14 DE NOVEMBRO DE 2022

POLÍTICA DE SEGURANÇA CIBERNÉTICA

FIDÚCIA SOCIEDADE DE CRÉDITO AO MICROEMPREENDEDOR À EMPRESA DEPEQUENO PORTE LTDA.

Sumário

1 – OBJETIVOS

Esta Política estabelece as diretrizes a serem observadas pelos colaboradores e prestadores de serviços da FIDÚCIA SCMEPP, no que se refere aos riscos cibernéticos, nos quais a supra instituição pode estar, ou mesmo tornar-se, suscetível.

Por conseguinte, define-se um conjunto de princípios, diretrizes e responsabilidades, que norteiam as atividades pertinentes à gestão de tais riscos, em suas várias facetas, conforme poder-se-á observar no decorrer dessa Política. Além disso, vislumbrando prover incolumidade à FIDÚCIA SCMEPP face aos riscos aos quais se expõe, delinear-se-á quais os procedimentos a serem levados a cabo para evitá-los, ou na iminência de sua ocorrência, transpô-los com a maior salubridade possível, por mais deletério que seja o evento. Com isso, oportuniza-se que por mais exíguo que seja o fato, o tratamento deverá ser feito na dosimetria necessária para o arrefecimento de sua carga de risco.

Em apertada síntese, ao dissertar essa Política, possibilita-se a identificação, avaliação, tratamento, monitoramento e comunicação de riscos os quais a organização possa incorrer, fornecendo valorosos insumos para a continuidade dos negócios da FIDÚCIA SCMEPP.

2 - VIGÊNCIA

Essa Política deve ser revisada e aprovada pelo Conselho de Administração, anualmente ou em prazo inferior, se assim requerido pelo regulador local, no caso de alteração na legislação aplicável ou se houver alguma alteração das práticas de negócios da FIDÚCIA SCMEPP ou evento que justifiquem, no entender da Diretoria, a atualização dessa Política. Após aprovada pelo Conselho de Administração, mediante lavratura de ata que preveja tal chancela, essa Política será amplamente divulgada internamente e será disponibilizada no seu website e Intranet

3 - PÚBLICO-ALVO

Essa política deverá ser diligenciada a todos os colaboradores da Fidúcia SCMEPP de forma a capilarizar os ditames aqui destilados.

Analogamente, todos os prestadores de serviços e correspondentes bancários dessa instituição deverão munir-se dos conceitos teorizados nessa política, intuindo alinhavar uma atuação *sui generis*, extrínseca e intrinsicamente, à luz dos dispositivos trazidos à baila nesse documento, evitando, por conseguinte, eventos que possam implicar em processos nefastos ou dispendiosos a todos os envoltos no processo.

4 - DISPOSIÇÕES GERAIS

4.1 - INTRODUÇÃO

De forma consonântica à Resolução 4.893, de 26 de fevereiro de 2021, emanada do CONSELHO MONETÁRIO NACIONAL, as instituições financeiras e demais instituições autorizadas a funcionar pelo BANCO CENTRAL DO BRASIL devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

O normativo busca contornar fissuras que, ao ocorrerem em meio à infraestrutura de TI, ou mesmo na ambiência intangível dos softwares, venham a comprometer a robustez e higidez dos vários tipos de dados existentes em organizações dessa magnitude, principalmente no tangente a três primordiais fatores:

a) Disponibilidade: garantir que o sistema funcione como o esperado quando requisitado pelos usuários, evitando perjúrios em função da indisponibilidade do meio informático;

b) Integridade: garantir o nível de confiança que se pode ter de uma informação. Nesse cenário, evidencia-se que uma informação deverá, indistintamente, ser apresentada em sua plenitude, evitando que qualquer detalhe, por mais ínfimo que seja, esboroe-se em seu processamento;

c) Confidencialidade: garantir o sigilo ou a privacidade, evitando que a informação seja acessada por pessoas não autorizadas. Nisso, além de garantir a disponibilidade e integridade das informações, deve-se atentar à confidencialidade de tal massa de dados, evitando seu acesso ou conhecimento por partes estranhas àquelas envolvidas no relacionamento que enseja a transferência de tais informações.

Dado o emaranhado de previsões, a Política relativa a tais realizações deve se compatibilizar com:

a) o porte, o perfil de risco e o modelo de negócio da instituição;

b) a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e

c) a sensibilidade dos dados e das informações sob responsabilidade da instituição.

Por conseguinte, ao se delinear a Política, posto esse cabedal de funções a ela imputadas, deve-se contemplar:

a) os objetivos de segurança cibernética da instituição;

b) os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética;

c) os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;

d) o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;

e) as diretrizes para:

a. a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

b. a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;

c. a classificação dos dados e das informações quanto à relevância;

d. a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

f) os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

a. a implementação de programas de capacitação e de avaliação periódica de pessoal;

b. a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros;

c. o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

g) as iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com as demais instituições referidas no art. 1º.

