Política de Segurança da Informação e Cibernética

TC S.A.

Julho, 2023

SUMÁRIO

FICHA TÉCNICA

Título:	Política de Segurança da Informação e Cibernética
Área Responsável:	Riscos e *Compliance*
Objetivo:	Definir regras e diretrizes para assegurar a independência, proteção e a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações para todos os Colaboradores
Aplicação:	As normas aqui contidas devem ser aplicadas a todos os sócios administradores, empregados, funcionários, trainees e estagiários do grupo TC, bem como aos prestadores de serviços alocados nas dependências da empresa de forma temporária (em conjunto os "Colaboradores" e, individualmente, "Colaborador")
Data de Aprovação:	31/07/2023
Aprovado por:	Comitê de Governança, Riscos e *Compliance* ("Comitê de GRC")
Data de Publicação:	2S23

LISTA DE ABREVIAÇÕES E SIGLAS

SIC – Segurança da Informação e Cibernética

TC – TC S.A.

2FA – Identificação por dois fatores

1. INTRODUÇÃO

O objetivo desta Política é definir as regras e diretrizes para assegurar a independência, proteção e a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações para todos os nossos Colaboradores – o que inclui nossos sócios, administradores e empregados, do TC Traders Club S.A e demais empresas do grupo.

2. REFERÊNCIAS

A construção desta Política, bem como os procedimentos inerentes a seu cumprimento observam, além das disposições internas das Políticas, procedimentos e disposições contratuais, as disposições regulatórias e legais (como também no CBG), constantes nas ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos; ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação; ABNT NBR ISO/IEC 27701:2019 – Tecnologia da Informação – Técnicas de segurança – gestão da privacidade da informação — Requisitos e diretrizes; Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018; Lei de Acesso à Informação (LAI) 12.527 de 18/11/2011; Resolução CVM nº 35/2021 e Resolução CMN nº 4893/2021.

3. ABRANGÊNCIA

As diretrizes aqui contidas devem ser aplicadas a todos os Colaboradores – o que inclui nossos sócios, administradores e empregados do TC Traders Club S.A. e demais empresas do grupo.

4. ÁREAS ENVOLVIDAS E RESPONSABILIDADES

4.1 CONSELHO DE ADMINISTRAÇÃO

- Avaliar e aprovar as diretrizes de segurança da informação, como as Políticas e procedimentos voltados ao tema.

4.2 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

- Deliberar sobre o orçamento para Tecnologia e Segurança da Informação;
- Aprovar as normas e procedimentos gerais relacionados à segurança da informação;
- Designar, definir ou alterar as atribuições da Área de Segurança da Informação;
- Aprovar as principais iniciativas para a melhoria contínua das medidas de proteção para detectar vulnerabilidades e artefatos maliciosos, monitorar e analisar possíveis ataques;
- Apoiar a implantação de soluções para eliminação ou minimização dos riscos;
- Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;
- Suportar perante toda a Organização as iniciativas da Área de Segurança da Informação.
- Garantir a recuperação dos sistemas de informação

4.3 DIRETORIA DE COMPLIANCE E SEGURANÇA DA INFORMAÇÃO

- Elaborar e revisar, mínimo anualmente, a Política de Segurança da Informação e Cibernética do TC;
- Garantir a efetividade e a eficácia da segurança sobre todas as tecnologias empregadas e as operações;

- Garantir ações educacionais, como treinamento específico sobre SI para novos colaboradores, além de iniciativas de atualização para os demais colaboradores;
- Participar das revisões dos procedimentos em casos de alterações nos sistemas de informação do TC.
- Assegurar a análise tempestiva de possíveis incidentes envolvendo informações classificadas e/ou dados pessoais;
- Disseminar a cultura de Segurança da Informação e Cibernética.

