SPC GRAFENO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

SPC GRAFENO INFRAESTRUTURA E TECNOLOGIA PARA O SISTEMA FINANCEIRO S.A.

SUMÁRIO

1. OBJETIVO 5
2. ABRANGÊNCIA 5
3. DOCUMENTOS DE REFERÊNCIA 5
4. ALÇADAS DE APROVAÇÃO 6
5. CONCEITOS GERAIS 6
6. PAPÉIS E RESPONSABILIDADES 6
6.1. CONSELHO DE ADMINISTRAÇÃO 6
6.2. COMITÊ DE GERENCIAMENTO DE RISCOS 6
6.3. DIRETORIA DE DADOS E SEGURANÇA DA INFORMAÇÃO 7
6.4. DIRETORIA DE TECNOLOGIA 7
6.5. COLABORADORES, TERCEIROS, FORNECEDORES, PARCEIROS E PARTES INTERESSADAS DA COMPANHIA 8
7. DIRETRIZES GERAIS 8
8. INVENTÁRIO E CONTROLE DE DISPOSITIVOS CORPORATIVOS 9
8.1. INSTALAÇÃO E UTILIZAÇÃO DE SOFTWARES 9
8.2. SEGURANÇA DE MÍDIAS DE ARMAZENAMENTO 9
8.3. GESTÃO DE ATIVOS DE TECNOLOGIA 10
8.4. USO DE EQUIPAMENTOS 10
8.4.1. Bring Your Own Device (BYOD) 10
9. PROTEÇÃO DE DADOS E INFORMAÇÕES 10
9.1. PREVENÇÃO A VAZAMENTO DE INFORMAÇÕES 10
9.2. TRILHAS DE AUDITORIA (RASTREABILIDADE) 11
9.3. CLASSIFICAÇÃO DA INFORMAÇÃO 11
9.4 GUARDA E DESLOCAMENTO DE INFORMAÇÕES 12
9.5. DESCARTE DE INFORMAÇÕES 12
10. CONFIGURAÇÃO SEGURA DE ATIVOS E SOFTWARE CORPORATIVOS 12
10.1. GESTÃO DE RISCOS DE SEGURANÇA 12
10.2. CONTROLE CONTRA SOFTWARE MALICIOSO 13
10.3. CRIPTOGRAFIA 13
11. GESTÃO DE INFRAESTRUTURA DE REDE 13
11.1. SEGMENTO DE REDES NA PLATAFORMA 13

11.2. RESILIÊNCIA DA PLATAFORMA 14
12. GESTÃO DE ACESSOS 14
12.1. CONCESSÃO DE ACESSO PARA SISTEMAS/APLICAÇÕES 14
12.2. CONCESSÃO DE ACESSO PARA BANCO DE DADOS 14
12.3. POLÍTICA DE SENHAS 15
12.4. REVOGAÇÃO DE ACESSOS 15
12.5. ACESSO FÍSICO 15
12.6. ACESSO REMOTO 16
13. GESTÃO CONTÍNUA DE VULNERABILIDADES 16
13.1. SCAN DE VULNERABILIDADES (MENSAL) 16
13.2. PENTEST INTERNO (TRIMESTRAL) 17
13.3. PENTEST EXTERNO (SEMESTRAL) 17
14. PROTEÇÃO PARA NAVEGAÇÃO WEB E E-MAIL 17
14.1. USO DA INTERNET 17
14.2. USO DO CORREIO ELETRÔNICO (E-MAIL) 18
15. RECUPERAÇÃO DE DADOS 18
15.1. RECUPERAÇÃO DE DESASTRE E DE CONTINUIDADE DOS NEGÓCIOS 18
15.2. PROCEDIMENTO DE BACKUP E RESTORE DE DADOS 18
16. DESENVOLVIMENTO SEGURO 19
16.1. CICLO DE DESENVOLVIMENTO OU ATUALIZAÇÃO DE SISTEMAS 19
16.2. GESTÃO DE MUDANÇAS 19
17. GESTÃO DE TERCEIROS 20
17.1. GESTÃO DE RISCOS DE SEGURANÇA EM TERCEIROS 20
17.2. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO, ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM 21
18. RESPOSTA A INCIDENTES 21
18.1. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 21
19. CONSCIENTIZAÇÃO DE SEGURANÇA 22
20. PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO 23
21. AVALIAÇÃO DE EFETIVIDADE DE SEGURANÇA DA INFORMAÇÃO 23
21.1. AVALIAÇÃO DE MATURIDADE DE SEGURANÇA 23
21.2. RELATÓRIO ANUAL DE EFETIVIDADE 23
22. DISPOSIÇÕES GERAIS 24

22.1. VIGÊNCIA 24
22.2. CASOS OMISSOS 24
22.3. DIVISIBILIDADE 24
23. REVISÃO DA POLÍTICA 24
24. VIOLAÇÕES 24
25. CONTROLE DE VERSÕES 24

1. OBJETIVO

A Política de Segurança da Informação e Cibernética (“Política”) tem como objetivo principal estabelecer as diretrizes para aplicar os controles necessários a fim de promover a segurança das informações da SPC Grafeno Infraestrutura e Tecnologia para o Sistema Financeiro S.A. ("Companhia"), em conformidade com a Resolução BCB nº 304/23.