Em outro panorama, face às deliberações arroladas acima, o normativo ainda metodiza a necessidade em se estabelecer o plano de ações e de respostas a incidentes à implementação da política de segurança cibernética, abrangendo, minimamente:

a) as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

b) as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e

c) a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

5 - RISCOS CIBERNÉTICOS NA FIDÚCIA SCMEPP

Sob a ótica da FIDÚCIA SCMEPP, a informação é um dos principais ativos de qualquer organização. Para a devida proteção desse bem, essa instituição estabelece a presente Política de Segurança Cibernética, a fim de garantir a aplicação dos princípios e diretrizes de proteção da propriedade intelectual e das informações da organização, dos clientes e do público em geral no hodierno ambiente virtualizado.

A estratégia fora desenvolvida para evitar violações da segurança dos dados, minimizar os riscos de indisponibilidade dos serviços, proteger a integridade e evitar qualquer vazamento de informação. A fim de alcançar esse objetivo, a estratégia está baseada na proteção de perímetro expandido, apoiado em processos de controle para detecção, prevenção, monitoramento e resposta a incidentes garantindo a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o correto manejo dos dados e informações. A informação deve ser protegida independentemente de onde ela esteja, seja em um prestador de serviço ou em domínios próprios, em todo o seu ciclo de vida, desde o momento que ela é coletada, passando pelo processamento, transmissão, armazenamento, análise e seu descarte.

Em um prisma análogo, existe ainda a preocupação com a invasão de hackers nos sistemas e máquinas da instituição. Para isso as informações transacionadas no sistema são todas criptografas e contam ainda com os mecanismos protecionistas da próprio software house. Localmente, a rede de internet, bloqueia a tentativa de acesso a sites selecionados pela Diretoria dessa instituição ao entendê-los como possíveis fontes maliciosas. As máquinas possuem antivírus atualizados e somente o e-mail corporativo pode ser acessado por intermédio dos meios eletrônicos usufruídos pela instituição.

No intuito de guardar informação e prover acesso aos dados brutos ou compilados, os colaboradores possuem acesso por alçada ao sistema de gestão de crédito, limitado ao horário comercial. Cada usuário possui sua senha e login, intransferíveis, e seu acesso pode ser monitorado. Não é permitido o carregamento de pen drive em nenhuma máquina, salvo autorização expressa do líder do setor, ou equivalente, ou da diretoria.

Para completar o mecanismo protecionista adotado pela instituição, toda operação gera obrigatoriamente documentos que são arquivados em locais apropriados.

Nisso, a FIDÚCIA SCMEPP trata dessa questão como a capacidade de prevenir, detectar, reduzir e, se possível, estancar a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Dentro dessa ótica, os princípios norteadores da segurança da informação podem ser enviesados da seguinte forma:

a) confidencialidade: a garantia de que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;

b) disponibilidade: o caráter assecuratório de que as pessoas autorizadas tenham acesso à informação sempre que necessário;

c) integridade: a certeza da exatidão e completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

Analogamente, encampa-se, de forma mesclada a tais previsões, a continuidade dos negócios, que inere ao desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais, capilarizados no ambiente cibernético, sejam devidamente identificados e preservados após a ocorrência de um desastre e até o retorno à situação normal de funcionamento dessa instituição.

Diante do cabedal de dados exposto acima, a FIDÚCIA SCMEPP, primacialmente, entabula as seguintes diretrizes no tocante à segurança cibernética e continuidade de negócios, que deverão, por seu expediente, direcionar a atuação prática dessa instituição:

a) definição de responsabilidades por colaborador e por alçada;

b) conscientização e treinamento de cada colaborador;

c) proteção e classificação dos dados, consoante a Lei Geral de Proteção de Dados;

d) proteção contra códigos maliciosos;

e) monitoramento continuado e fidedigno;

f) respostas a incidentes de segurança cibernética;

g) gestão de identidade de acessos;

h) segurança de dispositivos móveis usados pela instituição e seus colaboradores;

i) segurança em sistemas e aplicações;

j) segurança em redes;

k) manutenção do inventário de ativos da instituição;

l) manutenção do inventário de softwares da instituição;

m)manutenção de documento contendo dados dos funcionários, usuários e

parâmetros de acesso nos sistemas utilizados;

n) estabelecimento e monitoramento dos parâmetros de Firewall, prevenção de acessos ilegais, ilegítimos e de intrusos;

o) emissão de relatório de ocorrências de TI;

p) emissão de relatório de ocorrência de falhas de sistemas, servidores, rede ou ocorrências físicas que causaram indisponibilidade na execução dos serviços críticos exercidos pela instituição;

q) notificação, ao Banco Central do Brasil, de falhas críticas ocorridas na instituição.