4.4 Diretoria de Tecnologia

- Garantir o cumprimento dos requisitos de segurança no ambiente tecnológico e atuar em parceria com a Diretoria de Compliance e Segurança da Informação no atendimento aos requisitos de segurança e de continuidade das operações dos negócios;

4.5 Colaboradores, Terceiros, Fornecedores, Parceiros e Partes Interessadas do TC

- Preservar a integridade e guardar sigilo das informações que fazem uso;
- Zelar e proteger os equipamentos disponibilizados para a realização do seu trabalho;
- Transitar informações somente nos canais oficiais (slack, e-mail e google drive);
- Comunicar ao seu superior imediato qualquer irregularidade ou desvio;
- Cumprir as determinações desta Política e demais normas, sob pena de incorrer nas sanções disciplinares e legais cabíveis.

5. Diretrizes

Essa Política tem como diretrizes:

I – Garantir que somente pessoas autorizadas tenham acesso às instalações do TC e aos sistemas de informação, bem como proteger os processos críticos de negócio contra falhas, invasão ou desastres;

II – Certificar e manter atualizados mecanismos de proteção contra malwares;

III – Restringir o acesso às informações sensíveis de acordo com a necessidade de conhecimento para o negócio; e

IV – Proporcionar a consistência e tempestividade das informações que devem ser relevantes para a tomada de decisões ou que afetem suas atividades, por meio de processo de comunicação confiável, oportuno, compreensível e acessível.

Além disso, o TC se baseia em 09 pilares de segurança da informação na definição e cumprimento de suas diretrizes, sendo:

I – Confidencialidade: Garantir o acesso a informações somente por pessoas autorizadas.

II – Integridade: Garantir que a informação se mantenha em seu estado natural sem alterações indevidas.

III – Disponibilidade: Garantir que a informação esteja disponível sempre que necessário.

IV – Prevenção: Garantir as medidas de proteção dos ativos.

V – Detecção: Garantir o monitoramento constante do ambiente para identificar de forma rápida algum incidente.

VI – Resposta: Determinar o motivo do incidente e ações para que não volte a ocorrer.

VII – Tecnologia: Ferramentas e aplicações utilizadas para a prevenção, detecção e resposta.

VIII – Processos: Definições de políticas, normas e procedimentos para assegurar a segurança da informação.

IX – Pessoas: Todos colaboradores da TC e demais empresas do grupo de forma estruturada, treinada e orientada quanto a Segurança da Informação.

São de propriedade do TC todas as informações, criações e metodologias geradas utilizando-se integralmente ou parcialmente seus recursos.

6. Concessão, Revogação de Acessos e Critério de Senha de Acesso

6.1. Concessão de Acesso

a. Aplicações

Para a concessão de acessos deve ser necessário o registro por meio da ferramenta de chamados, a qual deve seguir um workflow de aprovação para posterior criação dos acessos.

A concessão de acessos aos sistemas de informação do TC deve seguir aos seguintes critérios:

I – Ser documentada e registrada por meio da ferramenta adequada;

II – Conter aprovação do gestor (superior direto) e do responsável da aplicação;

III – Ser concedida de forma que restrinja o acesso apenas às atividades do colaborador e/ou prestador de serviço, de acordo com a matriz de segregação, e de acordo com os tipos de perfis oferecidos por cada sistema em particular; e

IV – A solicitação de acessos para prestadores de serviços deve ser registrada pelo gestor responsável por meio da ferramenta de chamados.

Caso seja necessário a prorrogação dos acessos, compete ao gestor responsável pelo recurso solicitar renovação por meio de abertura de chamado na ferramenta com a devida justificativa.

B. Banco de Dados

Para a concessão de acessos a banco de dados deve ser necessário o registro por meio da ferramenta de chamados, a qual deve seguir um *workflow* de aprovação do gestor imediato e, mandatoriamente, pelo Diretor de TI para posterior criação dos acessos.

O TC tem critérios definidos para contratação de serviços relevantes de processamento e armazenamento de dados e incluem a identificação e segregação de dados dos clientes, além de garantia de confidencialidade, integridade, disponibilidade e recuperação de dados e informações processadas ou armazenadas de forma independente das demais empresas que compõe o grupo

A área de TI do TC é responsável pela prestação de serviços de processamento e armazenamento de dados e conta com um servidor próprio, cujo controle é feito por meio de mecanismos lógicos e físicos.

