Política Corporativa de Segurança Cibernética

Sumário Executivo

Esta Política estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando atender as disposições da Resolução CMN n° 4.893 do Banco Central do Brasil.

Política Corporativa de Segurança Cibernética

ÍNDICE

Política Corporativa de Segurança Cibernética

1. OBJETIVO

Estabelecer as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

a) Proteger o valor e a reputação da empresa;
b) Garantir a confidencialidade, integridade e disponibilidade das informações do Grupo Travelex Confidence, e de informações de terceiros por ele custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
c) Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;
d) Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
e) Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
f) Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias;
g) Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

2. ABRANGÊNCIA E APLICABILIDADE

A presente Política abrange os aspectos relativos à segurança da informação e controles sobre Riscos Cibernéticos, envolvendo tecnologias, processos, pessoas e instalações físicas, sendo aplicada a todas as áreas, colaboradores e prestadores de serviço das empresas do Grupo Travelex Confidence, formado pelo Travelex Banco de Câmbio S.A. e Confidence Corretora de Câmbio S.A. ("Grupo Travelex Confidence").

3. CONCEITOS

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.
Integridade: salvaguarda da exatidão e completeza 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.

Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets, ransomware), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

Malwares:

a) Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
b) Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
c) Spyware: software malicioso para coletar e monitorar o uso de informações;
d) Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

Engenharia Social:

a) Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
b) Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
c) Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
d) Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
e) Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes Externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

4. PRINCÍPIOS

A proteção e privacidade de dados dos clientes refletem os valores do Grupo Travelex Confidence e reafirmam o seu compromisso com a melhoria continua da eficácia do processo de Proteção de Dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

a) São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
b) Somente serão acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;

c) Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
d) As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

5. DIRETRIZES CORPORATIVAS

O cumprimento da Política Corporativa de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer às seguintes diretrizes:

a) Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
b) Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
c) Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pelo Grupo Travelex Confidence;
d) Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
e) Garantir a continuidade do processamento das informações críticas de negócios;
f) Atender às leis que regulamentam as atividades do Grupo Travelex Confidence e seu mercado de atuação;
g) Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
h) Comunicar imediatamente à área de Segurança Cibernética, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

6. ESTRUTURA DE GERENCIAMENTO

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela Política Corporativa de Segurança Cibernética.

6.1 Gestão de acessos às informações

Os usuários de rede criados, bem como os computadores conectados à rede, são autorizados, autenticados e identificados pelo serviço de banco de dados estruturado Active Directory (Microsoft), que armazena informações sobre objetos em rede (contas de usuários, contas de serviços, computadores, grupos de e-mail e de segurança).

A equipe de Segurança Cibernética é responsável pelo processo de criação e desativação dos logins de acesso à rede, mesmo se o processo for executado por outra área operacional (por exemplo TI), e somente poderá desativar o login de um funcionário do Grupo Travelex Confidence, após confirmação da demissão pelo RH ou através da solicitação formal do gestor mediato ou imediato do funcionário.

Para a criação de logins de prestadores de serviços (terceiros), a solicitação deverá partir do gestor responsável pelo projeto onde estará alocado o prestador de serviço. O gestor

responsável deverá informar mensalmente à Segurança Cibernética, o término do trabalho de cada prestador, para que seja desativado o seu login de rede.

As senhas dos usuários dos sistemas, bancos de dados e de rede são individuais, sigilosas e intransferíveis, não devendo ser divulgadas em nenhuma hipótese. O usuário é responsável por manter sua senha em sigilo, monitorar sua conta e comunicar imediatamente à equipe de Help Desk, em caso de suspeita de seu comprometimento.

Os acessos às informações em sistemas e bancos de dados do Grupo Travelex Confidence, são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, bem como cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

As regras para concessão e revisão periódica de acessos são aplicadas para todos os sistemas controlados pela área de Segurança Cibernética e todos os sistemas que necessitem da criação de login no banco de dados para o acesso direto.

6.2 Utilização de Correio Eletrônico e Navegação Web

Cada usuário é responsável pelo conteúdo armazenado e enviado através de sua conta de correio eletrônico.

O Grupo Travelex Confidence reserva o direito de monitorar e interferir no tráfego de mensagens, com o propósito de verificar o cumprimento dos padrões de segurança, sempre que julgar necessário.

É proibido o envio ou encaminhamento de mensagens do tipo "corrente" e "spam". É proibida a utilização de listas e/ou caderno de endereços da empresa para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão.

Informações confidenciais não devem, em hipótese alguma, ser enviadas por correio eletrônico sem que haja alguma forma de proteção contra vazamento e alteração.