Perfilado o rol de realizações atinentes à segurança cibernética, encampa-se, ainda, algumas diretrizes estritamente voltadas à gestão da informação, que, a reboque da segurança cibernética, visionam estabelecer um ambiente salubre para a manipulação de dados e informações:

a) as informações da FIDÚCIA SCMEPP, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida, atentando-se, prioritariamente, às nuances dissertadas pela Lei Geral de Proteção de Dados;

b) a informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada, coibindo-se qualquer utilização aleatória ou circunscrita externamente às diretrizes genuinamente encetadas para o evento em questão;

c) todo processo, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador ou equipe de colaboradores, para que a atividade não seja executada e controlada pelo mesmo colaborador ou equipe, no qual cada partícipe deverá possuir indubitável ciência de suas realizações, assim como ser munido da expertise necessária à análise da assertividade da etapa imediatamente anterior;

d) o acesso às informações e recursos só deve ser feito se devidamente autorizado pela área de Tecnologia da Informação, em consonância às diretrizes e deliberações oriundas da Diretoria da instituição, a serem convencionadas convictamente em documentos apensados a essa Política;

e) a identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas em ambiente sistêmico, ou em qualquer documento emitidos pelos meios eletrônicos e cibernético

usufruídos pela FIDÚCIA SCMEPP;

f) a concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades, devendo, tal mapeamento de atribuições e competência, alinhar-se às práxis das responsabilidades atribuídas a cada partícipe do processo, coadunadas às definições estratégicas carreadas pela Diretoria da instituição;

g) todo colaborador deve reportar os riscos às informações à área de Tecnologia da Informação, assim como levar a cabo as demais ações previstas nas diversas políticas de gerenciamento contínuo de riscos outorgadas pela Diretoria;

h) a área de Tecnologia da Informação deve divulgar amplamente, em consonância às diretrizes redigidas pela Diretoria da instituição, as responsabilidades sobre Segurança da Informação aos Colaboradores, que devem entender e assegurar estas diretrizes.

Consoante o delineado acima, pode-se vislumbrar uma ambiência diretiva que enobrece o tratamento sistêmico e cibernético dos sistemas utilizados pela instituição, assim como dos recursos usados adstritamente aos mesmos; em outro prisma, tonificou-se alguns preceitos voltados à manipulação de dados e informação. Presume-se que a junção de ambos os fatores contribui sobremaneira para a correta estipulação dos ditames concernentes à segurança cibernética e da informação. Diametralmente, no mesmo diapasão, para assegurar que as informações tratadas estejam adequadamente protegidas, na dosimetria requestada, a FIDÚCIA SCMEPP lança mão dos seguintes processos:

5.1 - GESTÃO DE ATIVOS DA INFORMAÇÃO

Os ativos da informação, de acordo com sua criticidade, devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente (salas com acesso controlado) e logicamente, assim como possuir documentação e planos de manutenção atualizados anualmente em consonância à sua utilização, estabelecendo planos preditivos e saneadores de máculas que podem recair sobre tais bens.

5.2 - CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser classificadas de acordo com a

confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações, usando, em sua totalidade, as delineações cuja Lei Geral de Proteção de Dados definira em seus dispositivos.

5.3 - GESTÃO DE ACESSOS

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da FIDÚCIA SCMEPP, subscritas e em consonância com os demais documentos, políticas e processos da instituição. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o colaborador, prestador de serviço ou qualquer outro terceiro que possua angaria tal acesso, a fim de patrocinar um cenário imputáveis a tais partícipes pelas ações e posturas tomadas.

5.4 - GESTÃO DE RISCOS

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos cibernéticos e de informação dessa instituição, para que sejam recomendadas as proteções adequadas. Os cenários de riscos de segurança da informação são escalonados pela área de Tecnologia da Informação, sob a supervisão e poder de anuência e/ou veto da Diretoria.

5.5 - GESTÃO DE RISCOS EM PRESTADORES DE SERVIÇO

Tão necessário quanto a gestão de riscos incidentes em meios cibernéticos internos, os prestadores de serviços contratados pela instituição deverão ser classificados considerando alguns critérios, tais como:

a) criticidade do segmento;

b) informações mais críticas manipuladas pelo fornecedor;

c) forma de acesso às informações;

d) frequência de acesso às informações;

e) histórico de fraude e/ou de vazamento de informação;

f) certificações;

g) data da última avaliação;

h) classificação do risco identificado na última avaliação

Dependendo da classificação do prestador de serviço referente aos critérios acima, esse deverá passar por avaliação de risco, que contempla a validação in loco dos controles de segurança da informação, avaliação remota das evidências ou outros processos de avaliação, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços, a fim de garantir que a acepção de seu serviço posicione-se de maneira coadunada a essa Política, bem como e potencialmente ao conjunto normativo emanado do Banco Central do Brasil.