C. Diretórios de Rede

As concessões de acesso aos diretórios de rede do TC devem ser de responsabilidades da área de TI e devem ser documentadas e registradas por meio da ferramenta de chamado, onde são aprovadas pelo gestor do colaborador e pelo proprietário do diretório/informação, caso aplicável.

6.2. Revogação de Acesso

A revogação de acesso deve ser realizada imediatamente após o desligamento do colaborador ou transferência de área. A área de Recursos Humanos deve informar a área de TI para que a revogação seja realizada imediatamente. As revogações de acessos devem ter filas especificas de atendimento para assegurar a priorização.

6.3. SENHA

Todos os sistemas, desde que não apresentem limitações técnicas, devem ser configurados para que exijam senhas conforme os critérios, mínimos, abaixo:

I – Contenha no mínimo 6(seis) e no máximo 12(doze) caracteres;

II – Seja complexa e tenha no mínimo: 1 (uma) letra maiúscula, 1 (uma) letra minúscula, 1 (um) caractere especial ou 1 (um) número;

III – Expire a cada 60 (noventa) dias, sendo permitido, no máximo, 90 dias;

IV – Seja bloqueada caso haja mais de 3 (três) tentativas de acesso inválida;

VI – Seja passível de desbloqueio a partir da confirmação da identidade do usuário (exemplo: confirmação de dados pessoais, cadastrais signo e/ou de operações), se possível com ligação gravada; e

VII – Todo armazenamento deve ser de forma criptografada, não sendo permitido gravar ou armazenar on-line, no browser.

VIII – Possuir 2FA em todos os sistemas e softwares, aplicações, banco dados etc. do TC.

7. CONTROLE DE ACESSO

7.1. ACESSO FÍSICO

O acesso às informações e aos ambientes físicos do TC deve ser permitido apenas às pessoas autorizadas, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação;

7.2. Acesso Lógico

O acesso às informações e aos ambientes tecnológicos deve ser permitido apenas às pessoas autorizadas pelo proprietário da informação, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação. O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

I – A utilização de identificadores individualizados, monitorados e passíveis de bloqueios e restrições (automatizados e manuais);

II – A remoção de autorizações dadas a usuários afastados ou desligados, ou ainda que tenham mudado de função;

III – A revisão, mínima trimestral, das autorizações concedidas.

8. Controles de Segurança Cibernética

8.1. Gestão de Incidentes de Segurança da Informação

O comportamento de possíveis ataques devem ser identificado por meio de controles de detecção implementados no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, Antivírus, Antispam, entre outros.

Os alertas devem ser gerados e registrados por meio da ferramenta de registro de incidentes e, posteriormente, deve ser seguido o fluxo do processo de resposta a incidentes.

8.2. Notificação de Incidentes

Os alertas de possíveis incidentes de Segurança da Informação devem ser notificados para os Diretores de Segurança da informação e de Tecnologia da Informação.

8.3. Prevenção a Vazamento de Informações

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados, vazados, adulterados ou destruídos sem autorização por usuários não autorizados.

Os principais objetivos do controle devem ser:

I – Monitoramento e controle das atividades de *endpoints* (computadores, notebooks, ou qualquer outro dispositivo);

II – Monitoramento e controle do fluxo de entrada e saída de dados da rede corporativa e softwares; e

III - Proteção dos dados à medida que se movem (transferências e compartilhamentos autorizados).

8.4. Testes de Intrusão

Os Testes de Intrusão devem ser internos e externos nas camadas de rede e as aplicações devem ser realizados, no mínimo, semestralmente. O teste na camada de rede deve incluir os componentes que suportam as funções de rede e aplicações/sistemas operacionais.

8.5. Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas de forma tempestiva e priorizadas de acordo com seu nível de criticidade.

8.6. Comunicação de Incidentes

A área de SI deve, tempestivamente, comunicar à Comitê de Segurança da Informação e aos órgãos de administração a ocorrência de incidentes relevantes que afetem seus sistemas críticos e tenham impacto significativo sobre os clientes.