O acesso ao e-mail corporativo através de aparelho celular, somente será permitido após aprovação da área de Segurança Cibernética.

Todo acesso internet é efetuado através de filtro apropriado que restringe o acesso a sites não permitidos pela área de Segurança Cibernética.

Todos os acessos à internet efetuados pelos usuários, são passíveis de monitoramento.

A concessão de acesso a sites bloqueados será efetuada somente após a análise e aprovação da área de Segurança Cibernética.

6.3 Controle sobre o uso de privilégios administrativos

São estabelecidas regras para padronizar e regulamentar a utilização de contas com privilégios administrativos (administradores de domínio, administrador local, administrador de banco de dados, usuário de sistema).

O privilégio administrativo para uma conta poderá somente ser concedido mediante a análise e aprovação da área de Segurança Cibernética.

Os colaboradores da empresa que possuírem o privilégio de administrador, somente poderão acessar local ou remotamente as estações/servidores que foram designadas para sua responsabilidade.

Para os acessos local ou remoto às estações/servidores, o colaborador deverá somente se conectar utilizando-se de seu próprio login de rede. Não é permitido o uso de "contas de serviço" para o login em servidores.

As contas de serviço que possuírem o privilégio de administrador do domínio, devem possuir a dupla custódia da senha, entre a área responsável e Segurança Cibernética.

É expressamente proibida a criação de logins de rede ou contas de serviço sem a autorização da área de Segurança Cibernética, bem como desativar, pausar ou desligar qualquer recurso de monitoração de segurança e rastreabilidade da informação, incluindo logs de acessos e de auditoria, exceto com autorização formal da área de Segurança Cibernética.

6.4 Classificação da Informação

O Grupo Travelex Confidence estabelece o processo de classificação da informação para apoiar a determinação das necessidades, das prioridades e do nível de segurança quando do tratamento das informações da empresa, abrangendo todo o seu ciclo de vida e em qualquer meio armazenamento ou comunicação.

A classificação e os controles de proteção, associados para a informação, devem levar em consideração as necessidades do negócio para compartilhar ou restringir a informação bem como os requisitos legais. Outros ativos além dos ativos de informação também devem ser classificados de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo.

Todas as informações da empresa devem ter um proprietário designado. O proprietário das informações é uma pessoa que tem responsabilidade autorizada para controlar sua criação, cessão de direitos, armazenamento, transporte, uso, retenção e descarte. O termo proprietário não significa que a pessoa tenha realmente qualquer direito de propriedade da informação.

Todas as informações devem ser identificadas e devem ter um proprietário responsável e a este caberá determinar a sua classificação, bem como executar análise crítica. O proprietário da informação pode definir controles de segurança adicionais, caso julgue necessário.

O Grupo Travelex Confidence estabelece 4 (quatro) categorias para a classificação da Informação (Confidencial, Restrito, Dados Pessoais e Público), as quais são baseadas nos critérios de Confidencialidade, Integridade e Disponibilidade.

Confidencial	São dados que podem causar um nível significativo de risco e impacto para a organização, suas afiliadas ou clientes se tais informações forem acessadas indevidamente, perdidas, alteradas ou tornadas públicas de qualquer forma.
Restrito	Dados restritos significam informações não pessoais que não são aprovadas para circulação geral fora da organização, onde a divulgação não autorizada, alteração ou destruição dos dados pode resultar em um nível moderado de

	risco ou impacto para a organização, suas afiliadas ou clientes. Não deve ser visto ou acessível a partes externas, a menos que seja aprovado pelo Proprietário dos Dados.
Dados Pessoais	Informação que permite identificar, direta ou indiretamente um indivíduo como Nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização, fotografia, dados do cartão bancário, renda, entre outras.
Público	Dados públicos são informações de domínio público que foram aprovadas para comunicação externa em que a divulgação, alteração ou destruição de dados resultaria em pouco ou nenhum risco para a organização, suas afiliadas ou clientes.

6.5 Inventário e controle de ativos (hardware e software)

Todos os ativos internos associados às informações e com recursos de processamento da informação devem ser identificados, possuir um responsável, mantido em um repositório com revisão periódica, bem como definida a classificação da informação sobre o ativo identificado.

Toda e qualquer aquisição de um novo software ou serviço, incluindo aqueles de armazenamento e computação em Nuvem, deve ser antes analisada pela área de Segurança Cibernética, a fim de se apurar os requisitos de *baseline* para segurança da informação e riscos cibernéticos.

6.6 Configuração segura de hardware e software em dispositivos móveis, desktops e servidores

São definidos procedimentos para aplicação de atualizações de segurança nos sistemas operacionais dos servidores e estações, bem como a atualização de versões dos equipamentos de infraestrutura de segurança e de rede, com o objetivo de prevenir e/ou responder aos incidentes de segurança.