Através dessa política, busca-se garantir a proteção adequada dos ativos de informação da empresa, prevenir incidentes de segurança, promover boas práticas e assegurar a conformidade com as regulamentações aplicáveis.

Estes controles visam os três principais aspectos da informação: confidencialidade, integridade e disponibilidade.

2. ABRANGÊNCIA

Os procedimentos descritos nesta Política são aplicáveis à Companhia, a todos os seus Colaboradores, e Prestadores de Serviços Terceirizados.

Esta Política deverá ser amplamente divulgada dentro da Companhia e disponibilizada a todos os integrantes e stakeholders do processo.

3. DOCUMENTOS DE REFERÊNCIA

- Código de Ética e Conduta
- Política de Gerenciamento de Riscos e Controles Internos
- Política de Governança e Compliance
- Plano Diretor de Segurança da Informação
- Manual de Gestão de Acesso
- Processo de Offboarding
- Política de Gestão de Terceiros
- Plano de Resposta a Incidentes
- Plano de Continuidade de Negócios
- Plano de Recuperação de Desastres
- Manual de Boas Práticas em Desenvolvimento Seguro

- Guia de Uso Aceitável
- Resolução BCB nº 304/2023 - Regulamenta a atividade de Registro de Ativos Financeiros
- Lei n° 13.709/2018 – Lei Geral de Proteção de Dados
- *Guidance on cyber resilience for financial market infrastructures* – BIS/IOSCO

4. ALÇADAS DE APROVAÇÃO

- Área de Segurança da Informação – responsável pela elaboração e revisão da Política;
- Comitê de Gerenciamento de Riscos – responsável pela revisão e aprovação em 1ª instância da Política;
- Conselho de Administração – responsável pela aprovação final da Política.

5. CONCEITOS GERAIS

Serão considerados como principais aspectos da segurança da informação, os seguintes itens:

- **Confidencialidade:** garante que a informação seja acessada apenas por colaboradores que tenham permissão;
- **Integridade:** garante que a informação acessada esteja correta e íntegra;
- **Disponibilidade:** garante que a informação esteja disponível no momento necessário.

Todas as diretrizes e controles desta política consideram como pilares da segurança da informação os colaboradores, processos e tecnologia.

6. PAPÉIS E RESPONSABILIDADES

6.1. CONSELHO DE ADMINISTRAÇÃO

- Avaliar e aprovar as diretrizes de segurança da informação, como as Políticas e procedimentos voltados ao tema;
- Aprovar o Plano Diretor de SI.

6.2. COMITÊ DE GERENCIAMENTO DE RISCOS

- Avaliar as Políticas e Procedimentos relacionados à segurança da informação e sugerir alterações, quando necessário;
- Avaliar o Plano Diretor de SI e sugerir alterações, quando necessário;

- Designar, definir ou alterar as atribuições da área de Segurança da Informação;
- Aprovar as principais iniciativas para a melhoria contínua das medidas de proteção para detectar vulnerabilidades e artefatos maliciosos, monitorar e analisar possíveis ataques;
- Apoiar a implantação de soluções para eliminação ou minimização dos riscos;
- Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;
- Suportar perante toda a Companhia as iniciativas da área de Segurança da Informação.

6.3. DIRETORIA DE DADOS E SEGURANÇA DA INFORMAÇÃO

- Auxiliar no processo de elaboração, padronização, revisão anual, aprovação e publicação de políticas da sua área;
- Planejar, coordenar, organizar, supervisionar e dirigir as atividades relativas ao processo de utilização e de governança de dados da Plataforma, como armazenamento e salvaguardas a serem adotadas;
- Manter a base de dados de eventos e perdas de riscos operacionais devidamente atualizada;
- Definir princípios e diretrizes para disseminação da cultura de governança de dados, incluindo treinamentos;
- Monitorar a estrutura de segurança cibernética de modo a atender os requisitos internos;
- Assegurar a implementação das Políticas de Segurança Cibernética e de Segurança da Informação em todos os aspectos relacionados à governança e segurança de dados;
- Definição políticas e acompanhamento dos processos que visam a proteção de dados sensíveis, cibersegurança, controle de acessos, detecção e mitigação de eventuais ataques;
- Gerir a segurança da informação e cybersecurity da Companhia;
- Identificar e gerir o risco regulatório, no âmbito da sua esfera de competência; e
- Atividades relacionadas ao cumprimento das políticas de gerenciamento de riscos e controles internos e gestão de terceiros.

6.4. DIRETORIA DE TECNOLOGIA

- Realizar a contenção de incidentes de segurança;
- Identificar e apurar as vulnerabilidades detectadas pela área de Segurança da Informação/Cibersegurança;
- Revisar e atualizar periodicamente o plano de resposta a Incidentes para garantir sua eficácia contínua;
- Realizar monitoramento constante da infraestrutura tecnológica sobre a capacidade de processamento, bem como sobre os alertas que possam identificar incidentes de segurança e cyber;
- Revisar e atualizar anualmente o Plano de Recuperação de Desastres (PRD);

- Garantir a recuperação dos sistemas de informação.
- Realizar regularmente testes de contingência para avaliar a capacidade de resposta da organização em cenários de emergência.

