SPC GRAFENO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

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

SUMÁRIO

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 e boas práticas do mercado.

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

- Política de Gerenciamento de Riscos e Controles Internos
- Plano Diretor de Segurança da Informação
- Manual de Acessos a Sistemas e Informações
- Manual de Gestão de Mudanças
- Política de Gestão de Terceiros
- Política de Gerenciamento de Incidentes
- Política de Continuidade de Negócios
- Política de Privacidade e Proteção de Dados
- Plano de Continuidade de Negócios
- Plano de Recuperação de Desastres
- Política de Proteção de Logs e Trilhas de Auditoria
- Documento AWS: Implantações Multi-AZ do Amazon RDS (https://aws.amazon.com/pt/rds/features/multi-az/)
- Manual de Uso de Criptografia
- Manual Integrado de Segurança no Desenvolvimento e Operações
- Manual de Uso Aceitável de Recursos de Tecnologia

- Resolução BCB nº 304/2023 - Regulamenta a atividade de Registro de Ativos Financeiros
- Lei n° 13.709/2018 – Lei Geral de Proteção de Dados

4. ALÇADAS DE APROVAÇÃO

- Área de Segurança da Informação – responsável pela elaboração e revisão da Política;
- Comitê de Riscos, Compliance e SI – responsável pela revisão e aprovação da Política;
- Conselho de Administração – responsável pela aprovação final da Política.

5. PAPÉIS E RESPONSABILIDADES

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.

COMITÊ DE RISCOS, COMPLIANCE E SI

O Comitê de Riscos, Compliance e Segurança da Informação é responsável por supervisionar e orientar a implementação das políticas de segurança da informação e cibernética, avaliar e monitorar os riscos associados, revisar e aprovar planos e medidas de mitigação, garantir a conformidade com normas e regulamentos, promover a conscientização e treinamento contínuo, e relatar regularmente ao conselho de administração sobre o status da segurança da informação e cibernética, além de coordenar a resposta a incidentes e assegurar a colaboração entre as diversas áreas da empresa.

DIRETORIA DE RISCOS, CI, COMPLIANCE E SI

A Diretoria de Riscos, CI, Compliance e Segurança da Informação é responsável por desenvolver, implementar e manter políticas e manuais de segurança da informação e cibernética, alinhadas aos requisitos regulatórios e melhores práticas. Ela gerencia riscos, monitora e responde a incidentes de segurança, assegura a conformidade com leis e regulações, realiza auditorias e testes de vulnerabilidade, e promove a conscientização e treinamento contínuo em segurança. A Diretoria também supervisiona a gestão de acessos e identidades, protege a infraestrutura e as aplicações, colabora com outras áreas da empresa, e reporta regularmente ao conselho de administração e alta direção sobre o status da segurança da informação e cibernética.

DIRETORIA DE TECNOLOGIA, DADOS E INOVAÇÃO

A Diretoria de Tecnologia, Dados e Inovação é responsável por implementar e manter a infraestrutura tecnológica segura e eficiente, garantir a aplicação das políticas de segurança da informação e cibernética, gerenciar a segurança de sistemas e redes, assegurar a atualização e o monitoramento contínuo de tecnologias de defesa contra ameaças, colaborar com a Diretoria de Riscos, CI, Compliance e SI na identificação e mitigação de riscos, promover a conscientização e

treinamento em segurança para as equipes de TI, e reportar regularmente sobre o status e incidentes de segurança tecnológica à alta administração.

COLABORADORES, TERCEIROS CONTRATADOS, FORNECEDORES E PRESTADORES DE SERVIÇOS

São responsáveis por cumprir rigorosamente as políticas e procedimentos de segurança da informação e cibernética, proteger os dados e ativos de informação da empresa, reportar imediatamente quaisquer incidentes ou suspeitas de violação de segurança, participar de treinamentos e programas de conscientização sobre segurança, utilizar de forma segura e adequada os sistemas e recursos tecnológicos fornecidos, e colaborar com a empresa na implementação de medidas de segurança, garantindo assim um ambiente seguro e em conformidade com as normas e regulamentos aplicáveis.

6. DIRETRIZES

6.1. DIRETRIZES GERAIS

- **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.

- **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.

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

- **BYOD:** Aplicar políticas de segurança para a utilização de dispositivos pessoais para acessar recursos e dados corporativos.

