro, análise e comunicação dos incidentes estão especificadas no processo de gestão de incidentes.

7. Continuidade dos Negócios

O Plano de Continuidade de Negócios (PCN), é implementado com o objetivo de mitigar os impactos e perdas de ativos da informação após um incidente crítico, buscando sempre um nível aceitável, por meio do mapeamento de processos críticos, testes periódicos de recuperação de desastres e análise de impacto nos negócios.

Com objetivo de melhoria contínua, o plano de continuidade de negócios (PCN) é constantemente revisado e ajustado quando necessário. O plano busca identificar constantemente os cenários que possam vir a comprometer as atividades chaves do Grupo, analisando o impacto e promovendo resiliência técnico organizacional, fortalecendo assim a organização na capacidade de antever ou, quando não for possível, responder de forma eficaz e assertiva a eventos desfavoráveis.

7.1 Classificação da criticidade dos incidentes

Os incidentes relacionados à segurança cibernética seguem a criticidade definida no processo de gestão de incidentes, considerando três tipos situação: crítica, catastrófica, inesperada.

7.1.1 Plano de ação de resposta a incidentes

Em caso de ocorrência de um incidente, o mesmo deve ser analisado e, em seguida criado um plano de ação para correção e minimizar o risco de recorrência. A elaboração e acompanhamento do plano são coordenados Área de Tecnologia da Informação, com colaboração de outras áreas interessadas.

8. Treinamento e conscientização em segurança da informação

O Grupo Rede Tendência apoia e incentiva a cultura do ambiente seguro, visando garantir e proteger os objetivos inicia desta política, ou seja, proteger efetivamente a informação.

A disseminação da cultura se dá através de distribuição de informativos sobre segurança da informação nos canais de comunicação corporativa, além de palestras de capacitação ministradas periodicamente aos colaboradores, com isso garantindo que todos esteja ciente das possíveis ameaças e vulnerabilidades que podem ser

exploradas no mundo cibernético, assim como quais procedimentos tomar em caso de detecção de um incidente.

O Grupo Rede Tendência está ciente da importância das atividades relacionadas a Segurança Cibernética, as quais estão em evolução constante, e diante deste fato aplica o conceito de melhoria continua nos controles, procedimento e políticas, os quais são revistas periodicamente, visando manter o ambiente de Segurança Cibernética alinhado com as melhores práticas, leis e regulamentos, incluindo sua participação em iniciativas de compartilhamento de informações sobre incidentes cibernéticos com outras instituições financeiras e/ou entidades de classe quando pautado assunto referente ao tema.

9. Compartilhamento de informações

O Grupo Rede Tendência tem o compromisso com a transparência e se compromete a compartilhar com o as autoridades regulatórias todos incidentes relevantes, prontamente, sempre que solicitado.

9.1 Compartilhamento de informações de ocorrências

Conforme objetivos da Circular do Banco Central n.3.909/18, Art. 22, o Grupo Rede Tendência entende a necessidade de promover e incentivar a troca de informações entre os integrantes do sistema financeiro nacional e promoverá o compartilhamento de ocorrências de segurança cibernética, incluindo situações relacionadas a fornecedores e prestadores de serviço, cujos registros estão armazenados no sistema de gestão de incidentes. As informações compartilhadas por outras instituições, de maneira similar, serão apresentadas e debatidas em Comissões Internas e Comitês, a fim de definir ações preventivas.

10. Contratação de serviços de armazenamento de dados e processamento e de computação em nuvem

Quando necessário, toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem estar aderentes com as diretrizes indicadas na circular do BACEN 3.909/18.

11. Relatório anual

Em alinhamento com a Resolução 3.909/18 do BACEN, anualmente, até o 31 de março, o Grupo deverá disponibilizar um relatório sobre a implementação do plano de ação de respostas a incidentes, com data base de 31 de dezembro do ano anterior ao relatório, contendo:

- A efetividade da implementação das ações a serem desenvolvidas pela instituição para adequar suas estruturas aos princípios e às diretrizes da política de Segurança Cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes ocorridos no período;
- Resultado dos testes de continuidade de negócios.

12. Documentação mínima a ser arquivada com base na resolução 3.909/18

Devem ficar à disposição do Banco Central do Brasil pelo prazo de 05 (cinco) anos:

- A presente Política;
- Ata do Conselho de Administração com a aprovação da Política;
- Documento relativo ao plano de ação e de resposta a incidentes;
- Relatório anual;
- Documentação sobre os procedimentos;
- Documentação que trata no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;

- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle que visam assegurar a implementação e a efetividade da política se Segurança Cibernética.