6.5. COLABORADORES, TERCEIROS, FORNECEDORES, PARCEIROS E PARTES INTERESSADAS DA COMPANHIA

- Preservar a integridade e guardar sigilo das informações que fazem uso;
- Zelar e proteger os equipamentos disponibilizados para a realização do seu trabalho;
- Transitar informações somente nos canais oficiais homologados e aprovados por Tecnologia e Segurança Cibernética;
- Comunicar ao seu superior imediato qualquer irregularidade, desvio, violação desta Política e/ou das demais normas e procedimentos de segurança da informação.
- Relatar o mais rápido possível à área de Segurança da Informação qualquer tipo de evento e fragilidades que possam causar danos de segurança aos ativos da empresa por meio de registro de Incidente da SPC Grafeno.
- Cumprir as determinações desta Política e demais normas, sob pena de incorrer nas sanções disciplinares e legais cabíveis.

7. DIRETRIZES GERAIS

Classificação de Dados: Definir categorias de classificação de dados (públicos, internos, confidenciais etc.). Especificar o manuseio apropriado e os requisitos de proteção para cada categoria.

Acesso e Autenticação: Implementar autenticação multifator sempre que possível. Gerenciar privilégios de acesso com base no princípio do menor privilégio. Encorajar o uso de senhas fortes e mudanças periódicas.

Política de Senhas: Definir requisitos para a complexidade de senhas. Estabelecer a política de troca de senhas regularmente. Desencorajar o compartilhamento de senhas e o uso de senhas repetidas.

Monitoramento e Detecção: Implementar sistemas de monitoramento de rede e detecção de intrusões. Analisar regularmente os logs de sistemas e redes em busca de atividades suspeitas. Estabelecer procedimentos para responder a incidentes de segurança.

Atualizações e Patches: Manter sistemas operacionais, aplicativos e dispositivos atualizados com os últimos patches de segurança. Estabelecer uma política para avaliar, testar e implementar patches de forma consistente.

Criptografia: Utilizar criptografia para proteger dados em repouso e em trânsito. Encriptar dispositivos móveis e unidades de armazenamento removíveis. Garantir que as chaves de criptografia sejam gerenciadas de forma segura.

Política de Uso Aceitável: Definir diretrizes claras para o uso apropriado dos recursos de tecnologia da informação. Informar os funcionários sobre as consequências do uso indevido.

Proteção para Endpoints: Utilizar soluções antivírus/antimalware atualizadas. Implementar firewalls e filtragem de conteúdo. Realizar varreduras regulares em sistemas e dispositivos.

Treinamento e Conscientização: Fornecer treinamento regular em segurança da informação para funcionários. Promover a conscientização sobre ameaças cibernéticas e práticas seguras.

Backup e Recuperação: Realizar backups regulares dos dados críticos e sistemas. Testar a recuperação dos dados para garantir a eficácia do processo.

Controle de Dispositivos: Implementar políticas de BYOD (Bring Your Own Device) com diretrizes claras de segurança. Utilizar soluções de gerenciamento de dispositivos móveis para controlar o acesso e as configurações dos dispositivos.

Monitoramento de Terceiros: Avaliar a segurança dos fornecedores terceirizados e parceiros de negócios.

8. INVENTÁRIO E CONTROLE DE DISPOSITIVOS CORPORATIVOS

8.1. INSTALAÇÃO E UTILIZAÇÃO DE SOFTWARES

É vedada a instalação de softwares sem licença, provenientes da internet, ou que de alguma forma tragam riscos ao nosso ambiente. Portanto, todos softwares utilizados pelos colaboradores da Companhia devem ser homologados pelas áreas de tecnologia e *cybersecurity.*

Este controle é detalhado no documento interno “**Guia de Uso aceitável**”.

8.2. SEGURANÇA DE MÍDIAS DE ARMAZENAMENTO

O armazenamento de dados deve ser realizado apenas nas ferramentas disponibilizadas pela Companhia, como por exemplo, o *Sharepoint e One Drive*.

8.3. GESTÃO DE ATIVOS DE TECNOLOGIA

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

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

- **Planejamento:** Alinhamento da estratégia corporativa com as ações de Tecnologia. Nessa fase é observado a revisão dos ativos que são utilizados, análise de custos de compra e instalação dos novos ativos;
- **Aquisição:** Definição do padrão técnico, fornecedores e acordos contratuais;
- **Implantação:** Configuração e instalação técnica seguindo os padrões estabelecidos anteriormente;
- **Gerenciamento:** Controle de inventário, apoio técnico, manutenção, atualização e monitoramento desses ativos;
- **Descarte:** Processo realizado quando um bem perde sua utilidade e torna-se antieconômico.

O controle da gestão desses ativos está detalhado no documento interno "**Guia de Uso Aceitável**".

8.4. USO DE EQUIPAMENTOS

Todo e qualquer equipamento utilizado nas dependências da SPC Grafeno deverá ter a ciência e o consentimento da área de Tecnologia da Informação.

8.4.1. Bring Your Own Device (BYOD)

Para garantir a proteção adequada dos dados e sistemas da SPC Grafeno, o uso de dispositivos móveis é possível desde que autorizado pelo gestor imediato e que cumpra os requisitos de segurança estabelecidos pela SPC Grafeno.

Estes controles estão detalhados no documento interno chamado "**Guia de Uso Aceitável".**

9. PROTEÇÃO DE DADOS E INFORMAÇÕES

9.1. PREVENÇÃO A VAZAMENTO DE INFORMAÇÕES

Através do controle preventivo de vazamento de dados e informações, a área de Segurança da Informação/Cyber, busca assegurar que dados confidenciais não sejam perdidos, roubados, mal utilizados, vazados, adulterados ou destruídos sem autorização por usuários não autorizados.