Para assegurar um reporte crível e tempestivo, existem canais de comunicação para que os prestadores de serviços informem as ocorrências de incidentes relevantes relacionados às informações da FIDÚCIA SCMEPP, armazenadas ou processadas na empresa contratada, em cumprimento às determinações legais e regulamentares. Outrossim, consigna-se, desde já, que tais veiculações deverão ser remetidas, de forma improrrogável, a supra autarquia, na forma delimitada nos diplomas regulamentares emanadas da mesma.

5.6 - TRATAMENTO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

A área de Tecnologia da Informação da FIDÚCIA SCMEPP realiza a monitoração de segurança do ambiente tecnológico da instituição, analisando os eventos e alertas com o objetivo de identificar possíveis incidentes, conclamando, o departamento envolto no centelhar do evento, para a tomada das medidas cabíveis e arrazoadas.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto de acordo com os critérios adotados pela instituição. Para o seu grau de relevância serão considerados aspectos como comprometimento de dados de clientes e impacto ao sistema interno. Nisso, arrola-se a seguinte classificação:

a) altamente críticos: são aqueles que podem comprometer desmedidamente a segurança cibernética da informação, obstruir a consecução operacionais e denotar dificultosa ação mitigadora, considerando-se, as ocorrências desse nível, como incidentes relevantes;

b) medianamente críticos: remetem aos incidentes que podem

comprometer, de forma conhecida e controlada, a segurança cibernética da informação, e apresentar uma ação saneadora já conhecida pela instituição, considerando-se, as ocorrências desse nível, como incidentes relevantes;

c) reduzidamente críticos: tangenciam àqueles eventos que fragilizam levianamente a segurança cibernética da informação, e requerem ações saneadoras palatáveis.

Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto e classificação (de acordo ao sumarizado acima), de acordo com o procedimento operacional interno e externo, naqueles casos em que houver a presença de qualquer prestador de serviço no ativo ou sistema alcançado pelo fato. O emaranhado de dados provenientes dessa mensuração será prontamente disponibilizado ao Banco Central do Brasil, em linha com o ambiente regulatório, assim como difundido às demais instituição que integram o Sistema Financeiro Nacional, de acordo com o meio emplacado pela supra autarquia, intentando refutar qualquer alastramento sistêmico dos incidentes manipulados.

Tencionando aprimorar a capacidade de resposta a incidentes cibernéticos, alguns cenários que possam afetar a continuidade de negócios são considerados nos testes periódicos abalroados pelo departamento de Tecnologia da Informação.

Em conivência com o abordado anteriormente, cada departamento, principalmente a área de Tecnologia da Informação, elaborará um relatório sobre a ocorrência de incidentes relevantes no período, ações realizadas de prevenção e respostas aos incidentes e resultados dos testes de continuidade. Este relatório deverá ser apresentado ao Conselho de Administração ou à Diretoria, na ausência daquele, conforme determinações legais e regulamentares.

Em caráter superlativo, delibera-se que o departamento de Tecnologia da Informação deverá coletar todos os relatórios das demais áreas e concentrá-los em registros e controles que alumiem os efeitos dos incidentes recaídos pela instituição; com isso, buscar-se-á identificar aqueles eventos demasiados periclitantes e as ações tomadas para seu esgotamento.

5.7 - CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

A FIDÚCIA SCMEPP promove a disseminação dos princípios e diretrizes de Segurança Cibernética e da Informação por meio de programas de conscientização e capacitação, com o objetivo de prover o aculturamento em tópicos afetos a esse contexto.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou online, relacionados a confidencialidade, integridade e disponibilidade da informação, assim como dos dispositivos acarreados pela gestão cibernética. Estas campanhas são difundidas por meio dos canais de comunicação reiteradamente utilizados pela instituição.

Ademais, na hipótese de difusão de qualquer sistema para clientes e/ou usuários, tal plataforma será complementada com instruções, dicas e indicações, por meio de pop-ups, páginas ou links, que vislumbrarão angariar um ambiente precaucional e alinhavados às diretrizes da segurança cibernética e da informação.

Por fim, consigna-se que a Diretoria da FIDÚCIA SCMEPP se compromete, primordialmente, com a assunção de todos os preceitos aqui ventilados, assim como endossa, irrestritamente, os feitos conscientizadores redigidos nesse tópico, buscando, sobremodo, o desenvolvimento contínuo de tais práxis, diante do presente e irrefreável desenvolvimento tecnológico.

5.8 - GOVERNANÇA COM AS ÁREAS DE NEGÓCIO E TECNOLOGIA

As iniciativas e projetos de quaisquer outras áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança cibernética e da informação, garantindo a confidencialidade, integridade e disponibilidade das informações no ambiente virtualizado.