Esta comunicação deve incluir:

I – A descrição do incidente, indicando de que forma os clientes foram afetados;

II – Avaliação sobre o número de clientes potencialmente afetados;

III – Medidas já adotadas pelo intermediário ou as que pretende adotar;

IV – Tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e

V – Qualquer outra informação considerada importante

8.7 DOCUMENTAÇÃO E RELATÓRIO DE INCIDENTES

O Comitê de Segurança da Informação deve documentar todos os incidentes em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, gerando relatório anual sobre a implementação do plano de ação e de resposta a incidentes nos moldes da regulação da CVM.

9. CONTROLE CONTRA SOFTWARE MALICIOSO

Todos os ativos (computadores, servidores, aplicações etc.) que estejam conectados à rede corporativa ou façam uso de informações do TC, devem ser protegidos com uma solução *anti-malware* determinada pela área de Segurança da Informação. Não é permitido que os usuários removam, desabilitem, alterem as configurações ou instalem outro programa de *anti-malware* em computadores conectados à rede corporativa.

10. CRIPTOGRAFIA

Toda solução de criptografia utilizada no TC deve seguir as regras de Segurança da Informação. O acesso às chaves criptográficas deve ser restrito aos colaboradores

responsáveis, conforme a necessidade de negócio. As chaves criptográficas devem ser armazenadas de maneira segura (criptografadas) e na menor quantidade de locais possíveis.

11. RASTREABILIDADE

Trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir os seguintes eventos:

I – Autenticação de usuários (tentativas válidas e inválidas);

II – Acesso a informações; e

III – Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

Os registros de eventos devem conter pelo menos as seguintes informações:

I – Identificação do usuário;

II – Tipo de evento;

III – Data e hora do evento;

IV – Resultado do evento (sucesso ou falha);

V – Local de origem do evento; e

VI – Nome de informações, componentes do sistema ou recursos afetados.

Todos os registros de eventos devem ser armazenados em um local central ou mídia protegida contra acesso não autorizado. Este repositório deve possuir mecanismos de controle de acesso, segregação física e/ou segregação de rede de modo a impedir o acesso e possível alteração por pessoas não autorizadas e com período mínimo de retenção de 5(cinco) anos

12. GUARDA E DESLOCAMENTO DE INFORMAÇÕES

É vedado o compartilhamento de dados, pastas, e quaisquer informações constantes no diretório do TC. Os dados devem permanecer armazenados no Google Drive compartilhado de cada área que deve ser acessível em https://drive.google.com/drive/u/1/shared-drives e file servers específicos de cada área, de acordo com a necessidade.

Todas as informações que necessitam ser armazenadas em suporte físico ou digital, quando da sua guarda pelo colaborador, devem respeitar os seguintes cuidados, de acordo com a classificação da informação:

I – Suporte físico: Todos os documentos contendo Informações Internas, Confidenciais e Secretas (“Informações Protegidas”) devem ser armazenados em arquivos físicos próprios indicados pelo TC, de acordo com os métodos identificação do conteúdo, incluindo sua data de arquivamento.

Documentos utilizados pelo colaborador em sua estação de trabalho, quando não estiverem sendo utilizados, devem sempre ser guardados em gaveta ou armário com chave, garantindo que permaneçam trancados quando se tratar de informações confidenciais e secretas.

Nenhuma anotação relacionada às Informações Protegidas deve ser deixada à mostra, seja em cima da mesa, do computador ou em divisórias, mesmo quando o colaborador estiver presente. Quando o Colaborador não estiver nas dependências da empresa, os documentos contendo Informações Protegidas não devem, em hipótese alguma, ficar expostos. Caso haja necessidade de necessidade de transporte dos documentos, o colaborador deve garantir que seu conteúdo não esteja aparente, por meio da utilização de pastas opacas e, caso o documento seja retirado dos arquivos físicos, deve solicitar autorização do responsável para o seu arquivamento e registro do respectivo deslocamento.