Os principais objetivos do controle são:

- Monitoramento e controle das atividades de *endpoints* (computadores, notebooks, ou qualquer outro dispositivo);
- Monitoramento e controle do fluxo de entrada e saída de dados da rede corporativa e softwares; e
- Proteção dos dados à medida que se movem (transferências e compartilhamentos autorizados).

9.2. TRILHAS DE AUDITORIA (RASTREABILIDADE)

Toda atividade na plataforma deve possuir recursos de trilha de auditoria para rastreabilidade. Esses registros devem ter os seguintes controles: controle de acesso, segregação física e/ou segregação de rede de modo a impedir o acesso e possível alteração por pessoas não autorizadas e com período mínimo de retenção de 5(cinco) anos.

Este controle é detalhado no documento **Manual de Boas Práticas em Desenvolvimento Seguro**.

9.3. CLASSIFICAÇÃO DA INFORMAÇÃO

O documento **Manual de Classificação da Informação**, descreve as 4 (quatro) classificações utilizadas pela SPC Grafeno e a forma de manuseio delas em diversos formatos de mídia:

Classificação	Risco	Exemplo de Informação
Público	Baixo	Apresentações institucionais, materiais de divulgação em sites públicos ou de forma pública no site da SPC Grafeno.
Uso Interno	Médio	Apresentações internas das mais diversas, trocas de informações entre áreas, materiais de divulgação interna, políticas e manuais não públicos e documentos e dados de processos internos.
Restrito	Alto	Operações financeiras ou de investimentos a serem realizadas ou em realização, documentos, dados pessoais e informações de sócios ou informações/operações de clientes e participantes.

Confidencial	Muito Alto	Planos de negócio, memorando ou atas de reuniões confidenciais, informações financeiras críticas, novos produtos e dados pessoais sensíveis.

9.4 GUARDA E DESLOCAMENTO DE INFORMAÇÕES

É vedado o compartilhamento de dados, pastas, e quaisquer informações constantes no diretório da Companhia. Os dados devem permanecer armazenados no recurso corporativo oficial adotado pela SPC Grafeno.

Apenas colaboradores autorizados podem compartilhar dados de propriedade da Companhia para terceiros.

9.5. DESCARTE DE INFORMAÇÕES

O descarte de informações será diferente para mídias físicas e mídias digitais. Abaixo segue a forma correta de descarte para cada uma delas:

- **Mídia física** (como por exemplo documentos impressos): deve ser utilizada fragmentadora de papel, para informações com classificação restrita ou confidencial. Para as demais classificações não se faz necessário o uso de fragmentadora;

- **Mídia digital** (como por exemplo um pen drive): a mídia deverá ser enviada para o *service desk* para que seja realizado o processo de *wipe* e, quando necessário, a mídia será destruída.

Temos também os dados armazenados em plataformas de terceiros. Quando terminado o contrato com estes fornecedores, a área de Segurança da Informação deverá ser acionada para providenciar esta exclusão de forma segura.

10. CONFIGURAÇÃO SEGURA DE ATIVOS E SOFTWARE CORPORATIVOS

10.1. GESTÃO DE RISCOS DE SEGURANÇA

Os processos para o gerenciamento de riscos de Segurança da Informação e Cibernética, preveem, dentre outros, a identificação de ativos de informação críticos, a avaliação de ameaças e vulnerabilidades, bem como a classificação dos ativos e informações de acordo com a sensibilidade.

Os riscos e os planos de ações são acompanhados, inclusive, pela área de Riscos e Controles Internos da Companhia e o monitoramento apresentado, periodicamente, ao Comitê de Gerenciamento de Riscos.

10.2. CONTROLE CONTRA SOFTWARE MALICIOSO

O controle contra software malicioso se refere a um conjunto de medidas e práticas que são implementadas para proteger sistemas de computador e redes contra softwares maliciosos, também conhecidos como malware. Malware é um termo genérico que engloba uma variedade de programas de software projetados para causar danos, roubar informações, espionar ou realizar outras atividades prejudiciais em sistemas de computador, dispositivos móveis e redes.

Os controles contra software malicioso visam identificar, prevenir, detectar e mitigar a presença e os efeitos do malware.

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

10.3. CRIPTOGRAFIA

A criptografia é o uso das técnicas de comunicação seguras que permitem que apenas o remetente e o destinatário pretendido de uma mensagem visualizem seu conteúdo.

Considerando que todos os sistemas da SPC Grafeno são WEB, todas as informações em trânsito deverão ser criptografadas através de certificados digitais. Informações em repouso, como banco de dados e estações de trabalho deverão também contar com recursos de criptografia.

11. GESTÃO DE INFRAESTRUTURA DE REDE

11.1. SEGMENTO DE REDES NA PLATAFORMA

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

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

Para solicitação de acesso aos dispositivos de rede, a área de Segurança da Informação deve analisar a topologia de rede, os protocolos e os riscos para o ambiente, podendo aprovar ou não.

11.2. RESILIÊNCIA DA PLATAFORMA

Todas os produtos da SPC Grafeno foram construídos seguindo o conceito de resiliência por padrão, tendo todos os seus componentes replicados em pelo menos dois ambientes que funcionam em sincronismo para que não haja perda de informações e tenha baixo tempo de resposta a indisponibilidades.