5.9 - SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS DE APLICAÇÃO E NA ADOÇÃO DE NOVAS TECNOLOGIAS

O processo de desenvolvimento de sistemas de aplicação e adoção de novas tecnologias deve garantir a aderência às políticas de segurança cibernética e da informação colapsadas pela FIDÚCIA SCMEPP e às boas práticas de segurança e governança de Tecnologia da Informação, citando, a título ilustrativo, os protocolos ITIL e COBIT.

Adjacentemente, todos sistemas desenvolvidos internamente ou por

terceiros, devem possuir, mas não se limitar, a exaustivas medidas testificadoras por parte da instituição, a fim de conferi-lo segurança, eficiência e alinhamento às exigências legais e regulamentes cuja FIDÚCIA SCMEPP se apercebe suscetível.

5.10 - GRAVAÇÃO DE LOGS

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional de forma a permitir identificar os seguintes fatores: É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional de forma a permitir identificar os seguintes fatores:

a) quem fez o acesso: identificação do colaborador ou prestador que realizara tal acesso;

b) quando o acesso foi feito: mensuração da data e hora em que o evento ocorrera;

c) o que foi acessado: desdenhar, irrefutavelmente, telas, funções e recursos acessados, bem como ressoar qualquer emissão ou download de documentos exarados pelo sistema abordado;

d) como foi acessado: identificar o meio de acesso, por meio do IP (Internet Protocol) e MAC (Media Access Control), minimamente, dos subsídios utilizados pelo proponente.

As informações dos registros (logs) ou trilhas de auditoria devem ser protegidas contra modificações e acessos não autorizados e estar, oportunamente, à disposição da Diretoria e do Banco Central do Brasil mediante qualquer pleito oficiado.

5.11 - PROGRAMA DE REVISÃO E APERFEIÇOAMENTO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

O supra programa é norteado pelos seguintes fatores:

a) regulamentações vigentes: mensuração, pelo departamento competente, dos principais direcionadores das atividades concernentes à Política em comento;

b) melhores práticas: cômputo das práticas difusas e aceitas no mercado, a fim de patrocinar uma ambiência indelével no tocante à segurança e assegurar que os sistemas estarão eivados de aceitação em todos os dispositivos em que forem empregues.

Aprofundando o campo de análise, envida-se, conforme sua criticidade, as seguintes posturas:

a) ações críticas: consiste em correções emergenciais e imediatas para mitigar riscos iminentes e possíveis desalinhamentos às asserções escrevinhadas acima;

b) ações de sustentação: iniciativas de curto / médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da organização e permitindo que ações de longo prazo/estruturantes possam ser realizadas;

c) ações estruturantes: iniciativas de médio / longo prazo que tratam a causa raiz dos riscos e que preparam a FIDÚCIA SCMEPP para o desenvolvimento dos recursos atualmente cadenciados na organização.

5.12 - PROTEÇÃO DO PERÍMETRO CIBERNÉTICO E DA INFORMACIONAL

Para proteção da infraestrutura contra um ataque externo, emprega-se ferramentas e controles contra:

a) ataques que afetem a disponibilidade (DDoS);

b) spam;

c) phishing;

d) ataques avançados persistentes (APT);

e) malware;

f) invasão de dispositivos de rede e servidores;

g) ataques de aplicação e scan externos.

Apensando o exposto, a FIDÚCIA SCMEPP vale-se de diversas ferramentas preventivas contra vazamento de informação, instaladas em estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além de criptografia e autenticações em meios eletrônicos usados pela instituição, ponderados por mecanismos que rastreiam toda a movimentação e troca de arquivos e afins nos sistemas e recursos tecnológicos utilizados pela organização.

De maneira subjacente ao prisma tecnológico, a prevenção ao vazamento de informação é materializada fisicamente junto aos colaboradores mediante assinatura de NDA que preveja, indistintamente, a repudia a qualquer veiculação de dados e informações inerentes, direta ou indiretamente, à instituição.

5.13 - TESTES PERIÓDICOS DE VARREDURAS E DETECÇÃO DE VULNERABILIDADES

Em periodicidade anual, minimamente, a FIDÚCIA SCMEPP realizará uma varredura em seus sistemas de modo a mapear qualquer vulnerabilidade, partindo das nuances estilizadas nessa Política. Assim, identificar-se-á, por meio desse procedimento, possíveis brechas encontradas na ambiência, que deverão ser classificadas em harmonia ao versado no tópico "Tratamento de Incidentes de Segurança Cibernética e da Informação".

Tal realização encontra plena aplicabilidade na priorização dos eventos que deverão ser abordados açodadamente, aplicando aquela estratégia que melhor se coadune à fissura detectada, em linha com os dispositivos aqui emergidos. Além disso, tais testes e possíveis incorreções apontadas deverão ser oficializados no relatório de testes periódicos de varreduras e detecção de vulnerabilidade que delineiem, minuciosamente, todos os desdobramentos da ocorrência.