II – Suporte digital: Todo e qualquer arquivo que contenha Informações Protegidas deve ser salvo na rede corporativa do TC, em diretório específico, que

inviabilize o acesso por colaboradores não autorizados e conforme previsão da matriz de segregação. Os arquivos devem ser salvos de forma a identificá-los quanto ao seu conteúdo e data de criação. Caso o arquivo deva ser armazenado em dispositivo móvel (como, por exemplo, em notebooks, por conta de reuniões externas), é indispensável que o Colaborador remova o arquivo do dispositivo após a sua utilização.

Todo e qualquer documento ou arquivo que contenha Informações Protegidas somente poderá ser movimentado se houver a possibilidade de recuperação ou análise dos registros de tal arquivo ou documento em caso de falhas de segurança que acarretem a perda ou o extravio das Informações Protegidas. Sempre com autorização da governança competente.

13. DESCARTE DE INFORMAÇÕES

O descarte de um documento físico e/ou a exclusão de um arquivo digital da rede do TC que contenha Informações Protegidas deve seguir as seguintes regras de descarte:

I – Suporte físico: Os documentos que possuírem Informações Públicas poderão ser descartados no lixo comum; já aqueles que possuírem Informações Protegidas devem ser destruídos manualmente ou, preferencialmente, por um aparelho fragmentador antes do descarte. No caso de Informações Secretas, o uso de aparelho fragmentador é obrigatório.

Na ausência de um aparelho fragmentador ou quando houver um grande volume de documentos a ser destruído, o colaborador deve deverá acionar o gestor responsável, que por sua vez, irá promover descarte adequado.

II – Suporte digital: Arquivos que contenham Informações Protegidas e estejam armazenados em suporte digital flexível deverão ser destruídos por meio de aparelho fragmentador.

Na ausência de um aparelho fragmentador ou quando houver um grande volume de suporte digital flexível a ser destruído, o colaborador deverá acionar o gestor responsável, que por sua vez, deve promover o descarte adequado, conforme regra.

Em se tratando de arquivos armazenados em suporte digital rígidos, como HD e pen drive, estes devem ser encaminhados à área de Segurança da Informação, em caixa lacrada, para destruição adequada.

Somente o responsável pela geração ou armazenamento do arquivo, ou do documento a ser descartado, tem competência para descartá-lo ou deletá-lo. Ainda, todo descarte deve ser registrado, a fim de manter um histórico que possibilite a realização de auditorias, caso necessário.

14. SEGMENTO DE REDES

Todas as regras de comunicação nos dispositivos de segurança e ativos de rede devem ser aprovadas de acordo com os critérios estabelecidos pela área de Segurança da Informação.

Para solicitação de alteração de uma nova regra de comunicação para os ativos da rede, a área requisitante deve enviar uma solicitação à área de Segurança da Informação.

Para solicitação de acesso aos dispositivos de rede, a área de Segurança da Informação deve analisar a topologia de rede, os protocolos e os riscos para o ambiente, podendo aprovar ou não. Essa análise deve ser baseada na arquitetura, segmentação e topologia de rede definida pela área de TI.

14.1. REDE CORPORATIVA

Para assegurar a eficiência e segurança da Rede Corporativa:

I – Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;

II – Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;

III – A área de TI deve manter um controle de ativos de rede atualizado, fornecendo-o à Segurança da Informação, quando solicitado;

IV – A área de TI deve realizar, periodicamente, revisões nas regras existentes nos firewalls e ativos de rede do TC; e

V – Para solicitação de criação, alteração e exclusão devem ter de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de Segurança da Informação, que deve a análise e aprovação, enviando para que seja executada pela área de TI.

14.2. Cópias de Segurança (Backup)

Para proteção das informações e dos arquivos digitais, cópias de segurança das informações poderão ser geradas e armazenadas pela área de TI em local apropriado e definido pela área de Segurança da Informação, e lá devem permanecer disponíveis caso seja necessária a restauração de quaisquer dessas informações (“Backup”). O Backup deve ser realizado considerando informações críticas utilizadas nas operações do TC e de acordo com a periodicidade e os procedimentos definidos pela área de Segurança da Informação.