13. Auditorias e controles

A Política de Segurança Cibernética e seus processos, estão sujeitos à avaliação de controles internos e auditorias.

14. Responsável perante o BACEN

O Diretor de Riscos é o responsável pela política de segurança cibernética, o qual encontra-se cadastrado no sistema do Banco Central do Brasil.

15. Responsabilidade

Todos os colaboradores, independentemente do nível hierárquico, são responsáveis por conhecer e cumprir as diretrizes, políticas, normas e procedimentos de Segurança Cibernética do Grupo Rede Tendência.

16. Sanções e Penalidades

O não cumprimento desta política e demais políticas, normas e procedimentos de segurança da informação, poderá incorrer em sanções administrativas e/ou legais, podendo culminar com o desligamento e eventuais processos criminais, se aplicável.

A área de Segurança da Informação é responsável por avaliar o grau de criticidade da violação, e solicitar o envolvimento de outras para a análise das punições cabíveis, como a área de Recursos Humanos e o departamento Jurídico.

17. Normativos internos relacionados

- Política de Segurança da Informação;
- Plano de Continuidade de Negócios;
- Processo de Gestão de Incidentes;

- Política de Utilização dos Recursos de Informática;
- Política de Gestão de Ativos;
- Política de Utilização do Correio Eletrônico;
- Política de Senhas;
- Política de Patches e Correções;
- Política de Segurança Física e Ambiental do Datacenter;
- Política de Utilização de Computadores Portáteis e Dispositivos de Comunicação;
- Política de Segurança de Rede Interna;
- Política de Backup e Restore;
- Política de Acesso ao Datacenter;
- Política de Chaves Criptográficas;
- Processo de Gestão de Mudanças.

18. Revisão

Para garantir a qualidade e adequação aos riscos da empresa, este documento deverá ser revisado e atualizado anualmente ou conforme a necessidade.

19. Histórico de alterações do documento

Data	Versão	Elaborado por: *	Resumo das alterações
10/2020	1.0	Fabio Peralta Martins - Coordenador de Infraestrutura	Elaboração
10/2020	1.0	Valzumiro Ceolim – Presidente	Aprovação
10/2020	1.0	Leonardo Hey Letteriello – Diretor de Tecnologia da Informação	Aprovação
10/2020	1.0	Rosângela Martinello – Diretora de Adm / RHDO	Aprovação
10/2020	1.0	Marcia Gabrielle Ceolim – Gerente Financeiro	Aprovação

11/2020	1.1	Fabio Peralta Martins - Coordenador de Infraestrutura	Revisão
11/2020	1.1	Leonardo Hey Letteriello – Diretor de Tecnologia da Informação	Aprovação
11/2020	1.2	Fabio Peralta Martins - Coordenador de Infraestrutura	Revisão
11/2020	1.2	Leonardo Hey Letteriello – Diretor de Tecnologia da Informação	Aprovação

* A assinatura dos responsáveis está disponível na cópia impressa, arquivada na área de Segurança da Informação

Anexo I. Termos

- Ativo – Patrimônio composto por bens (infraestrutura, pessoas, informação e aplicações) e direitos da empresa.
- Colaborador – Pessoa que presta serviços ao Grupo Rede Tendência, através de Contrato Individual de Trabalho, ou por vínculo a um Contrato de Prestação de Serviço.
- Incidente de segurança de informação – refere-se a qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.
- Informação – é produto resultante do processamento, manipulação e organização dos dados, sejam eles registros, voz e imagem.
- Gestor – Gerente, Coordenador ou Administrador.
- Sistema de Informação - é a expressão utilizada para descrever um Sistema seja ele automatizado, seja manual, que abrange pessoas, máquinas e/ou métodos organizados para coletar, armazenar, processar, transmitir e disseminar dados que representam informação para o usuário e/ou cliente.
- Usuário – Pessoa autorizada a utilizar os recursos e ativos de informação do Grupo Rede Tendência.
- Recursos – equipamentos (como computadores, celulares, impressoras entre outros), infraestrutura (como a rede, acesso à internet, entre outros) e informações.
- Incidente – ocorrência que pode afetar a segurança das informações.