Devem ser estabelecidas regras para especificação dos requerimentos mínimos de configurações dos servidores e estações de trabalho, visando garantir a segurança da informação.

a) Configuração segura de servidores

O local onde estão dispostos os servidores do Grupo Travelex Confidence, deve possuir controle de segurança física quanto à localização, cabeamento, controle de temperatura, rede elétrica e combate ao incêndio. O acesso deve ser restrito aos administradores e pessoas autorizadas. A entrada e saída de pessoas não pertencentes aos ambientes críticos, devem ser registradas e arquivadas de modo a permitir auditorias periódicas.

A administração do servidor deve ser realizada mediante sessões autenticadas por usuário e senhas.

O acesso remoto ao servidor deverá ser realizado por meio de ferramentas homologadas pela área de Segurança Cibernética e restrito às máquinas que realizam esta função na rede de gerenciamento.

O servidor deverá estar com o seu sistema de log e/ou alertas habilitados. Os logs não devem ser apagados sem a autorização foram da área de Segurança Cibernética.

O uso do servidor é restrito às atividades relacionadas aos negócios/serviços do Grupo Travelex Confidence, no sentido de manter os níveis altos de produtividade, disponibilidade e atualização tecnológica e de segurança.

Devem ser aplicados mecanismos de monitoramento de capacidade de memória, disco e comunicação com a rede e segurança, com o objetivo de prevenção e respostas aos incidentes.

Qualquer alteração de configuração deverá ser avaliada, homologada, aprovada e documentada pela área de TI.

b) Configuração segura de desktops (estações de trabalho)

A instalação física das estações de trabalho deve ser executada exclusivamente pela área de TI ou por empresas autorizadas formalmente.

O gabinete (CPU) somente deverá ser aberto por pessoa autorizada para manutenção ou atualização. Todas as estações devem possuir identificação de patrimônio do Grupo Travelex Confidence.

Os administradores locais das estações de trabalho devem ser analistas da equipe de suporte da área de TI, administradores do domínio ou pessoas autorização pela área de Segurança Cibernética e pela gerência solicitante.

Todas as estações de trabalho devem receber e aplicar corretamente as políticas de grupo (GPO) do Active Directory, homologadas pela área de TI e de Segurança Cibernética e somente aplicadas pela área de TI. Em caso de exceção, deve-se aplicar uma política local em cada estação, seguindo o padrão do domínio.

c) Configuração segura de notebooks

O uso do computador móvel é restrito às atividades relacionadas com os negócios/serviços do Grupo Travelex Confidence.

O usuário do computador móvel deverá assinar Termo de Custódia do computador móvel, declarando-se responsável pelo equipamento e seus dados.

O computador móvel deverá possuir etiqueta de identificação de patrimônio do Grupo Travelex Confidence.

Para os computadores móveis de colaboradores que com certa frequência utilizam o equipamento em ambiente externo, deve ser aplicado o mecanismo de criptografia de disco rígido para a proteção das informações.

Deve ser aplicado um sistema de firewall local que filtre os pacotes na interface wireless.

É proibida a instalação de outro software de antivírus que não seja o que foi disponibilizado e configurado pela área de TI do Grupo Travelex Confidence.

O software de antivírus corporativo deve estar atualizado sempre com a última versão disponibilizada. O serviço de antivírus do notebook, em hipótese alguma, poderá ser interrompido.

O compartilhamento de conexão com a internet, via wireless, deve ser bloqueado.

6.7 Controle de Comunicações de Redes

a) Classificação das zonas

As redes devem ser classificadas em quatro zonas de confiança que refletem os níveis de controle aplicados ao segmento de rede, aos sistemas e plataformas conectadas a estas:

- *Não confiável* – deve abranger todos os sistemas e serviços não controlados pela empresa, incluindo parceiros de negócios e redes públicas;
- *Intermediária* – deve abranger todas as redes e dispositivos utilizados para interagir com o ambiente não confiável, incluindo DMZ e servidores de acesso público;
- *Confiável* – devem ser consideradas nesta zona todas as redes internas (LAN/MAN), bem como os servidores não críticos e desktops de usuários internos;
- *Restrita* – deve abranger os sistemas/servidores de alta criticidade para o negócio da empresa.

b) Controle das comunicações

As comunicações de rede e entre zonas devem ser controladas por dispositivos de controle de segurança (firewalls, servidores Proxy, filtros de pacote e concentradores de VPN) posicionado na fronteira entre estas, em ordem de realizar o controle adequado.