- **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.

- **Confidencialidade:** Garantir que a informação seja acessada apenas por colaboradores que tenham permissão;

- **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.
- **Disponibilidade:** Garantir que a informação esteja disponível no momento necessário.

- **DLP: garantir que informações confidenciais e sensíveis não sejam acidentalmente ou intencionalmente divulgadas fora da organização**

- **Integridade:** garante que a informação acessada esteja correta e íntegra.

- **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.

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

- **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.

- **Manual 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.

6.2. USO ACEITÁVEL DE RECURSOS DE TECNOLOGIA

O Manual de Uso Aceitável de Recursos de Tecnologia, estabelece que todos os recursos tecnológicos, incluindo computadores, celulares, e-mail corporativo e outros mecanismos, devem ser utilizados exclusivamente para fins profissionais e de acordo com as políticas da empresa. Isso inclui dispositivos pessoais usados no modelo BYOD (Bring Your Own Device), que também devem ser registrados no inventário corporativo. Todos os dispositivos devem ser identificados, monitorados e mantidos de forma segura, com atualizações regulares e proteção contra ameaças cibernéticas.

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.

As regras para acesso à web e utilização de softwares estão claramente definidas para assegurar que o uso de recursos digitais, tanto em dispositivos corporativos quanto pessoais (BYOD), seja seguro e eficiente. Acessos a sites e a instalação de softwares não autorizados são estritamente proibidos, e todos os softwares utilizados devem ser devidamente licenciados e aprovados pela equipe de TI. A navegação na web deve seguir as diretrizes da empresa para evitar riscos de segurança, e qualquer atividade suspeita deve ser reportada imediatamente.

O processo de acesso VPN é definido para garantir conexões seguras e criptografadas, protegendo os dados corporativos durante acessos remotos, incluindo aqueles realizados por meio de dispositivos pessoais (BYOD). Somente usuários autorizados podem utilizar a VPN, e eles devem seguir rigorosamente os procedimentos de autenticação multifatorial. O uso da VPN é monitorado para detectar e responder a possíveis incidentes de segurança, assegurando que o acesso remoto aos recursos da empresa seja realizado de forma controlada e segura.

6.3. PROTEÇÃO DE DADOS E INFORMAÇÕES

A prevenção ao vazamento de informações é fundamental para garantir a integridade e confidencialidade dos dados corporativos. Políticas e controles rigorosos são implementados para evitar acessos não autorizados e divulgação inadequada de informações sensíveis. Ferramentas de monitoramento e sistemas de prevenção contra perda de dados (DLP) são utilizados para identificar e bloquear tentativas de vazamento, enquanto a conscientização dos colaboradores sobre boas práticas de segurança é continuamente promovida.

Logs e Trilhas de Auditoria são mantidas para registrar todas as atividades de acesso e manipulação de dados, permitindo a rastreabilidade e investigação de incidentes de segurança. Esses registros são armazenados de forma segura e revisados regularmente para detectar comportamentos anômalos e garantir a conformidade com as políticas de segurança. As diretrizes desse processo estão descritas no **Política de Proteção de Logs e Trilhas de Auditoria** da Companhia.

A guarda e deslocamento das informações são geridos com extrema cautela, assegurando que dados críticos sejam armazenados em locais seguros e transferidos de maneira protegida, utilizando criptografia e outras medidas de segurança. O descarte de informações, devem seguir procedimentos efetivos para garantir a completa eliminação de dados sensíveis, prevenindo a recuperação não autorizada. A Companhia deve adotar práticas seguras para o descarte de informações utilizar mecanismos para o descarte adequado de mídias e dispositivos eletrônicos.

- **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.

6.3.1. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação é aplicada para categorizar os dados de acordo com sua sensibilidade e criticidade, estabelecendo níveis apropriados de proteção e acesso.

