POLÍTICA

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

REVISÃO		PÁGINAS ALTERADAS	ÁREA RESPONSÁVEL	DESCRIÇÃO DA ALTERAÇÃO
Nº	DATA			
01	27/01/23	Todas	Governança de TI	Adoção Brasil
02	03/05/24	4, 5, 7 a 11, 16 a 19	Governança de TI	Alteração de periodicidade de revisão e revisão periódica
03	20/01/25	2, 4, 5, 6, 7, 9 a 11, 14, 15, 16, 17 e 19	Governança de TI	Alteração de periodicidade de revisão e revisão periódica

Esta Política será revisada a cada 24 (vinte e quatro) meses ou sempre que houver alguma alteração na diretriz descrita.

1. OBJETIVO

Os seguintes objetivos de Segurança foram desenvolvidos para apoiar a estratégia do negócio e monitorar o desempenho da Política de Segurança da Informação e do SGSI:

P - Proteja as informações contra perda, interrupção, uso indevido e abuso;
R - Reduzir e manter o risco a um nível aceitável acordado;
E - Eduque a equipe e os contratados para que estejam cientes da segurança;
P - Previna incidentes de segurança identificando ameaças e mitigando vulnerabilidades conhecidas;
A - Manter a disponibilidade do serviço por meio da continuidade dos negócios e do planejamento de recuperação de desastres;
R - Operar dentro de nossas obrigações regulatórias, legais e contratuais;
E - Envolva-se ativamente com todas as partes interessadas;
D - Mantenha o SGSI dinâmico, relevante, útil, eficiente e eficaz.

2. ABRANGÊNCIA

Esta política se aplica a todas as instituições do Grupo StoneX, inclusive às sediadas no Brasil.

3. LEGISLAÇÃO RELACIONADA

- Resolução CMN nº 4.893/21 e atualizações
- Política de Gestão de Incidentes de segurança da Informação (POL-052)
- Cadeia de Valor de Serviços Relevantes (BCAM e DTVM)
- Política de Privacidade de Dados (POL-054)
- Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018)
- NIST Cybersecurity Framework
- As regras e regulamentos aplicáveis do setor financeiro, relacionados a incidentes de segurança cibernética, governança corporativa cibernética e questões de regulamentação, e legislação de proteção de dados e privacidade, incluindo, mas não se limitando a: Autoridade de Conduta Financeira do Reino Unido (FCA), EUA Securities and Exchange Commission (SEC), a Financial Industry Regulatory Authority (FINRA), a US Commodity Futures Trading Commission (CFTC), a National Futures

Association (NFA), a Autoridade Monetária de Cingapura (MAS), CVM (Comissão de Valores Imobiliários), ANBIMA, B3 e o Banco Central do Brasil (BCB).

4. DEFINIÇÕES

4.1. SIGLAS & TERMINOLOGIA

4.1.1. CISO – Conselho de Segurança da Informação, pauta integrante do Comitê de TI

4.1.2. IAO - Proprietários de Ativos de Informação

4.1.3. LGPD – Lei Geral de Proteção de Dados

4.1.4. Pessoa Autorizada – Funcionário ou terceiro, devidamente autorizado, com acesso à sistemas StoneX

4.1.5. SGSI – Sistema de Gestão de Segurança da Informação

4.1.6. TI - Tecnologia da Informação

4.1.7. Usuário – funcionário ou prestador de serviço que acesse dependências ou sistemas do grupo StoneX

4.2. ÁREAS ENVOLVIDAS NO PROCESSO

4.2.1. Área Responsável

a. Governança de TI

4.2.2. Áreas Suporte

a. CISO

b. IAO

c. Gestores

d. Recursos Humanos

e. Usuários

5. DISPOSIÇÕES

5.1. DIRETRIZES

5.1.1. O SGSI serve como a pedra angular do compromisso contínuo das instituições com a construção de uma cultura segura e está sujeito a revisão e melhoria contínuas e sistemáticas. O SGSI é totalmente aprovado pelo Conselho do StoneX Group Inc., por meio do endosso da P-03 - Information Security Policy (Política Global de Segurança da Informação). Qualquer dúvida relacionada à SGSI deve ser direcionada à equipe de Governança de TI (DG-ITGovernance@stonex.com).