Os Firewalls devem ser dispositivos híbridos com capacidade de realizar controle de comunicações baseados em *deep packet inspection* aplicados na comunicação entre a Zona Não Confiável e a Intermediária bem como servir como Proxy de aplicações para comunicação entre as zonas Intermediária e Confiável.

As regras de controle de comunicações devem ser aplicadas para os seguintes casos:

i. Parceiros acessando aplicações da empresa através de VPN;
ii. Parceiros/Usuários/Funcionários remotos acessando serviços através de interface WEB a partir de um browser;
iii. Funcionários Remotos acessando aplicações da empresa por meio de VPN (Virtual Private Network) através de dispositivo governado pela área de TI. Neste caso, deve-se realizar a autenticação do usuário para que o acesso seja liberado;
iv. Visitantes e funcionários acessando a Internet por dispositivos não governados pela área de TI dentro da zona intermediária;
v. Funcionários acessando a internet a partir da zona confiável;

vi. Comunicação entre os serviços utilitários internos e externos como por exemplo, DNS e SMTP;
vii. Acesso a serviços públicos a partir de clientes e/ou redes não governadas pela TI da empresa;
viii. Comunicações internas a zona de confiança;
ix. Comunicações entre a zona de confiança e os sistemas e serviços da zona restrita.
x. Novas conexões à infraestrutura de rede devem ser previamente avaliadas pelas áreas de Segurança Cibernética e Infra TI, sob os aspectos de segurança e disponibilidade.

c) Regras para conexões em rede Wireless

As conexões via wireless (Wi-Fi) deverão ser permitidas somente através de Pontos de Acesso (AP), devendo ser bloqueadas qualquer outro tipo de conexão wireless, incluindo conexões do tipo ponto a ponto (Ad hoc).

O gerenciamento dos pontos de acesso deverá ser feito através de protocolos que façam uso de criptografia na transferência de dados através da rede, como por exemplo SSH e SSL.

É necessário a geração de trilhas de auditoria dos acessos de usuários, administradores e das alterações de configuração.

Deverá existir um processo para detecção automática de pontos de acesso não autorizados (Rogue Access Point) e conexões wireless ponto a ponto (Ad-hoc).

Somente o protocolo WPA2 deverá ser utilizado para conexões Wireless

Dispositivos móveis de terceiros ou particulares de colaboradores, somente poderão utilizar a rede de visitantes, em nenhuma situação este tipo de equipamento será conectado na rede corporativa.

Deverá existir um processo de verificação de conformidade do dispositivo antes do mesmo ingressar na rede wireless. Esse processo deverá ser auditável e gerar logs ou relatórios de confirmação.

Exceções devem ser submetidas a análise e aprovação de Segurança da Cibernética.

d) Configuração segura de hardware e software em dispositivos móveis, desktops e servidores

A utilização de dispositivos de gravação via USB/CDR/DVDR não é permitida.

6.8 Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantam a segurança na infraestrutura tecnológica de redes locais e internet, através do monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações.

a) Gerenciamento e regras de firewall

Os firewalls do Grupo Travelex Confidence devem estar com o sistema de log e/ou alertas habilitados. As mensagens geradas deverão ser correlacionadas e receberem análise crítica pela equipe que administra os equipamentos.

O gerenciamento dos firewalls deve ser realizado através de protocolos que façam uso de criptografia na transferência de dados através da rede, como por exemplo SSH e SSL.

Os administradores dos firewalls deverão ser assinantes ou constantemente checar os boletins de vulnerabilidades do fabricante do equipamento. Outras fontes de informações também são recomendadas.

Toda manutenção de regra de firewall (criação, alteração e exclusão de regras), deve passar pela aprovação da área de Segurança Cibernética.

Toda instalação física de equipamentos de firewall, deve passar previamente por um processo de Gestão de Mudanças, prevendo o procedimento de *rollback*.

Os firewalls devem ser mantidos em áreas seguras, protegidos por perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso efetivo. Estas áreas devem ser fisicamente protegidas de acesso não autorizado, dano ou interferência.

b) Monitoramento de ameaças e vulnerabilidades

O processo de monitoramento de ameaças e vulnerabilidades do Grupo Travelex Confidence, abrange as intrusões detectadas e prevenidas, protegendo a rede de atividades maliciosas como por exemplo: SQL injections, cross-site scripting, buffer overflows, etc.

Também fazem parte do monitoramento, as ameaças relacionadas a vírus, trojans, worms, spyware e rogueware, com o impedimento de afetar a rede e demais dispositivos, bem como os ataques do tipo Botnet e APT Zero Day, que são ameaças (ataques) conhecidas por atingir uma rede de computadores, infectando-os com softwares maliciosos que podem ser controlados remotamente, obrigando-os a enviar spam, espalhar vírus ou executar ataques de DDoS, sem o conhecimento ou o consentimento dos seus "donos".