São definidas as 4 (quatro) classificações utilizadas pela SPC Grafeno e a forma de manuseio delas em diversos formatos de mídia:

Classificação	Risco	Descrição	Exemplo de Informação
Público	Baixo	São aquelas que podem ser divulgadas para todos, inclusive fora do ambiente corporativo da SPC Grafeno. Devido a sua natureza, as informações públicas não necessitam de controles de segurança sofisticados.	Apresentações institucionais, materiais de divulgação em sites públicos ou de forma pública no site da SPC Grafeno.
Uso Interno	Médio	São informações que podem ser utilizadas por todos os colaboradores da SPC Grafeno para a execução das atividades do dia a dia. Estas não podem ser divulgadas para o ambiente externo.	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	São informações sensíveis com acesso liberado a grupos de colaboradores. Essas informações podem trazer vantagens competitivas, portanto o uso deve ser controlado de acordo.	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	São aquelas informações que têm o acesso restrito a colaboradores que tiverem o acesso explicitamente permitido. São informações consideradas vitais para a SPC Grafeno.	Planos de negócio, memorando ou atas de reuniões confidenciais, informações financeiras críticas, novos produtos e dados pessoais sensíveis.

Todas as informações devem ser classificadas de acordo com sua sensibilidade e importância para a Companhia. A classificação determinará o período de retenção e as medidas de segurança associadas. As regras de classificação, armazenamento e retenção de dados pessoais, devem seguir as diretrizes da **Política de Privacidade e Proteção de Dados Pessoais**, da SPC Grafeno.

Todos os colaboradores da SPC Grafeno independente do cargo ou função, devem seguir os controles indicados nesta Política. Devem classificar todas as informações geradas ou manipuladas (e ainda não classificadas) e utilizar os controles indicados para cada uma delas no momento devido.

Os procedimentos para Classificação da Informação nos documentos internos, estão inseridos no **Anexo I** desta Política.

6.4. CONFIGURAÇÃO SEGURA DE ATIVOS E SOFTWARE CORPORATIVOS

A gestão de riscos de segurança e cyber, deve assegurar que todos os ativos e softwares corporativos sejam configurados de acordo com as melhores práticas e padrões de segurança. Isso inclui a realização de avaliações regulares de riscos para identificar vulnerabilidades e implementar controles eficazes. A configuração segura deve abranger desde a instalação inicial até a manutenção contínua, garantindo que os sistemas estejam protegidos contra ameaças e que sejam mantidos atualizações e patches de segurança.

Além disso, controles rigorosos devem ser aplicados para prevenir e mitigar o impacto de software malicioso. Isso inclui o uso de ferramentas de antivírus e antimalware atualizadas, a realização de varreduras regulares e a aplicação de políticas de segurança para a execução de softwares.

A criptografia deve ser utilizada para proteger dados sensíveis em repouso e em trânsito, garantindo que informações críticas sejam codificadas de forma adequada para prevenir acessos não autorizados e garantir a confidencialidade e integridade dos dados. O **Manual de Uso de Criptografia** da SPC Grafeno descreve esse processo.

6.5. GESTÃO DE INFRAESTRUTURA DE REDE

A segmentação de rede deve ser cuidadosamente planejada e implementada para proteger os ativos de segurança e garantir a integridade da rede corporativa.

Todas as alterações nas regras de segurança e configuração dos ativos de rede devem ser aprovadas pelo departamento de Segurança da Informação (SI) para assegurar que estejam alinhadas com as políticas de segurança e não comprometam a proteção da infraestrutura. Essa abordagem permite uma gestão eficaz dos riscos e mantém a integridade das configurações de rede.

Além disso, a resiliência da plataforma deve ser assegurada através da replicação eficiente de dados entre ambientes para evitar perda de informações críticas. A empresa deve implementar soluções de replicação e backup que garantam a continuidade dos negócios e a recuperação rápida em caso de falhas ou desastres. A estratégia de resiliência deve incluir a verificação regular dos processos de replicação e a realização de testes de recuperação para assegurar que os dados possam ser restaurados de forma eficaz quando necessário. Este nível de resiliência também é exigido dos fornecedores de serviços críticos.

6.6. GESTÃO DE ACESSOS

A concessão de acessos a sistemas, aplicações e bancos de dados deve ser rigorosamente controlada e baseada no princípio do menor privilégio, garantindo que os usuários tenham apenas

os acessos necessários para desempenhar suas funções. O processo de concessão de acesso deve incluir a verificação de autorizações adequadas e a documentação de todas as solicitações. Além disso, a Política de Senhas definida deve ser seguida rigorosamente, assegurando que senhas fortes e únicas sejam utilizadas e regularmente atualizadas para proteger contra acessos não autorizados.