O colaborador poderá solicitar à área de TI a restauração de informações relacionadas às atividades profissionais por ele desenvolvidas no âmbito de sua relação com o TC. Para tanto, deve encaminhar um pedido para a área de TI, que somente deve fazer a restauração e liberar o acesso ao colaborador, após aprovação da área de Segurança da Informação. A existência de Backup não significa que o colaborador tem autorização para excluir ou corromper arquivos armazenados na infraestrutura técnica do TC.

É vedado aos colaboradores armazenar arquivos pessoais, bem como realizar backups das informações do TC em dispositivos de mídia removíveis que possam estar conectados ao computador. A utilização de dispositivos de armazenamento somente

deve ser permitida se justificada e aprovada pela área de Segurança da Informação, mediante a assinatura de um Termo de Responsabilidade pelo colaborador e monitoramento do processo.

O período de retenção das cópias de segurança deve levar em consideração o tipo de informação armazenada e as disposições previstas na legislação sobre o assunto, sendo responsabilidade da área de Segurança da Informação verificar estes requisitos e instaurar os procedimentos, seja como a forma de organização dos documentos guardados, formas de exclusão, entre outros.

15. GESTÃO DE ATIVOS DE TI

O processo de gestão de ativos de TI deve ser estabelecido e documentado, em sistema interno, garantindo que sejam gerenciados e monitorados.

O processo de gestão de ativos deve levar em consideração o ciclo de vida do ativo:

I. **Planejamento:** Alinhamento da estratégia corporativa com as ações de TI. Nessa fase é observado a revisão dos ativos que são utilizados, análise de custos de compra e instalação dos novos ativos;

II. **Aquisição:** Definição do padrão técnico, fornecedores e acordos contratuais;

III. **Implantação:** Configuração e instalação técnica seguindo os padrões estabelecidos anteriormente;

IV. **Gerenciamento:** Controle de inventário, apoio técnico, manutenção, atualização e monitoramento desses ativos;

V. **Descarte:** Processo realizado quando um bem perde sua utilidade e torna-se antieconômico.

16. Uso Aceitável dos Ativos de Informação

Os colaboradores devem seguir as diretrizes formalizadas para uso, armazenamento e compartilhamento de informações do TC, de tal forma a zelar pela confidencialidade, de acordo com a classificação da informação, proteger contra vazamento e compartilhamento indevido.

O uso de equipamentos fornecidos pelo TC é permitido e encorajado desde que seu uso seja apropriado a atividade e fins do negócio do TC.

É estritamente proibido e inaceitável:

I – Sigam a legislação corrente (sobre pirataria, pedofilia, ações discriminatórias etc.);

II – Não criem riscos desnecessários para os equipamentos, informações ou para o negócio;

II – Atacar e/ou pesquisar em áreas não autorizadas (Hacking);

IV – Executar atividades que desperdice os esforços do pessoal técnico ou dos recursos da rede;

VI – Introduzir de qualquer forma um vírus de computador dentro da rede corporativa; e

VII – Monitoramento.

17. Uso do Correio Eletrônico (E-mail)

O uso do e-mail corporativo do TC é individual. O usuário é responsável por toda mensagem enviada pelo seu endereço. É proibido o envio de mensagens pelo e-mail corporativo que:

I – Contenha linguagem ofensiva, hostil, ou de qualquer forma, inapropriada;

II – Seja relativa a conteúdo pornográfico;

III – Possa prejudicar a imagem do TC (ou de qualquer outra organização); e

IV – Seja incoerentes com as políticas do TC.