Este nível de resiliência também é exigido dos fornecedores de serviços críticos.

12. GESTÃO DE ACESSOS

12.1. CONCESSÃO DE ACESSO PARA SISTEMAS/APLICAÇÕES

Para concessão de acessos às aplicações/sistemas da SPC Grafeno, o solicitante abrirá um chamado ao Service Desk através da ferramenta específica da área.

O fluxo de concessão de acessos às aplicações/sistemas, conterá as seguintes premissas:

- Conter aprovação do gestor (superior direto) e/ou do responsável da aplicação, para o caso de aplicações/sistemas com restrições de licença, dados confidenciais, dentre outros;
- Ser concedida de forma que restrinja o acesso apenas às atividades do colaborador e/ou prestador de serviço, de acordo com a matriz de segregação de função, e de acordo com os tipos de perfis oferecidos por cada sistema em particular;
- A solicitação de acessos para prestadores de serviços deve ser registrada pelo gestor responsável por meio da ferramenta de chamados e será realizada em caráter temporário, com data de expiração. Caso seja necessário a prorrogação dos acessos, compete ao gestor responsável pelo recurso solicitar renovação por meio de abertura de chamado na ferramenta com a devida justificativa.
- O acesso sempre será concedido baseado na necessidade para o cumprimento das atividades de trabalho do colaborador, relacionadas com o cargo ou função.

O procedimento para a concessão de acessos, está contido no documento “**Manual de Gestão de Acesso**”.

12.2. CONCESSÃO DE ACESSO PARA BANCO DE DADOS

Para concessão de acessos ao Banco de Dados da SPC Grafeno, o solicitante abrirá um chamado ao Service Desk através da ferramenta específica da área.

O fluxo de concessão de acessos ao Banco de Dados, conterá as seguintes premissas:

- Conter aprovação do gestor imediato e, obrigatoriamente, do Diretor de Tecnologia e do Head de Segurança da Informação;
- O acesso ao Banco de Dados, após as aprovações devidas, será liberado através da ferramenta de cofre de senhas, pela qual armazenará a rastreabilidade dos acessos (gravação e logs).

12.3. POLÍTICA DE SENHAS

O acesso ao ambiente de informações ocorre através de senhas de rede e de e-mails integrados. As senhas deverão satisfazer os seguintes requisitos de complexidade:

- Não conter partes significativas do nome da conta do usuário ou o nome todo;
- Ter pelo menos 08 (oito) caracteres de comprimento;
- Conter caracteres de três das quatro categorias a seguir: caracteres maiúsculos (A-Z), caracteres minúsculos (a-z), números (0-9) e caracteres especiais (ex.: !, $, #, %).
- Tempo Mínimo de Vida: 02 Dias
- Troca Periódica: a cada 90 dias
- Bloqueio por Tentativas Inválidas: 05 tentativas
- Possuir autenticação de 2 fatores (2FA) em todos os sistemas e softwares, aplicações, banco dados, entre outros sistemas da Companhia.

12.4. REVOGAÇÃO DE ACESSOS

Na ocorrência de desligamento de qualquer colaborador da Companhia, o acesso ao ambiente de informações (rede, sistemas, banco de dados, infraestrutura e aplicações) será bloqueado imediatamente, conforme especificado no documento **“Processo de Offboarding”.**

Nos casos de mudança de área e alteração de cargo, os acessos anteriormente concedidos deverão ser revogados e uma nova solicitação de acessos deverá ser realizada, para atendimento às funcionalidades que o colaborador exercerá na nova área ou novo cargo.

12.5. ACESSO FÍSICO

Seguindo a premissa da empresa de “remote first” o escritório da SPC Grafeno é um ponto para acesso à internet e reuniões, sem nenhum ativo de tecnologia relevante para os dados. Desta forma, os esforços estão concentrados na segurança dos notebooks e de acesso físico ao ambiente.

Para o acesso ao prédio da SPC Grafeno o colaborador utilizará o aplicativo de controle e liberação de acessos, devidamente autorizado pela equipe de Service Desk, assim como para acessar as portas internas do andar da Companhia no edifício.

Os equipamentos de acesso às portas e catracas, possuem log de acesso com o dia e horário.

12.6. ACESSO REMOTO

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

Todas as aplicações corporativas estão configuradas na modalidade *SaaS de cloud*, portanto, o acesso é realizado diretamente através da internet com os devidos controles de segurança.

13. GESTÃO CONTÍNUA DE VULNERABILIDADES

A gestão contínua de vulnerabilidades é o processo para garantir a segurança da informação e a proteção dos ativos da SPC Grafeno contra ameaças cibernéticas. Isso envolve a identificação, avaliação e mitigação de potenciais vulnerabilidades em sistemas, redes, aplicativos e infraestrutura. O processo inclui atividades como o scan de vulnerabilidades mensal, o pentest interno trimestral e o pentest externo semestral.