O acesso físico e remoto aos recursos da empresa deve ser igualmente protegido por políticas e controles de segurança robustos. Para o acesso físico, medidas como acessos biométricos e sistemas de vigilância devem ser implementadas para assegurar que somente indivíduos autorizados possam entrar em áreas restritas. Para o acesso remoto, mecanismos de autenticação multifatorial e VPNs seguras devem ser utilizados para proteger a integridade e confidencialidade dos dados durante a transmissão, de acordo com o **Manual de Uso Aceitável de Recursos de Tecnologia**.

A revogação de acessos é um componente crítico da gestão de acessos, garantindo que os privilégios de acesso sejam imediatamente removidos quando não forem mais necessários, como no caso de desligamento de colaboradores ou terceiros ou mudanças de função. Este processo deve ser executado de forma eficiente e registrada adequadamente para manter a segurança e a conformidade com as políticas internas, assegurando que todas as etapas sejam seguidas corretamente para evitar riscos de segurança.

O **Manual de Acessos a Sistemas e Informações** descreve detalhadamente os procedimentos para concessão, manutenção e revogação de acessos, bem como as diretrizes da Política de Senhas. Este manual serve como um guia abrangente para garantir que todos os processos de gestão de acessos sejam realizados de forma segura e conforme as normas estabelecidas pela Companhia.

6.7. GESTÃO CONTÍNUA DE VULNERABILIDADES

O objetivo do processo é identificar, avaliar e mitigar vulnerabilidades em sistemas e aplicações para proteger a infraestrutura da empresa contra ameaças cibernéticas. A gestão contínua de vulnerabilidades é essencial para garantir a segurança dos ativos de informação e a conformidade com as políticas de segurança da Companhia.

O processo inclui a realização de scans de vulnerabilidades mensais, que permitem a identificação proativa de falhas de segurança e a implementação de correções antes que possam ser exploradas. Além disso, a empresa realiza testes de penetração (pentests) no mínimo anualmente, podendo ocorrer retestes de acordo com o planejamento anual da área de Segurança da Informação (SI), para avaliar a segurança dos sistemas e identificar possíveis fraquezas que possam ser exploradas por um invasor.

O **Manual Integrado de Segurança no Desenvolvimento e Operações**, descreve em detalhes os procedimentos para a execução de scans de vulnerabilidades e pentests, bem como as ações

corretivas e preventivas necessárias para manter a segurança contínua dos sistemas e aplicações da Companhia.

6.8. 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 na **Política de Continuidade de Negócios**, no **Plano de Continuidade de Negócios** e no **Plano de Recuperação de Desastres**.

6.8.1. 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.

Para assegurar a confiabilidade dos dados, deve-se definir uma estratégia de backup e restauração, bem como a integridade dos dados, admitindo-se a aplicação das regras definidas pelo fornecedor de infraestrutura.

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.

6.9. DESENVOLVIMENTO SEGURO

6.9.1. CICLO DE DESENVOLVIMENTO OU ATUALIZAÇÃO DE SISTEMAS

O ciclo de desenvolvimento e atualização de sistemas abrange uma série de medidas para garantir que os requisitos de segurança sejam incorporados desde o início do processo de desenvolvimento. Isso inclui a definição clara dos requisitos de segurança que devem ser atendidos para cada projeto, bem como a adoção de boas práticas de segurança durante todas as fases do desenvolvimento. A segregação lógica de ambientes é fundamental para evitar que problemas em um ambiente afetem

outros, garantindo que os ambientes de desenvolvimento, teste, homologação e produção sejam mantidos separados.

Além disso, a segregação de perfis de acesso é implementada rigorosamente para assegurar que apenas usuários autorizados possam acessar informações e recursos específicos em cada ambiente. A validação de segurança do código fonte é um passo crítico para identificar e corrigir vulnerabilidades antes que o software seja implantado. O inventário e controle das APIs são mantidos para garantir que todas as interfaces sejam gerenciadas de forma segura, protegendo contra acessos não autorizados e outros riscos.

O processo de security by design é adotado para integrar considerações de segurança em todas as etapas do ciclo de vida do desenvolvimento de software. Isso inclui a identificação e tratamento das vulnerabilidades desde o início, permitindo uma abordagem proativa à segurança.
Todos esses processos e procedimentos são detalhados no **Manual Integrado de Segurança no Desenvolvimento e Operações**, que serve como um guia abrangente para assegurar que todas as práticas de desenvolvimento seguro sejam seguidas rigorosamente.