Os acessos à internet são controlados e gerenciados através de políticas de filtro web, com o bloqueio de navegação para os endereços web que apresentarem riscos de segurança. As exceções são liberadas através de análise prévia da área de Segurança Cibernética, mediante aprovação da Diretoria responsável pela solicitação.

Qualquer incidente relacionado às ameaças/ataques efetivos no ambiente, devem ser registrados e tratados através do processo Registro e Resposta aos Incidentes, contendo a análise da causa-raiz, solução pontual, solução definitiva, impacto operacional, impacto financeiro e classificação de risco.

c) Monitoramento de Infraestrutura

A área de TI realiza o monitoramento dos Servidores e Links com alertas na tela do computador, na televisão da área, bem como alertas por celular.

Em relação às lojas físicas do Grupo Travelex Confidence é realizado monitoramento interno sobre indisponibilidade e latência dos links. Pela análise do comportamento, pode-se identificar um possível ataque.

Qualquer incidente relacionado à indisponibilidade e latência de servidores e links, devem ser registrados e tratados através do processo Registro e Resposta aos Incidentes, contendo a análise da causa-raiz, solução pontual, solução definitiva, impacto operacional, impacto financeiro e classificação de risco.

d) Trilhas de auditoria e monitoramento

Qualquer informação que é produzida, transmitida, processada ou armazenada está sujeita a monitoramento e auditoria, portanto, o Grupo Travelex Confidence em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

A geração dos registros de trilha de auditoria (log) deve estar sincronizada com relógio confiável elegível na rede. Todos os registros devem ter a marcação de horas no mesmo formato, sincronizados com um relógio principal.

e) Atualização de patches de segurança e antivírus

A área de TI é responsável por manter uma rotina de identificação e monitoramento de atualizações de sistemas operacionais, antivírus e versões (firmware) de equipamentos de rede e de segurança.

Para atualizações críticas, deve-se prever a preparação de um ambiente de homologação para receber e testar a nova atualizações, antes de realizar a instalação nos equipamentos (desktops, servidores, firewalls, etc.).

As atualizações necessárias que não poderão ser aplicadas, por qualquer impossibilidade no ambiente, deverão ser comunicadas à área de Segurança Cibernética.

f) Testes de Segurança (Pentest)

A área de Segurança Cibernética realiza periodicamente testes de penetração no ambiente tecnológico e de rede, para avaliar as atividades do sistema, envolvendo a busca de vulnerabilidades em potencial, falhas de hardware/software, deficiência em sistema operacional, componentes de publicação na internet, dentre outros. Aplica-se a avaliação do impacto sobre os gaps identificados e a diligência com as áreas responsáveis para a devida tratativa e solução técnica.

6.9 Gestão de registro e tratamento de incidentes

O gerenciamento de registro e tratamento de incidentes é de responsabilidade das áreas de TI, Risco Operacional e Segurança Cibernética do Grupo Travelex Confidence.

Os incidentes identificados devem ser registrados por todos os colaboradores da empresa, através de sistema disponibilizado para esse objetivo.

Na abertura de um incidente deve ser mencionado o tipo do incidente ocorrido, conforme detalhado abaixo, mas não se limitando a tais:

a) **Falha de Segurança Cibernética/Informação:** informações sensíveis/confidenciais disponíveis sem restrição; compartilhamento de senhas; acesso não autorizado, ataque cibernético, malwares, etc.;
b) **Falha ou Erro em sistemas:** sistema com mensagem de erro; sistema realizando cálculo errado, sistema travado, etc.;
c) **Indisponibilidade:** queda de link de internet; linha telefônica indisponível; falta de energia elétrica, etc.;
d) **Lentidão:** rede, banco de dados, sistemas apresentando lentidão excessiva, etc.;
e) **Falha Operacional:** processo não executado da forma correta e/ou definida, etc.;
f) **Fraudes:** operações atípicas que denotam fraudes.

O relato do evento (incidente) deve ser bem detalhado a fim de prover informações suficientes para a investigação e devidas tratativas.

Dependendo do tipo do incidente, o registro será direcionado para a equipe correspondente responsável pela tratativa e resposta ao incidente, pelo qual deverá detalhar a causa raiz, a solução pontual, a solução definitiva, plano de ação e prazo, para se evitar recorrência e o impacto operacional.

Consideram-se nesse escopo de gerenciamento a abrangência para informações recebidas de prestadores de serviço do Grupo Travelex Confidence.