13.1. SCAN DE VULNERABILIDADES (MENSAL)

O scan de vulnerabilidades envolve o uso de ferramentas de segurança para identificar possíveis pontos fracos em sistemas e redes. Isso pode incluir configurações inadequadas, falhas de segurança conhecidas em softwares e outras brechas. O processo ocorre mensalmente e envolve as seguintes etapas:

- **Seleção de Ferramentas:** Escolher uma ferramenta ou conjunto de ferramentas de varredura de vulnerabilidades que sejam adequadas ao ambiente da Companhia;
- **Configuração:** Configurar as ferramentas de varredura para procurar vulnerabilidades específicas, seguindo padrões e diretrizes de segurança;
- **Varredura:** Executar a varredura nas redes, sistemas e aplicativos para identificar possíveis vulnerabilidades;
- **Coleta de Resultados:** Receber os resultados da varredura, que podem incluir uma lista de vulnerabilidades encontradas e suas classificações de gravidade;
- **Avaliação e Priorização:** Avaliar a gravidade e o impacto potencial de cada vulnerabilidade e priorizá-las com base em riscos;

- **Relatório:** Preparar um relatório detalhado que descreve as vulnerabilidades encontradas, os métodos utilizados para explorá-las e as recomendações para mitigação.

13.2. PENTEST INTERNO (TRIMESTRAL)

O teste de penetração (pentest) interno é uma avaliação mais aprofundada da segurança dos ativos digitais da Companhia. Os pentests envolvem a simulação de ataques reais para identificar brechas que podem não ser detectadas por ferramentas automatizadas. O processo inclui:

- **Planejamento:** Definir os objetivos do pentest, escopo, sistemas a serem testados e possíveis cenários de ataque;
- **Coleta de Informações:** Coletar informações sobre a infraestrutura e sistemas da empresa que serão testados.
- **Exploração:** Tentar explorar as vulnerabilidades identificadas para determinar se é possível acessar sistemas ou dados sensíveis.
- **Relatório:** Preparar um relatório detalhado que descreve as vulnerabilidades encontradas, os métodos utilizados para explorá-las e as recomendações para mitigação.

13.3. PENTEST EXTERNO (SEMESTRAL)

Um pentest externo é semelhante a um pentest interno, mas em vez de simular ataques de dentro da rede, ele simula ataques vindos do ambiente externo. Isso ajuda a avaliar a capacidade de defesa da empresa contra ameaças externas. O processo é semelhante ao pentest interno, mas os focos e os métodos de ataque podem variar.

14. PROTEÇÃO PARA NAVEGAÇÃO WEB E E-MAIL

14.1. USO DA INTERNET

O acesso a websites pelos colaboradores da SPC Grafeno deve seguir regras de conduta e segurança para garantir a experiência online de forma protegida. Essas diretrizes visam proteger os dados, privacidade e evitar potenciais ameaças cibernéticas.

O acesso à Internet será autorizado para os usuários que necessitarem desses recursos para o desempenho das suas atividades profissionais na Companhia.

Desta forma, não é permitido o acesso a sites que não estejam de acordo com as regras de segurança, sendo necessária a aderência ao Código de Ética e Conduta da SPC Grafeno.

14.2. USO DO CORREIO ELETRÔNICO (E-MAIL)

O correio eletrônico (e-mail) é um instrumento de comunicação interna e externa e deve ser utilizado prioritariamente para a execução de tarefas relacionadas à Companhia.

As mensagens devem ser escritas em linguagem profissional, não podendo comprometer a imagem ou os princípios éticos da Companhia.

O correio eletrônico (e-mail) é um instrumento de uso individual sendo o seu colaborador responsável por toda e qualquer mensagem enviada por meio de seu endereço.

Todas as informações trocadas via e-mail, são consideradas como propriedade da Companhia e podem ser monitoradas sem aviso prévio.

15. RECUPERAÇÃO DE DADOS

15.1. RECUPERAÇÃO DE DESASTRE E DE CONTINUIDADE DOS NEGÓCIOS

A Companhia possui procedimentos de recuperação de desastres e continuidade de negócios implementados para minimizar os impactos e perdas de ativos de informação em caso de incidente crítico.

Esses procedimentos incluem o mapeamento de processos essenciais, análise do impacto nos negócios e realização regular de testes periódicos de recuperação de desastres. Todas essas medidas são descritas nos documentos "**Plano de Continuidade de Negócios**" e "**Plano de Recuperação de Desastres**".

Todos os ativos que suportam os negócios da SPC Grafeno são mapeados e com os riscos mapeados (Análise de Impacto aos Negócios) e fazem parte dos testes periódicos de contingência.

15.2. PROCEDIMENTO DE BACKUP E RESTORE DE DADOS

O backup da plataforma SPC Grafeno é realizado através de imagens diárias completas do ambiente de produção, através de *Snapshots* armazenados em *Cloud* (nuvem).

O backup deve ser realizado considerando informações críticas utilizadas nas operações da Companhia e de acordo com a periodicidade e os procedimentos definidos pela área de Segurança da Informação. Não são realizados backups em estações de trabalho, portanto não devem ser utilizadas para armazenamento de dados.

O processo de restauração de dados e informações, deve ser testado periodicamente, para avaliar a disponibilidade e integridade das informações.

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

É vedado aos colaboradores armazenar arquivos pessoais, bem como realizar backups das informações da Companhia em dispositivos de mídia removíveis que possam estar conectados ao computador. A utilização de dispositivos de armazenamento somente deve ser permitida se justificada e aprovada pela área de Segurança da Informação, mediante a assinatura de um Termo de Responsabilidade pelo colaborador e monitoramento do processo.