6.9.2. GESTÃO DE MUDANÇAS

O processo de gestão de mudanças, contido no **Manual 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.

6.10. 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 contratados 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:

Análise Prévia

- **Avaliação de Segurança:** Os fornecedores, prestadores de serviços e parceiros, devem passar por uma avaliação de segurança que inclui a verificação de suas políticas de segurança da informação, processos de gestão de riscos e conformidade com regulamentações relevantes. Devem demonstrar práticas robustas de proteção de dados, incluindo criptografia, controle de acesso e políticas de resposta a incidentes. A área de SI/Cyber poderá realizar testes de penetração (pentests) para

avaliar a robustez das medidas de segurança do fornecedor, de acordo com o alinhamento e devida autorização do fornecedor.

- **Requisitos de Conformidade:** Os fornecedores, prestadores de serviços e parceiros devem comprovar conformidade com normas e padrões de segurança reconhecidos, como ISO/IEC 27001, NIST, GDPR, ou outros regulamentos aplicáveis. A documentação de certificações e auditorias recentes deve ser fornecida para avaliação.
- **Gestão de Acessos e Dados:** Deve ser verificado se os fornecedores, prestadores de serviços e parceiros possuem controles adequados de gestão de acessos, garantindo que apenas pessoal autorizado tenha acesso a dados sensíveis. Também é importante avaliar as políticas de retenção e descarte de informações para assegurar a proteção contínua dos dados.
- **Capacidade de Resposta a Incidentes:** Os fornecedores, prestadores de serviços e parceiros devem possuir um plano de resposta a incidentes bem definido, incluindo procedimentos para a detecção, notificação e mitigação de incidentes de segurança. A capacidade de realizar investigações e fornecer relatórios de incidentes deve ser comprovada.
- **Questionário de Due Diligence:** Será aplicado um questionário de due diligence abrangente para coletar informações detalhadas sobre as práticas de segurança do fornecedor. As respostas a este questionário servirão como base para a análise prévia e ajudarão a identificar potenciais riscos.
- **Avaliação Contínua:** A segurança do fornecedor deve ser monitorada continuamente, com revisões periódicas e reavaliações para garantir que os padrões de segurança sejam mantidos ao longo do tempo. Qualquer mudança significativa na operação do fornecedor que possa impactar a segurança deve ser comunicada e reavaliada.

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

Na contratação de serviços relevantes em nuvem, os requisitos devem ser avaliados quanto a aderência à **Política de Gestão de Terceiros**, 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;

- A Companhia deve informar ao Banco Central do Brasil todas as contratações e alterações relacionadas a terceirizações relevantes no prazo de até 10 (dez) dias após a contratação ou alteração contratual;

- Para serviços relevantes de processamento, armazenamento de dados e computação em nuvem no exterior, a Companhia deve observar as disposições da Resolução nº 304 do Banco Central do Brasil (BCB).

6.11. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O processo de gestão de incidentes, no contexto desta Política, é o estabelecimento de procedimentos e responsabilidades para identificar, gerenciar e resolver incidentes de segurança da informação e cibernética.

Incidentes de segurança podem incluir tentativas de acesso não autorizado, malware, violações de dados e outras atividades que possam comprometer a integridade, confidencialidade e disponibilidade dos ativos de informação da empresa. Todos os incidentes devem ser tratados conforme a **Política de Gerenciamento de Incidentes**, garantindo uma resposta rápida e eficaz para minimizar impactos negativos.

Para incidentes de segurança envolvendo dados pessoais e sensíveis, a Companhia deve adotar medidas imediatas para mitigar o impacto e proteger as informações afetadas. Em conformidade com as regulamentações de proteção de dados, é obrigatório notificar o órgão regulador de proteção de dados, detalhando a natureza do incidente, os dados comprometidos e as ações corretivas adotadas. Este processo assegura a transparência e a conformidade legal, protegendo os direitos dos titulares de dados.

Além disso, incidentes relevantes de segurança da informação e cibernética devem ser comunicados ao Banco Central, conforme as diretrizes estabelecidas pela regulamentação vigente. A comunicação ao Banco Central deve incluir uma descrição detalhada do incidente, suas causas, consequências e as medidas corretivas implementadas.

