Política de Segurança Cibernética

A Política de Segurança Cibernética ("Política") tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética, no intuito de minimizar as ameaças à imagem e aos negócios da Cartos.

Deverá, assim, ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A Política está de acordo com as leis, regulamentação e autorregulação aplicáveis de Regulação e Melhores Práticas para a Administração de Recursos de Terceiros, bem como as boas práticas de mercado.

1. Princípios da Segurança dos dados e dos sistemas de informação

O objetivo das regras sobre segurança cibernética é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação devem assegurar:

- a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais)

- a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário)

- a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas).

Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional contratada pertence à Cartos. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da Cartos poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

A Cartos exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

2. Responsabilidade

2.1. Responsável pela Segurança Cibernética

Seguem abaixo uma lista não exaustiva dos deveres e responsabilidades do Responsável pela Segurança Cibernética:

- Testar a eficácia dos controles utilizados e informar os riscos residuais.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política, bem como definir e assegurar a segregação das funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo, eliminando, ou ao menos reduzindo, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, mantendo evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Cartos.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

- Proteger continuamente todos os ativos de informação da Cartos contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Cartos.

- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Cartos, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Cartos.

- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da Cartos operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Cartos.

- Garantir um backup em nuvem, devidamente criptografado com as rotinas de retenção (2 últimas semanas / cabeça de mês / cabeça de ano – por 5 anos).

- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Cartos, mediante campanhas, treinamentos e outros meios de endomarketing.

Caberá a todos os Colaboradores conhecer e adotar as definições da Política de Confidencialidade e Segurança da Informação, bem como da presente Política, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança cibernética, o qual recorrerá ao Responsável pela Segurança Cibernética, se for o caso.

Em caso de incidente que afete a segurança cibernética da Cartos e/ou descumprimento desta Política, o Colaborador deverá comunicar imediatamente ao Responsável pela Segurança Cibernética, diretamente ou por meio do canal apropriado. Em caso de descumprimento, ainda que involuntário, estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei.

3. Identificação/avaliação de riscos (risk assessment)

A Cartos periodicamente, no mínimo uma vez ao ano, deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção. Esse processo será conduzido pela equipe de TI, o qual deverá ser documentado pelo Responsável com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da Cartos e seus riscos de cibersegurança. A Cartos poderá contratar uma empresa terceirizada para tanto, caso o Responsável pela Segurança Cibernética julgue necessário.

Após a condução do referido processo, deverá discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Cartos, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade de o evento acontecer.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, na avaliação inicial:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso (“Phishing”);
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política; ou

4. Ações de prevenção e proteção

A Cartos estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

Todas as informações encontradas nos ambientes da Cartos são tratadas como confidenciais e sigilosas, e as orientações de tratamento encontram-se na presente Política, no capítulo sobre a Política de Confidencialidade e Segurança da Informação e Comunicação com o Público no Manual de Compliance, e no capítulo sobre Código de Ética da Cartos, divulgados para todos os Colaboradores da Cartos, em especial os com acesso às informações e aos sistemas da Cartos, incluindo orientações que definem a maneira pela qual devem usar a tecnologia.

4.1.1. Mensagem Instantânea

A Cartos reconhece que, em determinados casos, a MI pode ser uma fonte valiosa de informação, bem como um método eficiente de comunicação. A Cartos, portanto, permite aos Colaboradores usar o recurso de MI para comunicações relacionadas a suas atividades enquanto as MIs são enviadas e recebidas usando a plataforma designada pela Cartos para tais comunicações. Os Colaboradores são proibidos de usar uma plataforma não designada para enviar e receber MIs relacionadas as atividades de gestão.

4.1.2. Política de Retenção de Comunicações Eletrônicas

A Cartos implantou uma **"Política de Retenção de E-mail"** em que a Cartos tentará reter todos os e-mails e mensagens instantâneas. A Política de Retenção de E-mail da Cartos é composta por diversos fatores:

- O Responsável pela Segurança Cibernética é responsável pela supervisão da política;
- Os Colaboradores devem abster-se de conduzir suas atividades por meio de qualquer rede de comunicação não pré-aprovada pela Cartos (p.ex., e-mail externo, mensagem instantânea ou mensagem de texto não fornecido pela Cartos ao Colaborador ou que não possa ser capturado pelo sistema de retenção de e-mail);
- Todas as comunicações eletrônicas contempladas pelas exigências aplicáveis de manutenção de registro estão identificadas e preservadas da forma adequada;
- O descarte permanente de e-mails da rede da Cartos deve ser conduzido de uma forma que proteja a confidencialidade, mediante prévia aprovação do Responsável pela Segurança Cibernética; e
- O treinamento sobre a Política de Retenção de Comunicações Eletrônicas deve ser dado mediante o início do vínculo com a Cartos e anualmente após isso.