5.14 - ELABORAÇÃO DE CENÁRIO DE INCIDENTES CONSIDERADO NOS TESTES DE CONTINUIDADE

À obviedade, deve-se realizar testes vislumbrando testificar qual será a reação da instituição e de seus colaboradores mediante a instauração de alguma incidência na rotina normalmente observada. Adicionalmente a isso, tais testes não devem ser realizados aleatoriamente, mas sim guardar relação direta com os eventos que podem se justapor nos meandros organizacionais, principalmente aqueles afetos ao universo cibernético.

Nisso, deve-se registrar, mediante os testes efetuados, quais são as implicações observadas na normalidade daquele processo, realizações necessárias para a continuidade paliativa daquele processo (reinício), assim como as posturas de longo prazo que visionem a normalização daquele processo

Para conferir a eficiência necessária ao processo, os resultados apercebidos nos supramencionados testes deverão ser guindados no Relatório de Testes de Continuidade, condensando todas as informações acima arroladas, de forma a patrocinar a assunção de atividades saneadoras àquelas máculas observadas que podem se converter em desastres se não tratados corretamente.

Primeiramente, considerar-se-á, nos testes aqui abalroados, os incidentes de maior reincidência no exercício imediatamente anterior ou cuja ocorrência se apresente desmedida vertiginosamente, instaurando a necessidade de análises e testes de continuidade intuindo não comprometer a lisura processual. Nisso, mediante os relatórios de incidência preenchidos, quando da sucessão de tais eventos, mensurar-se-á quais tópicos devem ser primeiramente tratados

Em outro prisma, dada a experimentação já observada nessa instituição, elenca-se, abaixo, cenários que deverão ser testados a reboque daqueles identificados na forma do parágrafo anterior, posta a sua importância e no dia a dia institucional:

INCIDENTE:	POSSÍVEIS CAUSAS A SEREM TESTADAS:
Interrupção de energia elétrica	Fatores externos inerentes à rede ou à localidade em que as instalações prediais se encontram; Fatores internos que comprometem a rede interna, tais como curto-circuito, infiltrações, etc.; Sobrecarga da rede atualmente instalada.
Superaquecimento de ativos	Falha no sistema de climatização e arrefecimento.
Indisponibilidade de dados	Servidores instáveis ou indisponíveis; Backup indisponível ou sem integridade.
Falha na rede de internet	Obstrução do sinal por fatores externos, como falhas no provedor, rompimentos de cabos, etc; Mau funcionamento de recursos internos, tais como switchs, roteadores, etc.
Ataques cibernéticos a servidores	Falha no firewall e demais itens de segurança; Furto de senhas e demais credenciais de segurança.
Incêndio	Casos fortuitos.
Desastres naturais	Casos fortuitos.
Falha de hardware	Equipamentos defasados ou inaptos à utilização; Desempenho ínfimo diante do necessário.
Desempenho ínfimo diante do necessário	Colaborador negligente ou falha humana; Proteção física dos ativos ineficiente.

5.15 - PRAZOS ESTIPULADOS PARA REINÍCIO OU NORMALIZAÇÃO DAS ATIVIDADES

Em linha com o disposto no capítulo “Tratamento de Incidentes de Segurança Cibernética e da Informação e Continuidade de Negócios”, os incidentes são

classificados por níveis de criticidade, de acordo com seus desdobramentos e profundidade de seus efeitos dilaceradores.

Por óbvio, quão maior a dificuldade no saneamento de tal gargalo, maior será o prazo para reinício ou normalização daquela atividade. Nada obstante, há de se ter claro que algumas incorreções apresentarão processos paliativos que poderão ser invocados concomitante à sucessão da incidência, forjando contributos para um reinício com maior celeridade do processo atingido pelo evento danoso.

Nisso, ventila-se, no quadro abaixo, os prazos a serem observados, segregando-se pela tipicidade de incidentes decretada acima, assim como pela existência, ou não, de atividades suplementares à mesma. A reboque, disseca-se, ainda, o reinício da normalização, ao passo que essa última consiste no realinhamento igualitário da atividade nos moldes anterior a ocorrência dos incidentes e aquele à consecução operacional, por meio de qualquer forma usada para tanto:

	Prazo de Reinício		Prazo de Normalização
Tipicidade de Incidência	Existência de processos paliativos	Inexistência de processos paliativos	Existência de processos paliativos
Altamente críticos	2h	6h	7 dias
Medianamente críticos	30 minutos	2h	4 dias
Reduzidamente críticos	Imediato	30 minutos	2 dias

Abordando com maior minudência, pondera-se a volatilidade das ocorrências e do prazo de arrumação das mesmas. Nisso, torna-se patente desde já que os períodos acima engradados tangenciam ao interregno máximo a ser observado para a conclusão do evento ao qual aquele intervalo remete, podendo, tal realização, ser levado a cabo em menor decurso de tempo. Sem embargo, se tal prazo expirar e, por consequência, aperceber inobservância, tal cenário deverá ser grassado ao Banco Central do Brasil, nos moldes abaixo circunscritos.