5.1.2. Um conjunto de políticas, padrões de controle, procedimentos e processos para a segurança da informação deve ser definido, em apoio à Política de Segurança da Informação e seus objetivos declarados, publicado e comunicado a todos os funcionários e partes interessadas aplicáveis.

a. **Políticas de tecnologia da informação e segurançda da informação – são** revisadas e aprovadas pela equipe de governança de TI global e pelo Conselho local;

b. **Padrões de controle -** revisados e aprovados por um proprietário de controle designado ou representante da administração**;**

c. **Procedimentos -** revisados e aprovados por um chefe de departamento ou líder de equipe;

Diretrizes - revisadas e aprovadas por um especialista no assunto (SME) (pode ser o autor).

5.1.3. É importante notar que os 'Padrões de Controle' devem ser considerados os requisitos mínimos de controle para a segurança da informação (ou a 'linha de base'). Quando controles adicionais de segurança da informação são necessários para fins legais, regulatórios ou de governança, os controles de linha de base devem ser aprimorados de acordo, e a documentação fornecida quando necessário.

5.1.4. As pessoas autorizadas devem executar suas funções em conformidade com as diretrizes estabelecidas, em especial o as pessoas autorizadas devem respeitar a privacidade dos outros.

5.1.5. As instituições devem definir e implementar mecanismos de governança adequados para a gestão da segurança da informação. Estes incluem a identificação e atribuição de responsabilidades de segurança, para iniciar e controlar a implementação e operação da segurança da informação em toda a Empresa.

5.1.6. As instituições descritas nesta política utilizam os serviços do Chief Information Security Officer (CISO) da SFromneX Inc (Headquarters).

5.1.7. Os procedimentos devem ser implementados para especificar, quando e por quem as autoridades (aplicação da lei, órgãos reguladores, autoridades de supervisão) serão notificadas em caso de incidente de segurança, que a Empresa é obrigada a comunicar.

5.1.8. O SGSI deve estar sujeito a uma revisão independente e contínua por meio de atividades de auditoria interna e externa; e avaliação de conformidade.

5.1.9. Todo acesso à Web deve ser controlado através de aplicativo instalado nas máquinas dos usuários, impedindo o acesso a sites considerados indevidos. Em casos de exceção, uma solicitação pode ser realizada através do Portal Service Desk informando o motivo da exceção, impacto do bloqueio e usuários afetados.

5.1.10. Quaisquer controles identificados como excluídos do SGSI devem ser notificados através da abertura de chamado.

5.1.11. Os riscos de segurança da informação devem ser identificados, mitigados e monitorados por meio de um processo formalizado de gestão de risco.

5.1.12. Os riscos de segurança da informação devem ser identificados, mitigados e monitorados por meio de um processo formalizado de gestão de risco, conforme as seguintes orientações globais:

- P-04 - Política de Gestão de Riscos da Informação

5.1.13. Todos os candidatos a emprego devem ser avaliados em relação à sensibilidade da função para a qual estão sendo considerados.

5.1.14. Todas as informações pessoais coletadas em relação a pedidos de emprego individuais devem ser tratadas como confidenciais e tratadas de acordo com as leis e regulamentos de proteção de dados.

5.1.15. A educação e o treinamento de conscientização sobre segurança da informação devem ser disponibilizados a todos os funcionários para garantir que eles estejam cientes das ameaças à segurança da informação que a Empresa enfrenta e suas responsabilidades e obrigações seguindo orientação dos documentos:

- P-07 - Política de Educação, Treinamento e Conscientização em Segurança

5.1.16. Todos os funcionários e, quando relevante, contratados e fornecedores terceirizados, receberão treinamento de conscientização sobre segurança como parte de seu programa de orientação e atualizações regulares sobre políticas de segurança e padrões de controle, bem como notificação de quaisquer alterações na legislação e diretrizes aplicáveis.

5.1.17. O treinamento de segurança e conscientização dado ao pessoal deve ser relevante para as funções e responsabilidades individuais.

5.1.18. Os processos disciplinares de RH devem ser aplicados quando os funcionários que deliberadamente ou por negligência cometem uma violação de segurança. No entanto, isso não começará antes da verificação de que ocorreu uma violação de segurança e garantirá que o tratamento correto e justo seja aplicado, conforme diretrizes da política de Boa Conduta (POL-028).

5.1.19. Quando uma violação grave de segurança for verificada, deve-se considerar a revogação imediata dos direitos e privilégios de acesso do funcionário e a necessidade de relatar às autoridades (aplicação da lei, órgãos reguladores, autoridades de supervisão).