16. DESENVOLVIMENTO SEGURO

16.1. CICLO DE DESENVOLVIMENTO OU ATUALIZAÇÃO DE SISTEMAS

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

- Definição de requisitos de segurança para novas demandas que impactarem ambientes críticos;
- Adoção de boas práticas para desenvolvimento seguro;
- Segregação lógica dos ambientes de desenvolvimento, teste/homologação e produção;
- Segregação de função no processo de desenvolvimento, teste e homologação e produção;
- Todo código-fonte desenvolvido, e obrigatoriamente anterior a sua implantação, deve passar por análise e validação de segurança; e
- Inventário, controle e gerenciamento seguro de APIs.

16.2. GESTÃO DE MUDANÇAS

O processo de gestão de mudanças é um conjunto estruturado de abordagens e atividades utilizadas para planejar e implementar as melhorias, correções e novos serviços da Companhia. Envolve a identificação das necessidades de mudança, a definição de metas claras, a comunicação eficiente com os stakeholders, a elaboração de um plano detalhado, a alocação de recursos adequados, a condução das alterações propostas e a monitorização contínua dos resultados.

O processo de gestão de mudanças também assegura que todas as solicitações sejam registradas, analisadas, autorizadas, priorizadas, planejadas, testadas, implementadas, documentadas e revisadas, em um processo formalizado e comunicado dentro da Companhia.

17. GESTÃO DE TERCEIROS

17.1. GESTÃO DE RISCOS DE SEGURANÇA EM TERCEIROS

A avaliação de terceiros sob o aspecto de segurança da informação é o processo para garantir que parceiros, fornecedores e prestadores de serviços externos atendam aos padrões de segurança exigidos pela Companhia. Nesse contexto e conforme detalhado na **Política de Gestão de Terceiros** da SPC Grafeno, são as seguintes atividades executadas:

- **Identificação de Terceiros Relevantes:** Identificação dos terceiros que têm acesso a informações confidenciais, sistemas ou processos críticos da Companhia e classificá-los com base na sensibilidade dos dados ou serviços que eles terão acesso.

- **Coleta de Informações:** Coleta das informações detalhadas sobre o terceiro, incluindo suas práticas de segurança da informação, histórico de incidentes de segurança e políticas internas, bem como realizar a avaliação de conformidade do terceiro com regulamentações e padrões relevantes de segurança.

- **Questionários de Due Diligence:** Preparar questionários ou avaliações detalhadas que abordem aspectos específicos da segurança da informação, como controle de acesso, gestão de vulnerabilidades e resposta a incidentes e solicitar que o terceiro preencha esses questionários de forma precisa e completa.

- **Análise de Respostas:** Analisar as respostas dos questionários para avaliar a maturidade e a eficácia das práticas de segurança do terceiro e identificar lacunas de segurança, se houver, e comparar as respostas com as políticas internas da organização.

- **Continuidade dos Negócios:** Avaliar os procedimentos a serem seguidos no caso da interrupção de serviços relevantes contratados, especialmente os de processamento e armazenamento de dados e de computação em nuvem contratados.

- **Avaliação de Riscos:** Avaliação dos riscos associados ao terceiro, considerando fatores como o tipo de acesso concedido, a sensibilidade dos dados compartilhados e a importância dos serviços prestados, determinando o nível de risco aceitável em relação à segurança da informação.

- **Contratos e Acordos de Segurança:** Incluir cláusulas contratuais que estabeleçam as obrigações de segurança do terceiro, incluindo requisitos específicos de conformidade.

- **Reavaliação Periódica:** Realizar reavaliações regulares da segurança dos terceiros para garantir que eles continuem atendendo aos padrões estabelecidos e ajustar as medidas de segurança conforme apropriado com base em mudanças no ambiente de ameaças ou nos requisitos regulatórios.

17.2. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO, ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Na contratação de serviços críticos em nuvem, os requisitos devem ser avaliados quanto à aderência a Política de Segurança da Informação da SPC Grafeno, conforme listados abaixo, mas não se limitando a:

- Procedimentos que consideram os cenários para a substituição da empresa contratada e o reestabelecimento da operação normal da instituição em caso de indisponibilidade do serviço prestado;

- As minutas de contratos ou de aditivos contratuais relativos a serviços relevantes de processamento e armazenamento de dados e de computação em nuvem devem ser encaminhadas ao Banco Central do Brasil, no mínimo, 60 (sessenta) dias antes da assinatura dos respectivos instrumentos contratuais;

- Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever o tratamento para mitigar os efeitos dos incidentes relevantes e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

18. RESPOSTA A INCIDENTES

18.1. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

No contexto deste documento, incidente de segurança da informação é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança em geral, ligado aos ativos Pessoas, Processos ou Ambientes Físicos, levando à perda de um ou mais princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade.

O documento **Plano de Resposta a Incidentes** da SPC Grafeno descreve os procedimentos e ações a serem tomados em caso de ocorrência de incidentes de segurança cibernética ou violações

de dados. O objetivo desse plano é minimizar os danos causados por tais incidentes, garantir uma resposta eficaz e rápida e, ao mesmo tempo, aprender com esses eventos para melhorar a postura de segurança da organização. Dentre os principais elementos do Plano de Resposta a Incidentes estão:

- **Equipe de Resposta a Incidentes:** Esta seção define as funções e responsabilidades de cada membro da equipe designada para lidar com incidentes. Isso inclui líderes, analistas técnicos, comunicadores, entre outros.