4.1.3. Procedimentos Operacionais

O Responsável pela Segurança Cibernética revisará a Política de Retenção de E-mail, anualmente, para garantir que seus backups estejam funcionando e que a Cartos possa disponibilizar e-mails, caso solicitado por um regulador.

4.1.4. Uso de Ativos

A utilização dos ativos da Cartos, incluindo computadores, telefones, Internet, programas de mensagem instantânea, e-mails e demais aparelhos se destina a fins profissionais, e deve ser feita com cuidado.

Dispositivos Móveis

Considerando que deseja facilitar a mobilidade e o fluxo de informação entre seus Colaboradores, a Cartos permite o uso de seus equipamentos portáteis. Por "dispositivo móvel", entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da Cartos, ou aprovado e permitido pelo Responsável pela Segurança Cibernética, como: notebooks, smartphones e pendrives (mediante prévia autorização/liberação).

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os Colaboradores que utilizem tais equipamentos.

O Colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Cartos, mesmo depois de terminado o vínculo contratual mantido com a Cartos.

É permitido o uso de rede banda larga de locais conhecidos pelo Colaborador como: sua casa, hotéis, fornecedores e clientes. O Colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará que assumiu todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à Cartos e/ou a terceiros.

4.1.5. Uso de e-mail

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Cartos, inclusive que contenha fins políticos locais ou do país (propaganda política). O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente. Em nenhuma hipótese um Colaborador pode emitir uma opinião por e-mail em nome da Cartos, salvo se expressamente autorizado para tanto pelo Diretor de Compliance.

Acrescentamos que é proibido aos Colaboradores o uso de e-mail da Cartos para as seguintes atividades:

- Enviar mensagens (i) não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Cartos; (ii) pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar; (iii) que torne seu remetente e/ou a Cartos vulnerável a ações civis ou criminais; (iv) com informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação e (v) que inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;

- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- Apagar mensagens pertinentes de correio eletrônico quando a Cartos estiver sujeita a algum tipo de investigação.

- Produzir, transmitir ou divulgar mensagem que (i) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Cartos; (ii) contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador; (iii) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança, bem como que vise:

o obter acesso não autorizado a outro computador, servidor ou rede;

o interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado; o burlar qualquer sistema de segurança; o vigiar secretamente ou assediar outro usuário; o acessar informações confidenciais sem explícita autorização do proprietário; o acessar indevidamente informações que possam causar prejuízos a qualquer pessoa; o inclua imagens criptografadas ou de qualquer forma mascaradas;

o contenha anexo(s) superior(es) a 50 MB para envio (interno e internet) e 50 MB para recebimento (internet).

As mensagens de e-mail deverão incluir assinatura com o seguinte formato: (i) nome do Colaborador, Nome da empresa, Disclaimer, Telefone(s) e Correio eletrônico, conforme especificado pela equipe de TI da Cartos.

4.1.6. Uso da Internet

Todas as regras atuais da Cartos visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da Internet. Embora a conexão direta e permanente da rede corporativa com a Internet ofereça um grande potencial de benefícios, também propicia riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na Internet está sujeita a divulgação e auditoria. Portanto, a Cartos reserva-se o direito de monitorar e registrar todos os acessos a ela, nos termos da legislação aplicável. Como mencionado, os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet são de propriedade da Cartos, que pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede/Internet, estejam em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

A visualização de sites, blogs, fotologs e webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física) obsceno, pornográfico ou ofensivo é terminantemente proibida.

Programas licenciados e instalados nos computadores, principalmente via Internet ("downloads"), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do Responsável pela Segurança Cibernética.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado poderá excluído pela equipe de TI. Os Colaboradores não poderão em hipótese alguma utilizar os recursos da Cartos para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional. O download e a utilização de programas de jogos são proibidos.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à Cartos ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados. Os Colaboradores não poderão utilizar os recursos da Cartos para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo superior. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Cartos cooperará ativamente com as autoridades competentes.

4.1.7. Identificação e uso de senhas

Observado o disposto na Política de Confidencialidade e Segurança da Informação, a senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails, que também devem ser acessados via webmail, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

Todos os dispositivos de identificação utilizados na Cartos, como o número de registro do Colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a Cartos e a legislação (cível e criminal).