Os incidentes classificados como risco "Crítico" devem ser apresentados ao Comitê de Gestão de Riscos do Grupo Travelex Confidence, o qual decidirá sobre o compartilhamento de informações sobre os incidentes relevantes com outras instituições e disponibilização ao Órgão Regulador.

Perante ao Banco Central do Brasil (Órgão Regulador), deve ser nomeado o Diretor responsável pela Política de Segurança Cibernética, bem como para a execução do processo de resposta aos incidentes.

Anualmente, com data-base em 31/12, deve ser emitido o relatório sobre o gerenciamento de incidentes do período, com a disponibilização ao Órgão Regulador.

6.10 Continuidade de Negócios

O processo de gestão de continuidade de negócios, relativo a segurança da informação, deve ser implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, 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 de nuvem e os testes previstos para os cenários de ataques cibernéticos.

O processo de gerenciamento do Plano de Continuidade de Negócios do Grupo Travelex Confidence abrange a Análise de Impacto de Negócios (BIA-PCN) das áreas críticas da empresa, conduzido pela área de Segurança Cibernética/Continuidade de Negócios, pelo qual são realizados o inventário de processos críticos, o tempo necessário de retorno da operação em caso de incidente e ativação da contingência, a interdependência de processos e sistemas, as pessoas chaves que serão acionados em caso de ativação da contingência e os impactos financeiro, operacional, regulatório e de imagem. O BIA deve ser revisto anualmente.

Testes periódicos (anuais) são conduzidos pela área de Segurança Cibernética/Continuidade de Negócios, de acordo com os cenários de incidentes previstos, como a indisponibilidade do ambiente tecnológico e abandono de edifício, com apoio operacional da área de TI e tem o objetivo de aferir a efetividade do ambiente de contingência planejado para os processos e sistemas críticos.

6.11 Cópias de segurança de dados e informações

A área de TI é responsável por manter o processo de backup das informações críticas do Grupo Travelex Confidence.

Esse processo consiste no backup em disco, através da técnica de duplicação de dados, pela qual tem a finalidade de analisar, identificar e remover duplicidade nos dados, diminuindo assim a quantidade de informação a ser armazenada.

São realizados backups dos File Server e de pastas de rede que contenham os backups dos bancos de dados.

A equipe de TI é responsável por verificar, diariamente, a execução dos backups realizados.

6.12 Aquisição, Desenvolvimento e Manutenção Segura de Software

Os aspectos de segurança da informação estão envolvidos nas seguintes fases do Ciclo de Aquisição, Desenvolvimento e Manutenção de Software, a saber:

a) Conceituação e Planejamento
b) Análise e Design
c) Construção e Desenvolvimento
d) Homologação
e) Implantação

a) Ambiente Seguro de Desenvolvimento

Devem existir procedimentos formais e documentados que detalhem o Ciclo de Desenvolvimento com as devidas aprovações necessárias cada migração entre as fases acima mencionadas.

A Gerência de TI deve seguir o processo formal e documentado, visando garantir que a integridade do software esteja preservada através do controle das versões e das mudanças feitas no produto. Este processo deve estar formalizado na metodologia que subsidia o Ciclo de Desenvolvimento do Grupo Travelex Confidence.

Deve ser mantido o processo de garantia de qualidade de processo e produto para que se determine a existência de problemas e defeitos em todos os softwares durante seu processo de elaboração e manutenção.

O acesso aos códigos-fonte e a itens associados (como desenhos, especificações, planos de verificação e validação) dos softwares em produção ou em processo de desenvolvimento deve ser controlado e restrito aos indivíduos autorizados. Não deve ser divulgado a terceiros a natureza e o conteúdo de qualquer informação que componha ou tenha resultado de atividades profissionais do Grupo Travelex Confidence.

Serão aplicadas medidas administrativas no caso de ocorrência de infrações relaciona a divulgação para terceiros de informações pertinentes ao desenvolvimento do projeto.

b) Fase de Conceituação e Planejamento

A descrição dos requisitos de segurança da informação deve fazer parte da fase do processo de levantamento de requisitos. Estes requisitos devem constar nos documentos de requisitos de projetos, com o objetivo de atribuir de forma equilibrada controles de segurança ao software desde o início do seu ciclo de vida e identificar as funcionalidades de segurança mais apropriadas para assegurar o nível de segurança necessário às informações tratadas pelo software.

A área de Segurança Cibernética deve ser envolvida na aprovação destes requisitos de segurança.

As informações processadas, apresentadas, transmitidas e armazenadas pelo software deverão ser identificadas e classificadas (caso já não estejam) durante sua concepção quantos aos requisitos de segurança, conforme item 6.3 desta Política.