5.16 - COMUNICAÇÃO AO BANCO CENTRAL DO BRASIL

Quando da ocorrência de incidentes e da inobservância fortuita aos prazos

estabelecidos na forma do tópico “Prazos estipulados para reinício ou normalização das atividades”, as situações, principalmente aquelas que angariem interrupções dos serviços considerados relevantes, deverão ser pronta e tempestivamente comunicadas ao Banco Central do Brasil, oficiando tal deliberação no Relatório de Comunicação de Incidentes Relevantes ao Banco Central do Brasil.

Nisso, encampa-se que tal delato deverá ser levado a cabo na iminência de consecução de dois fatos considerados agravantes do quadro atual da instituição:

a) descumprimento do prazo saneador, em função de complicações ou cenário dificultosos que potencializem o teor deletério do fato ocorrido, ou que acometam intransponíveis óbices ao retorno das atividades, diante de incidentes relevantes;

b) fato que reverbere imediata paralisação das atividades naquelas situações em que as mesmas não poderão ser levadas a cabo do modo previsto no “Plano de Ação e de Respostas a Incidentes”

A partir disso, paralelamente ao exarar do supra relatório, a equipe de Tecnologia da Informação e, a seu critério, demais departamentos da FIDÚCIA SCMEPP deverão atuar com extremo afinco na dissolução do gargalo, seja no âmbito de restabelecimento do sistema ou mesmo na idealização de processos paliativos e que não configurem a obstrução total do processo.

6 - PLANO DE AÇÃO E DE RESPOSTAS A INCIDENTES NA FIDÚCIA SCMEPP.

Em linha com os dispositivos legais e normativos que regem a matéria em alusão, encampa-se, em caráter superveniente na exegese das realizações procedurais aqui normatizadas, o plano de ação a seguir guindado, de forma a obter máxima eficiência no cumprimento dos detalhes objetos desse documento, assim como no tratamento de possíveis incidências.

Nesse panorama, redigir-se-ão as ações, rotinas, procedimentos, controles e tecnologias a serem levadas a cabo consoante os tópicos a seguir:

a) preparação: essa etapa ocorre anteriormente à incidência, em linha com o tópico, a seguir versado, "Conscientização em Segurança Cibernética e da Informação". Nisso, considera-se capital o conhecimento de todas as nuances, diretrizes e demais procedimentos pactuados nessa Política e demais documentos assemelhados a esse. Por conseguinte, todos os colaboradores, no ato de sua integração, serão submetidos à leitura dessas laudas e demais normativos que desovam as ações afetas a essa temática, bem como, na ocorrência de qualquer atualização, serão cientificados dos procedimentos adicionados / excluídos / incrementados. A partir desse cenário, torna-se substancial a ciência ineludível dessa carga diretiva, constituindo-se no ponto de fricção desse plano de ação;

b) identificação: em posse do âmbito preparatório, os colaboradores estarão aptos a identificar qualquer evento que se furte à normalidade dos fatos costumeiramente observados. Ademais, em linha com o disposto no tópico "Segurança no Desenvolvimento de Sistemas de Aplicação e na Adoção de Novas Tecnologias" as plataformas utilizadas deverão estar munidas de recursos que expilam, de pronto, notificações, avisos e comunicação a despeito de qualquer incidente em ocorrência ou que poderão ocorrer em virtude de qualquer desídia no tocante à manipulação desse gargalo;

c) classificação e contenção: uma vez identificada a incidência, tal gap deverá ser classificado na forma do capítulo "Tratamento de Incidentes de Segurança Cibernética e da Informação", a fim de agremiar tratativas assertivas aos acontecimentos. Diante desse cenário, a equipe de Tecnologia da Informação deverá ser acionada para conter o ponto destoante, tendo primazia pela contenção e inocorrência de qualquer óbice à consecução operacional do processo que sedia o deletério evento. Ao se deparar com tais cenários, adotar-se-á uma ou mais das seguintes medidas:

7 - BASE LEGAL, INFRALEGAL E REFERENCIAL.

A Fidúcia SCMEPP, enquanto instituição devidamente regulada pelo BANCO CENTRAL DO BRASIL, observa, irrestrita e ininterruptamente, os normativos emanados desta autarquia, com o fito de atuar em consonância às melhores práticas no tangente ao Gerenciamento do Risco Cibernético, reconhecidas globalmente e transcritas pelo BC, por meio dos supramencionados textos reguladores.