Este procedimento é essencial para garantir que a Companhia atenda aos requisitos regulatórios e mantenha a confiança dos stakeholders. Todos esses procedimentos estão detalhados na **Política**

de Gerenciamento de Incidentes, que fornece orientações claras para a resposta adequada a diferentes tipos de incidentes de segurança.

6.12. PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO

A Diretoria de Riscos, CI, Compliance e 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.

6.13. AVALIAÇÃO DE MATURIDADE DE SEGURANÇA

A Avaliação de Maturidade de Segurança da Informação é conduzida com base em frameworks internacionais reconhecidos, como o NIST Cybersecurity Framework ou ISO/IEC 27001. Esta avaliação permite medir a eficácia dos controles de segurança implementados e identificar áreas de melhoria contínua. O processo envolve uma análise detalhada das práticas de segurança da informação da empresa, avaliando aspectos como governança, gestão de riscos, proteção de dados, resposta a incidentes e conformidade regulatória.

Os resultados da avaliação, incluindo os controles estabelecidos e o grau de maturidade atingido, são apresentados ao Comitê de Riscos, Compliance e Segurança da Informação. Este comitê revisa os resultados, avalia a adequação das medidas de segurança em vigor e decide sobre ações corretivas ou melhorias necessárias. A apresentação periódica ao comitê assegura que a alta administração esteja informada sobre o estado da segurança da informação na empresa e apoia a tomada de decisões estratégicas para aprimorar a postura de segurança da organização.

6.14. 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.

6.15. 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.

7. DISPOSIÇÕES GERAIS

7.1. VIGÊNCIA

Esta Política vigorará por prazo indeterminado.

7.2. CASOS OMISSOS

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

7.3. DIVISIBILIDADE

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

8. REVISÃO DA POLÍTICA

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

9. 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.

10. 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
4.0	06/08/2024	Áreas de Segurança da Informação	Revisão do documento
4.0	27/08/2024	Comitê de Riscos, Compliance e SI	Revisão e aprovação do documento
4.0	03/10/2024	Conselho de Administração	Aprovação final do documento.
5.0	20/02/2025	Área de Segurança da Informação	Revisão do documento
5.0	14/03/2025	Comitê de Riscos, Compliance e SI	Revisão e aprovação do documento
5.0	08/04/2025	Conselho de Administração	Aprovação final do documento