É também proibido o compartilhamento de login para funções de administração de sistemas. A Área Administrativa da Cartos é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos Colaboradores.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários não possuem perfil de administrador. E as senhas deverão ter pelo menos 8 caracteres, sendo um deles, especial, e são renovadas a cada 180 dias, sendo que a última não poderá ser repetida obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 5 (cinco) tentativas de acesso, a conta do usuário será bloqueada pelos próximos 30 minutos (caso não seja desbloqueada manualmente pelo administrador). Para o desbloqueio é necessário que o usuário entre em contato com a equipe de TI. Caso o Colaborador esqueça sua senha, ele deverá requisitar formalmente a troca, para que a equipe de TI realize o cadastro de uma nova senha. Deverá ser estabelecido um processo para a renovação de senha. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 180 dias, não podendo ser repetida a última senha. Os sistemas críticos e sensíveis para a Cartos e os logins com privilégios administrativos devem e desse prazo máximo. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, conforme previsto na Política de Seleção e Contratação de Colaboradores.

Portanto, assim que algum usuário for demitido ou solicitar demissão, a Área Administrativa deverá imediatamente comunicar tal fato à equipe de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

4.1.8. Conexão na Rede da Cartos

É proibida a conexão de qualquer equipamento na rede da Cartos sem a prévia autorização pelas áreas de informática e compliance.

4.1.9. Controles e Registros de Atividades

A Cartos implementou controles robustos de acesso utilizando duplo fator de autenticação em seu sistema de e-mail e nos sistemas críticos da Cartos (Controle de acesso lógico adequado aos ativos da organização).

4.2. Procedimentos de Segurança Cibernética de Terceiros Contratados

Os Colaboradores externos da Cartos, dentre os quais os seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de cibersegurança. A computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de Colaboradores externos, envolve determinados riscos que devem ser levados em conta pela Cartos, demandando certos cuidados proporcionais a esta identificação de ameaças.

4.2.1. Avaliação dos terceiros contratados

Nesse sentido, a área de Compliance da Cartos deverá verificar o conteúdo mínimo de compliance em segurança cibernética de terceiros que (i) gerem acesso a informações e sistemas confidenciais ou sensíveis, (ii) prestem serviços de computação em nuvem, (iii) tenham conexões lógicas (links) com a Cartos ou (iv) qualquer outros que a área de Compliance julgue que por qualquer motivo possa gerar risco de cibersegurança à Cartos, previamente à sua contratação, na forma do Anexo A a esta Política.

O resultado será encaminhado ao Responsável pela Cibersegurança para avaliação da capacidade deles de evitar ataques cibernéticos e da potencial contratação, devendo a decisão sobre a contratação ficar formalizada, sendo periodicamente reavaliada.

4.2.1. Requisitos de segurança da informação nos contratos com terceiros

A Cartos deverá incluir em contratos com Colaboradores externos requisitos de segurança da informação nos contratos de prestação de serviços, bem como verificar a efetividade dos controles implementados pela empresa contratada para atender aos requisitos durante a vigência do contrato, na forma menciona acima.

5. Plano de Resposta a Incidentes

Os Colaboradores poderão reportar incidentes diretamente ao Responsável pela Segurança Cibernética ou por meio do canal de reporte de incidentes: **E-mail: canaldenuncia@cartos.com.br**

5.1. Procedimento em caso de incidente

Uma vez que o Responsável pela Segurança Cibernética tenha sido acionado devido a um potencial incidente, este deverá se reunir com o TI.

Avaliação Inicial

Nessa etapa inicial, aspectos e decisões fundamentais deverão ser analisadas pelo Comitê e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.

Incidente Caracterizado

Se for caracterizado um incidente, devem os membros do Comitê tomar as medidas imediatas, que poderão abranger se (i) será registrado um boletim de ocorrência ou queixa crime, (i) é necessário envolver consultor ou advogado externo; (iii) haverá comunicação interna ou externa, em especial a Investidor que tenha sido afetado. Além disso, o Comitê, em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

Recuperação

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um acompanhamento, conforme o caso, em periodicidade a ser definida, com um sumário elaborado pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos.

Também deverá se avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações, tais como manifestação pública na mídia, com eventual contração de PR, enquanto o Comitê verificará se todas as informações necessárias ao portfólio estão seguras e a área de gestão definirá se decisões de investimento são requeridas. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Cartos, devem ser comunicados ao Comitê. Colaboradores externos relevantes deverão ser mantidos atualizados.

6. Reciclagem e revisão

A Cartos deverá manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Também realizará campanha de conscientização em cibersegurança, com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger as informações como parte de suas responsabilidades por meio do Programa de Treinamento da Cartos.

O Responsável pela Segurança Cibernética, realizará a revisão e atualização desta Política periodicamente, no mínimo anualmente ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Responsável pela Segurança Cibernética.