18. Ciclo de Desenvolvimento ou Atualização de Sistemas

O ciclo de desenvolvimento de sistemas deve contemplar os seguintes requisitos mínimos de segurança da informação:

I – Definição de requisitos de segurança para novas demandas que impactarem ambientes críticos;

II – Adoção de boas práticas para desenvolvimento seguro;

III – Segregação lógica dos ambientes de desenvolvimento, teste/homologação e produção;

IV – Segregação de função no processo de desenvolvimento, teste e homologação e produção;

V – Todo código-fonte desenvolvido, e obrigatoriamente anterior a sua implantação, deve passar por análise e validação de segurança através do uso de ferramenta específica para descoberta de possíveis falhas de vulnerabilidade; e

VI – Inventário, controle e gerenciamento seguro de APIs.

19. Gestão de Mudanças

O processo de gestão de mudanças deve assegurar que todas as solicitações sejam registradas, analisadas, autorizadas, priorizadas, planejadas, testadas, implementadas, documentadas e revisadas, através da ferramenta Confluence.

É dever de cada time/squad/tribo realizar o registro das mudanças realizadas no sistema.

O processo de gestão de mudanças deve levar em consideração as seguintes informações do Plano de Mudança:

I. **Classificação da mudança:** Simples, complexa ou emergencial;

II. **Impactos da mudança:** Possíveis consequências da implantação da mudança;

III. **Plano de mudança:** Atividades a serem executadas para implementar a mudança;

IV. **Plano de reversão:** Atividades a serem executadas para desfazer a mudança e voltar ao estado inicial do processo;

V. **Aprovadores:** Revisores e aprovadores do Plano de Mudanças.

20. ACESSO REMOTO

Todos os colaboradores que tenham acesso a informações privilegiadas devem ter acesso apenas pelo notebook corporativo, estando conectado a uma VPN.

Para assegurar o monitoramento de acesso de informações, deve ser necessário habilitar *Remote Access Monitoring* em todos os aparelhos corporativos.

O acesso remoto a ativos de informação deve possuir controles de autenticação e criptografia provendo identificação por meio da combinação de dois componentes distintos (autenticação via usuário de rede e token).

A requisição de acesso remoto deve ser realizada pelo colaborador por meio da ferramenta de chamados.

A solicitação deve conter as seguintes informações:

I – Sistema(s) para o qual deseja-se obter o acesso;

II – IP do computador;

III – IP do Servidor/Aplicação; e

IV – Justificativa.

O usuário somente deve ter o acesso liberado após preenchimento e aprovação da governança. Esse tipo de acesso deve passar por revisões, mínimas trimestrais e os acessos devem ser revogados após três meses de inatividade.

Deve ser utilizado software disponibilizado pelo TC com as configurações recomendadas e a autenticação para o acesso deve ser necessariamente por meio de senhas, não sendo permitido o acesso simultâneo para o mesmo usuário.

21. Recuperação de Desastre e de Continuidade dos Negócios

O processo de recuperação de desastre e de continuidade de negócios deve ser implementado com o intuito de reduzir os impactos e perdas de ativos da informação após possível incidente crítico, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos

São diretrizes do programa de Continuidade de Negócios:

I – Estabelecer os objetivos, metas, controles, processos e procedimentos relevantes para melhorar a Continuidade de Negócio e obter resultados alinhados com as políticas e objetivos estratégicos do TC;

II – Identificar e garantir a aplicação dos requisitos legais e regulatórios para o TC previstos nas instruções, regulamentações, dentre outros;

III – Realizar testes anuais de mesa e simulações de desastre que garantam a manutenção da continuidade, bem como o funcionamento do plano de continuidade do TC;

IV – Revisão anual (ou a partir de mudança relevante) de toda a documentação pertinente a Gestão de Continuidade de Negócios;

V – Analisar o impacto da interrupção das atividades do TC ao longo do tempo, determinar os seus tempos de recuperação e identificar as atividades críticas e recuperá-las em um nível e tempo aceitáveis;

VI – Assegurar que todos os profissionais compreendam suas responsabilidades perante a Continuidade de Negócios, por meio da realização de treinamentos e conscientização sobre o tema;

VII – Desenvolver estrutura de gerenciamento e resposta a crises, suportada por níveis adequados de autoridade e competência, que assegurem a comunicação efetiva às partes interessadas;