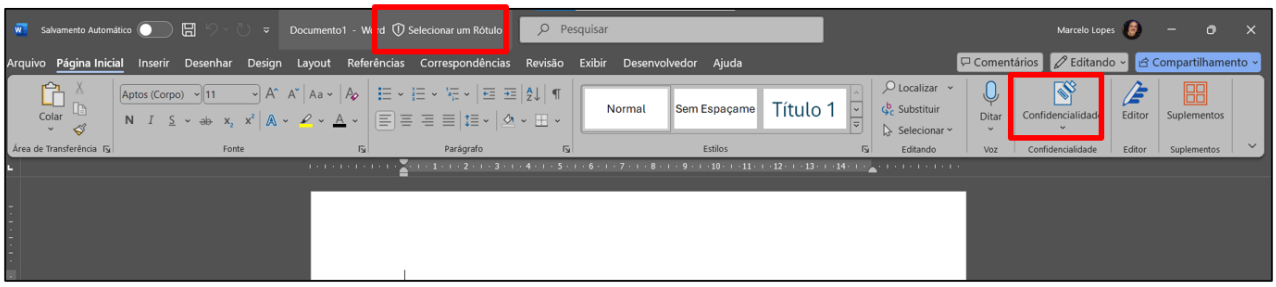
ANEXO I - PROCEDIMENTO PARA CLASSIFICAÇÃO DA INFORMAÇÃO

Como classificar as informações nos aplicativos do Microsoft Office 365

Word, Power Point e Excel

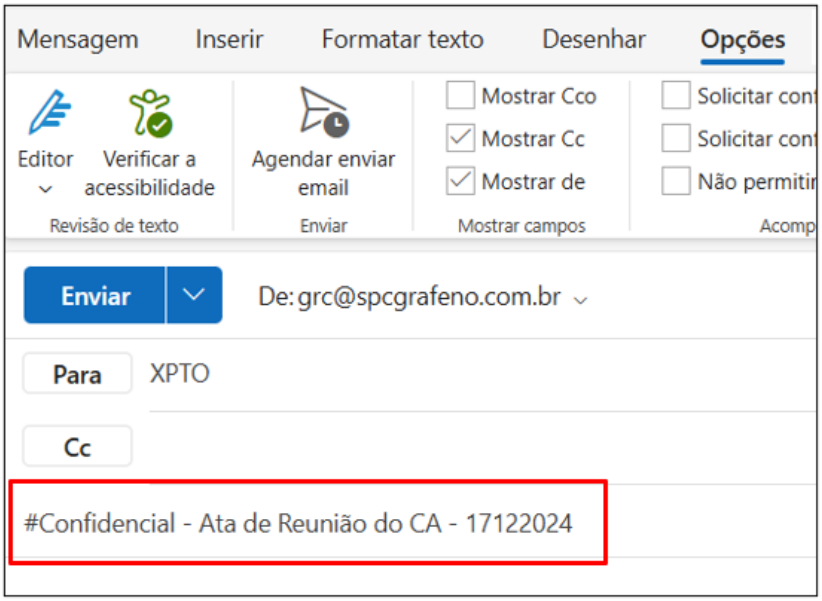
Abra o documento, planilha ou apresentação e vá até a aba "Página Inicial".

Selecione "Selecionar um Rótulo" ou "Confidencialidade" e escolha a classificação apropriada, como "Público", "Interno", "Confidencial" ou "Restrito".



Outlook

Ao redigir uma mensagem de e-mail, rotule a classificação adequada da mensagem, bem como dos anexos, levando em consideração a mensagem e o arquivo anexado devem receber a mesma classificação.



Controles aplicáveis

Abaixo seguem listados os controles aplicáveis para cada tipo de mídia em todos os momentos do ciclo de vida versus classificação.

- **Informações públicas**

Mídia	Rotulagem	Controle de acesso	Descarte seguro
Papel	**X**		
E-mail	**X**		
Documentos eletrônicos	**X**	**X**	
Aplicações	**X**	**X**	

- **Informações internas**

Mídia	Rotulagem	Controle de acesso	Descarte seguro
Papel	**X**		
E-mail (interno)	**X**	**X**	
Documentos eletrônicos	**X**	**X**	**X**
Aplicações	**X**	**X**	**X**

- **Informações restritas**

Mídia	Rotulagem	Controle de acesso	Descarte seguro
Papel	**X**		**X**
E-mail	**X**	**X**	
Documentos eletrônicos	**X**	**X**	**X**
Aplicações	**X**	**X**	**X**

- **Informações confidenciais**

Mídia	Rotulagem	Controle de acesso	Descarte seguro
Papel	**X**	**X**	**X**
E-mail	**X**	**X**	
Documentos eletrônicos	**X**	**X**	**X**
Aplicações	**X**	**X**	**X**

Para melhor entendimento dos controles citados, segue abaixo uma descrição breve e, como utilizá-los:

- **Rotulagem:** Deve-se definir a classificação das informações contidas no documento através de rótulos explícitos. Para documentos digitais e impressos, deve-se incluir a classificação acompanhada de #interna, #pública, #interna; #restrita ou #confidencial, no rodapé da página e para e-mails, este rótulo deve ser indicado no campo assunto.

- **Controle de acesso:** Forma de gerenciar, controlar e registrar quem tem permissão de acessar as informações contidas em um sistema, arquivo, ambiente ou instalação. Deve ser utilizado no local de armazenamento de documentos eletrônicos. As permissões e níveis de acesso devem ser revisadas periodicamente.

- **Descarte seguro:** Procedimento adequado para o descarte de informações, independente da mídia utilizada, que garantirá que estas informações não sejam recuperadas.

  Como garantir este controle:

  - Utilização de fragmentadoras de papel, quando possível;
  - Informar aos times de tecnologia a descontinuação das aplicações para que os dados possam ser apagados definitivamente;
  - Processo de wipe para os equipamentos (estações de trabalho, celulares e etc.) que não serão mais utilizados.

Em alguns casos, pode haver a necessidade criptografar a informação a ser enviada, para que apenas seu emissor e seu receptor sejam capazes de ter acesso ao conteúdo do material criptografado. A criptografia é normalmente utilizada para:

- Envio de e-mails. Garante que somente o destinatário correto do e-mail tenha acesso às informações;
- Armazenamento de arquivos. Mesmo que tenham acesso ao arquivo, somente pessoas autorizadas terão acesso às informações corretas.

***