O cliente (requisitante) deve aceitar formalmente os controles propostos, o risco existente pela não implantação dos controles ou registrar seu compromisso de implementá-los no processo de negócio. O importante é garantir a ciência de quais são os riscos e os benefícios existentes.

c) Testes de Segurança

Deve existir um processo formal e documentado para a realização de testes de segurança antes da migração do software do ambiente de desenvolvimento para a produção. Este processo deverá definir o responsável pela execução dos testes, assim como descrever o seu escopo e profundidade.

Os testes de segurança não devem fazer o uso de dados reais, ou seja, oriundos da produção. Os testes devem ser realizados em ambiente segregado destinado especificamente para este fim, e por equipe distinta daquela participante do desenvolvimento do sistema. Portanto é importante que nos requisitos do software já sejam levantadas as informações que comporão os testes de segurança para que elas possam ser geradas e disponibilizadas no momento adequado para execução dos testes.

O teste funcional de segurança é obrigatório para todos os softwares desenvolvidos para uso do Grupo Travelex Confidence. Consiste em realizar a verificação de cada controle de segurança do sistema. O teste funcional deve, portanto, considerar cada item contido na especificação de segurança.

Os testes funcionais devem envolver o cliente na fase de Homologação. Em caso de êxito nos testes, este explicitamente registrará sua aprovação.

d) Contratação de Terceiros

O desenvolvimento de software por terceiros deve ser controlado. O contrato firmado deve especificar a metodologia utilizada nas etapas do Ciclo de Desenvolvimento de Software, dispor sobre as questões de propriedade intelectual, acordos de confidencialidade e contemplar o direito de o Grupo Travelex Confidence auditar o terceiro, com o objetivo de assegurar que todos os requisitos de segurança descritos estão sendo atendidos.

e) Pacote de Software

A aquisição de Software Pacote deve seguir um processo formal e documentado de avaliação funcional (executado pela área usuária) e técnica (executada pela área de desenvolvimento). A análise técnica deve contemplar o levantamento dos requisitos de segurança, especificação das funcionalidades, projeto da arquitetura e testes, bem como a avaliação sobre critérios de Riscos Operacionais e proteção aos dados e informações.

O contrato com o fornecedor deve conter cláusulas que protejam ao Grupo Travelex Confidence dos riscos de descontinuidade da prestação de serviços de suporte e manutenção corretiva e evolutiva, bem como dos riscos de não atendimento de prazos legais de adequações do software.

Em caso de Pacotes de Software que automatizem operações críticas do Grupo Travelex Confidence, os controles devem ser implementados para proteção contra o risco de o fornecedor sair do mercado ou descontinuar o software, como a adoção de uma terceira parte atuando como custodiante do código fonte.

As mudanças em Pacotes de Software devem ser executadas de forma controlada pelos fornecedores. Devem ser estabelecidos processos que formalizem o recebimento, mudança, homologação, distribuição e armazenamento em repositório centralizado dos patches e versões dos Software Pacote.

6.13 Operações de Terceiros

O contrato dos prestadores de serviços deve, necessariamente, estabelecer que a Política Corporativa de Segurança Cibernética seja cumprida na íntegra, assim como as normativas de segurança relacionadas ao escopo da contratação e ainda, estabelecer as penalidades decorrentes de qualquer violação das regras de segurança definidas.

Todo prestador de serviços deve estar atualizado com relação às regras de segurança do Grupo Travelex Confidence e somente utilizar os serviços para os quais possui permissão.

Qualquer equipamento de propriedades do prestador de serviços apenas é instalado e/ou utilizado no âmbito do Grupo Travelex Confidence, mediante identificação e autorização.

Os acessos lógicos dos prestadores de serviços são gerenciados conforme o item 6.1 desta Política.

O Grupo Travelex Confidence poderá, a qualquer tempo, monitorar, auditar e suspender os acessos concedidos para prestador de serviços, independentemente de qualquer aviso ou comunicado prévio.

6.14 Processamento, Armazenamento de dados e Computação em Nuvem

Conforme a Resolução CMN n° 4.893 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, o Grupo Travelex Confidence deve assegurar um procedimento efetivo que assegure a aderência às regras previstas na regulamentação em vigor.

Para os fins de aderência regulatória sobre a análise de riscos operacionais e cibernéticos, de continuidade de negócios, de confidencialidade, de disponibilização de informações ao Órgão Regulador, de Resposta a Incidentes, dentre outros, deve-se contemplar o processo de *due-diligence* junto ao fornecedor do produto ou serviço contratado, **previamente à formalização do contrato** de prestação de serviços entre a contratante (Grupo Travelex Confidence) e a contratada (Fornecedor).