Nessa seara, consigna-se a Resolução 4.893, emanada do Conselho Monetário Nacional e difundida pelo Banco Central do Brasil, como um dos pilares para o tratamento de assuntos atinentes ao Gerenciamento de Risco Cibernético. A reboque desse normativo, encampa-se outros textos que, de igual forma, delimitam e disciplinam a atuação das instituições reguladas e fiscalizadas pelo BC, sem os quais, ou mesmo na iminência de tergiversação às premissas ali compenetradas, tal gerenciamento torna-se deficiente ou mesmo inócuo face à premente necessidade do estabelecimento de políticas nesse mote. Nisso, quando o assunto assim requerer, o documento citar-se-á no capítulo que melhor lhe aprouver.

Cumpre atestar que, além dos normativos legais e infralegais supraditos, que são o fulcro basilar para as diligências concernentes ao tema aqui aludido, a FIDÚCIA SCMEPP se incumbe de buscar, taxativa e incessantemente, previsões, acordos, tratados e demais leis que regulem a matéria de fato, intuindo tornar inexequível qualquer ato que se apresente de maneira contraventora às redações desferidas em tais textos, ou, na hipótese de tal mácula ocorrer, que seja precipuamente identificada, avalizada e severamente desbaratada, consonântico às premissas aqui sugestionadas e às exigências impetradas no conjunto legal e infralegal guindadas nesse documento.

8 - DIVULGAÇÃO INTERNA DA POLÍTICA DE GERENCIAMENTO DE RISCO CIBERNÉTICA

Além da redação levada a cabo nessa política, impende-se levá-la à baila, vislumbrado proporcionar aos colaboradores internos, em qualquer momento, a possibilidade de tempestiva consulta ao texto aqui condensado, a fim de deletar dúvidas que possam insurgir ou mesmo se nortear mediante qualquer ocorrência pautada nesse documento.

O amplo acesso a estas informações pelo público interno é indispensável, a fim de instrumentalizar os colaboradores para o desenvolvimento de suas atividades e a tomada de decisões em um ambiente de transparência e comprometimento com as praxes aqui abalroadas.

Outrossim, com tal veiculação encabeça-se altivas bases de transparência, bom atendimento às demandas atinentes, em conivência com a toda a carga legal e infralegal que regulam, taxativamente, o setor de atuação da FIDÚCIA SCMEPP, assim como estabelecer um engajamento inequívoco por parte dos colaboradores, posto a desmedida importância desse tópico em meio às nuances de instituições da tipicidade da FIDÚCIA SCMEPP.

Dado isso, o primeiro contato do colaborador com esse documento arregimentar-se-á no momento de sua integração junto ao quadro de colaboradores, no qual o presente documento será apresentado. A reboque de tal previsão, instruir-se-á esse mesmo colaborador a efetuar a leitura do documento em sua concretude, a fim de que os pontos abordados sejam consensados em todo o espectro de time de colaboradores

Enriquecendo o tema, os canais de comunicação utilizados pela FIDÚCIA SCMEPP para a divulgação de informações institucionais pertinentes a essa Política foram seletamente escolhidos, a fim de irrigar a base técnica dos prepostos e colaboradores, principalmente daqueles que atuam na linha de frente no relacionamento com os clientes. A definição do canal, ou do conjunto de canais, a ser empregado em cada situação, dependerá do tipo de informação e do colaborador a que se destina:

a) reuniões periódicas: intui-se rever os principais pontos atinentes à Política, assim como discutir sua efetividade;

b) intranet: é uma ferramenta estratégica, por meio do qual a FIDÚCIA SCMEPP capilariza a política, assim como demais políticas da instituição, a fim de prover um repositório de acesso tempestivo e democrático;

c) e-mails corporativos: despacho de e-mails com as principais notícias

veiculadas em mídias de comprovada verossimilidade, assim como de novas leis, regulamentos ou comunicados que influam no tema, observadas nos sítios da internet dos órgãos anuentes.

No âmbito externo, aos fornecedores, parceiros e público em geral, tal documento manter-se-á disponível por meio de uma página web, acessível em Política de Gerenciamento do Risco Cibernética (fiduciascm.com.br), em que arregimentar-se-á a correta leitura por parte do stakeholder interessado na leitura. Ademais, aqui se torna patente que quaisquer dúvidas no tocante ao aqui verbalizado poderão ser dirimidas pelos canais de atendimento da FIDÚCIA SCMEPP, acessíveis pelos seguintes meios:

a) email: atendimento@fiduciascm.com.br;
b) tel: (15) 3442-6400.
Baixe o App

Google Play Apple Store
Nos siga nas Redes Sociais

Facebook Instagram Linkedin

Fale com a gente:
Atendimento: (15) 3442-6400

Ouvidoria: 0800 067 5757

E-mail: atendimento@fiduciascm.com.br