VIII – Estabelecer papéis e responsabilidades das partes envolvidas;

IX – Identificar e avaliar os terceiros que exercem função crítica na cadeia de valor e colaboração do processo de negócio;

X – Assegurar a revisão periódica do desempenho do Sistema de Gestão de Continuidade de Negócio e a implementação de ações corretivas e de melhoria;

XI – Adotar práticas de mitigação de risco adequadas à dimensão das ameaças e à extensão de seus possíveis impactos;

XII – Estabelecer a identificação de práticas para retomada de serviços e mitigação do risco operacional em processo formal de análise de impacto no negócio; e

XIII – Preservar a integridade física das pessoas.

22. PRIVACIDADE DE DADOS PESSOAIS

Esta Política obedece à Lei de Proteção de Dados Pessoais, bem como a Política de Governança de Dados do TC, no que tange ao tratamento e o controle de dados pessoais em meio eletrônico, especialmente, como deve ser realizado esse

tratamento, desde a coleta dos dados até o seu descarte. Sempre importante relembrar que, como Controlador de Dados, as diretrizes de privacidade de dados do TC são planejadas para garantir a segurança, a integridade, e o adequado tratamento dos dados pessoais durante a execução dessas atividades, especialmente no que tange a identificação de clientes, suas operações e posições de custódia, compreendidos como dados sensíveis.

Em casos de incidente de segurança envolvendo dados pessoais, o Encarregado de Dados deve ser notificado imediatamente para que proceda, junto a área de Segurança da Informação, todos os procedimentos de contenção e informar, caso seja necessário, o Jurídico e o Comitê de Segurança da Informação.

23. Treinamento, Atualização e Divulgação

O TC conta com programas de treinamento e conscientização periódicos de seus colaboradores.

O programa é vivo e se adequa periodicamente às necessidades identificadas no monitoramento das situações e interações com os colaboradores. Assim como esta Política, é amplamente divulgado e disponibilizado aos novos colaboradores e, sempre que atualizado, é informado a todos os colaboradores do TC.

24. Aquisição de Novas Plataformas

Todas as aquisições de novas plataformas e/ou softwares devem seguir um fluxo de aprovações e avaliações para contratação, envolvendo a área solicitante, área de Financeiro e a área de Segurança da Informação.
A avaliação de Segurança da Informação deve consistir em verificar enquadramento aos requisitos de Segurança da Informação e Cibernética do Grupo TC.

25. AUDITORIA INTERNA

A auditoria interna deve executar, de forma tempestiva, a execução de avaliação dos controles de Segurança da Informação, elaboração de relatórios com indicações das constatações dos pontos de fragilidade e recomendações para correções e/ou implantação de controles, permitindo que o TC se antecipe e elimine as vulnerabilidades que possam existir no ambiente de infraestrutura.

26. DESCUMPRIMENTO DA POLÍTICA

Na hipótese de violação desta Política, a área de Compliance, em conjunto com o Jurídico e a área de Recursos Humanos, podem determinar sanções de acordo com o Código de Ética e Conduta da Empresa.

27. DISPOSIÇÕES GERAIS

27.1. ALTERAÇÃO

Esta Política deverá ser revisada, no mínimo, anualmente, e poderá ser modificada, emendada ou revogada, a qualquer momento, mediante deliberação e aprovação da Diretoria, principalmente no caso de alteração superveniente nas leis e nos regulamentos a ela aplicados.

27.2. CONFLITO

No caso de conflito entre qualquer item desta Política e do Contrato Social, prevalecerá o disposto neste. E no caso de conflito entre qualquer item desta Política e de leis e regulamentos, prevalecerá o disposto nestes.

27.3. AUTONOMIA

Caso qualquer item desta Política seja considerado inválido, ineficaz ou ilegal, a sua disposição será limitada, sempre e quando possível, para que a validade, eficácia e legalidade dos demais itens não sejam afetados.

27.4. VIGÊNCIA

Esta Política entrará em vigor e será divulgada na data de sua aprovação pela Diretoria.