- **Classificação e Categorização de Incidentes:** Descreve como os incidentes serão classificados e categorizados de acordo com sua gravidade e impacto. Isso ajuda a priorizar ações de resposta de acordo com a natureza do incidente.

- **Procedimentos de Notificação:** Define como a equipe e as partes interessadas devem ser notificadas sobre um incidente, tanto interna quanto externamente, incluindo reguladores e clientes, se necessário.

- **Isolamento e Mitigação:** Descreve as etapas que devem ser tomadas para isolar o incidente e reduzir seus impactos, como desligar sistemas comprometidos, bloquear tráfego malicioso etc.

- **Coleta de Evidências:** Detalha os procedimentos para coletar evidências relacionadas ao incidente. Isso pode incluir registros de log, capturas de tela, arquivos maliciosos etc.

- **Análise e Investigação:** Define como a equipe conduzirá a análise do incidente para entender sua origem, extensão e impacto. Isso pode envolver análise forense, revisão de registros de atividades, identificação de vetores de ataque, etc.

- **Comunicação Externa e Interna:** Especifica como a Companhia se comunicará com a mídia, clientes, parceiros e partes interessadas internas durante e após um incidente.

- **Recuperação e Restauração:** Detalha os procedimentos para recuperar sistemas afetados e restaurar operações normais após a mitigação do incidente.

- **Aprendizado e Melhoria Contínua:** Análise pós-incidente, onde a Companhia avalia como o incidente foi tratado, o que poderia ter sido feito de forma diferente e como melhorar o plano de resposta para futuros incidentes.

19. CONSCIENTIZAÇÃO DE SEGURANÇA

Os treinamentos periódicos de Segurança da Informação da SPC Grafeno fornecem aos colaboradores as habilidades e o conhecimento necessários para reconhecer e enfrentar ameaças cibernéticas em constante evolução, abordando tópicos como práticas de senha segura, phishing, engenharia social e requisitos de segurança, para que os colaboradores se tornem participantes ativos na proteção dos dados da Companhia e a agirem como a primeira linha de defesa contra potenciais violações de segurança.

20. PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO

A Diretoria de Dados/SI da SPC Grafeno estabelece o plano diretor de segurança da informação visando estabelecer diretrizes e ações para garantir a implementação da Política de Segurança da Informação e Cibernética da SPC Grafeno.

O Plano Diretor de SI é revisado anualmente e aprovado pelo Conselho de Administração da SPC Grafeno.

21. AVALIAÇÃO DE EFETIVIDADE DE SEGURANÇA DA INFORMAÇÃO

21.1. AVALIAÇÃO DE MATURIDADE DE SEGURANÇA

A área de Segurança da Informação da SPC Grafeno aplica o processo de avaliação de maturidade de segurança da informação por meio de um modelo (framework) internacional, que envolve uma abordagem sistemática e processual para avaliar e melhorar a postura de segurança da Companhia

Isso pode envolver revisão de políticas, procedimentos, sistemas e tecnologias em uso. Com base na avaliação, a Companhia atribui uma pontuação de maturidade para cada controle, indicando o nível de implementação e eficácia.

21.2. RELATÓRIO ANUAL DE EFETIVIDADE

De acordo com o art. 87 da Resolução nº 304, do Banco Central, deve ser elaborado relatório, com periodicidade mínima anual, com data-base de 31 de dezembro, contendo as conclusões dos exames realizados, recomendações relacionadas a eventuais deficiências, incluindo cronograma para correção, quando aplicável e manifestação dos responsáveis pelas áreas pertinentes sobre as deficiências encontradas em verificações anteriores e as medidas efetivamente tomadas para correção, quando aplicável.

O relatório deve estar à disposição do Banco Central do Brasil pelo prazo mínimo de 5 (cinco) anos contados de sua emissão.

22. DISPOSIÇÕES GERAIS

22.1. VIGÊNCIA

Esta Política vigorará por prazo indeterminado.

22.2. CASOS OMISSOS

Os casos omissos serão regulados pelo Conselho de Administração da Companhia, conforme necessário.

22.3. DIVISIBILIDADE

A invalidade ou ineficácia de qualquer disposição desta Política não afetará os demais dispositivos, que permanecerão em pleno vigor e efeito.

23. REVISÃO DA POLÍTICA

Esta Política deverá ser revisada anualmente. Eventuais correções ou aprimoramentos devem ser objeto de recomendação ao Conselho de Administração.

24. VIOLAÇÕES

As violações dos termos da presente Política serão examinadas pelo Comitê de Ética da SPC Grafeno, poderá aplicar as ações disciplinares descritas na Política de Consequências, reportando ao Conselho de Administração.

25. CONTROLE DE VERSÕES

Versão	Data	Responsável	Ocorrência
1.0	26/09/2019	Diretor de Dados e SI	Elaboração do documento
1.0	26/09/2019	Diretor de Tecnologia	Revisão do documento
1.0	26/09/2019	Conselho de Administração	Aprovação do documento
2.0	19/12/2022	Conselho de Administração	Aprovação do documento

3.0	27/06/2023	Área de Segurança da Informação	Revisão do documento para aderência à Res. 304 e PFMI
3.0	15/09/2023	Comitê de Gerenciamento de Riscos	Revisão e aprovação do documento
3.0	29/09/2023	Conselho de Administração	Aprovação final do documento