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, bem como as alterações contratuais desses serviços, devem ser previamente comunicadas ao Banco Central do Brasil, no mínimo, sessenta dias antes da contratação dos serviços ou das alterações contratuais.

6.15 Utilização de dispositivos móveis

Os usuários fazem parte do processo de proteção da rede da empresa e dos dados confidenciais que são armazenados ou acessados usando um dispositivo móvel (celular, smartphone, tablete, etc.), devendo tomar as seguintes medidas:

a) Fazer o melhor para proteger o dispositivo contra perda ou roubo;

b) Informar imediatamente Infraestrutura de TI ou Segurança Cibernética sobre um dispositivo perdido ou roubado;

c) Manter o sistema operacional e os aplicativos atualizados e/ou verificando com a TI se você não tem certeza de como fazê-lo;

d) Usar apenas aplicativos originais e aprovados para acessar dados da empresa;

e) Usar os programas e práticas de segurança para evitar pirataria e/ou adulterações em software/configurações de segurança no dispositivo;

f) Certificar-se de que o dispositivo está programado para bloquear a tela com uma senha ou PIN, se estiver ocioso após cinco minutos;

g) Atentar-se sobre o manuseio de informações em dispositivos móveis no aspecto de segurança e classificação de informação.

6.16 Conscientização de Segurança da Informação e Riscos Cibernéticos

A área de Segurança Cibernética é responsável por aplicar procedimentos sobre a conscientização de segurança da informação e riscos cibernéticos para funcionários e prestadores de serviços.

O funcionário contratado deve realizar o treinamento online (obrigatório) sobre Segurança da Informação.

As Campanhas de conscientização e capacitação contendo palestras, boletins periódicos de segurança da informação, dentre outros, devem ser intensificados como um programa da área de Segurança Cibernética, contendo mecanismos de aferição do programa de capacitação e conscientização dos funcionários.

Mesa Limpa

Os papéis e mídias removíveis de computador que contenham informação sensível ou crítica ao negócio do Grupo Travelex Confidence, quando não estiverem sendo utilizados, devem ser guardados de maneira adequada, de preferência, em gavetas ou armários trancados.

Todas as outras informações, que não sejam públicas, devem ser guardadas em segurança quando os funcionários deixam o edifício no final do seu dia de trabalho.

Durante o expediente deverá ser evitado deixar sobre a mesa de trabalho, sem o devido acompanhamento, os itens abaixo listados:

a) Documentos confidenciais com informações de clientes, parceiros e competidores.
b) Agendas, folhas de papel, livros, blocos e cadernos de anotações;
c) Mídias removíveis (Pen Drivers, HD externo, CD e DVD;
d) Chaves e Cartões de Acesso;
e) Senhas em POST-IT ou qualquer outro bloco de notas.

Os documentos devem ser retirados das impressoras pelos seus responsáveis, imediatamente após sua impressão. Os documentos encontrados à deriva por funcionários do Grupo Travelex Confidence, devem ser entregues para a área de Segurança Cibernética.

7. VIOLAÇÕES À POLÍTICA

São consideradas violações à Política Corporativa de Segurança Cibernética e às respectivas normativas, as seguintes situações, não se limitando a estas:

a) Quaisquer ações ou situações que possam expor o Grupo Travelex Confidence à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
b) Uso indevido de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do gestor da informação;
c) Uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do Grupo Travelex Confidence;
d) A não-comunicação imediata à área de Segurança Cibernética sobre quaisquer descumprimentos da Política.

Indícios de irregularidades no cumprimento das determinações desta política devem ser comunicadas imediatamente para o endereço de e-mail segurancacibernetica@travelexbank.com.br e serão alvo de investigação interna. Averiguando-se a efetiva irregularidade, o Colaborador estará sujeito as penalizações aplicáveis pelo Grupo Travelex Confidence (advertência verbal, advertência escrita, suspensão e demissão justa causa).

Eventuais exceções deverão ser avaliadas e aprovadas pelo Gerente de Segurança Cibernética e Diretor Jurídico, conforme análise de risco, impacto e critérios de mitigação e aceitabilidade.

8. RESPONSABILIDADE

A Alta Administração do Grupo Travelex Confidence se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas recorrentes em Comitês internos da empresa.

9. REVISÃO

As revisões e atualizações desta Política, bem como da estratégia de segurança cibernética deverão ocorrer anualmente, ou de acordo com as revisões de processos, necessidades de negócios e adequações para atendimento legal ou regulatório.

Declaramos que a presente é a versão atualizada e aprovada pelo Comitê Executivo em 14/12/2022