5.1.20. As regras que abrangem o uso aceitável de ativos devem ser claramente definidas, documentadas e implementadas. Funcionários, contratados e fornecedores terceirizados que utilizem ou tenham acesso concedido a informações ou sistemas de informação devem estar cientes das políticas de uso e padrões de controle aceitáveis e serão responsáveis por seu acesso e uso desses ativos, conforme as seguintes orientações globais:

- P-05 - Política de Uso Aceitável

5.1.21. A Empresa deve implementar um esquema de classificação de informações para garantir que as informações recebam o nível apropriado de proteção de acordo com sua importância e requisitos de confidencialidade.

- Política de Privacidade (POL-054)

5.1.22. Os procedimentos de manuseio de mídia devem ser implementados para evitar a divulgação não autorizada de informações ou uso indevido, de acordo com o sistema de classificação de segurança da informação.

- Política de Privacidade (POL-054)

5.1.23. Todos os ativos de informação devem ter um cronograma definido de retenção e descarte. Revisões de registros serão realizadas regularmente para determinar se devem ser selecionados para preservação permanente, destruídos ou retidos para fins legais, regulamentares ou de preservação permanente histórica. Quando os registros são arquivados, eles devem ser recuperados por pessoas autorizadas quando necessário. Procedimentos para relacionados a retenção de dados devem seguir a Política de Privacidade (POL-054) norteada pelas orientações globais, a saber:

- P-02 - Política do Programa de Segurança da Informação
- P-10 - Política de Gerenciamento de Configuração
- ITG-015 - Uso Aceitável
- P-21 - Política de Dados
- PS-21-2 – Descarte de Ativos de TI e Padrão de Dados
- P-24 - Política de Retenção de Dados

5.1.24. O acesso a todas as informações e sistemas de informação deve ser controlado e orientado pelos requisitos do negócio. O acesso lógico e físico só será concedido aos usuários de acordo com sua função e em um nível que lhes permita desempenhar suas funções (need-to-know).

- P-18 – Política de Gestão de Acesso

5.1.25. Processos formais devem ser implementados para controlar a alocação de direitos de acesso à informação e aos sistemas de informação. Os procedimentos devem abranger todas as fases do ciclo de vida do acesso do usuário, desde o registro inicial

de novos usuários até a exclusão dos direitos de acesso quando eles não forem mais necessários.

5.1.26. A criação de contas de usuário com privilégios mais elevados, como administradores, deve ser controlada e restrita aos usuários que têm uma necessidade comercial clara de gerenciar sistemas de informação ou redes.

5.1.27. Um processo de revisão formal deve ser implementado para garantir que, os direitos de acesso do usuário aos sistemas regulados financeiramente e a infraestrutura de segurança de TI sejam revisados regularmente. Isso garante que os direitos concedidos a um indivíduo no passado permaneçam válidos e que o usuário tenha uma necessidade comercial contínua de mantê-los.

5.1.28. Todos os usuários devem ser autenticados usando um autenticador antes de obter acesso às informações da Empresa ou sistemas de informação. A consideração de múltiplos fatores adicionais será considerada apropriada para o método de acesso em uso.

5.1.29. Ferramentas devem ser implementadas para garantir o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade e integridade da informação e dos sistemas de informação. No mínimo, a criptografia para todos os dados em repouso deve ser implementada.

5.1.30. Todas as chaves criptográficas devem ser protegidas contra modificação, perda e destruição. Todas as chaves secretas e privadas devem ser protegidas contra divulgação não autorizada. Qualquer equipamento usado para gerar, armazenar e arquivar chaves deve ser mantido fisicamente seguro. Devem ser levados em consideração os regulamentos e restrições nacionais que se aplicam ao uso de técnicas criptográficas em diferentes regiões do mundo e a questão do fluxo transfronteiriço de informações criptografadas, deve-se observar a orientação global ITG-026 (Cryptography).

5.1.31. As instalações de processamento de informações devem ser alojadas em áreas seguras, fisicamente protegidas de acessos não autorizados, danos e interferências por perímetros de segurança definidos. Os controles de segurança interna e externa em

camadas devem estar em vigor para impedir ou impedir o acesso não autorizado e proteger os ativos, especialmente aqueles que são críticos ou sensíveis, contra-ataques forçados ou sub-reptícios.

5.1.32. As áreas que mantêm, armazenam e/ou processam dados confidenciais, como dados pessoais, serão automaticamente classificadas como áreas seguras. Somente pessoas autorizadas terão acesso permitido às áreas seguras e os visitantes devem ser acompanhados em todos os momentos. Telas de computador e documentos em uso em áreas seguras devem ser protegidos contra visualização por pessoas não autorizadas. As instalações contratadas por terceiros, como centros de dados e instalações de armazenamento fora do local, terão controles de segurança física equivalentes ou adicionais implementados e detalhados nas obrigações contratuais relevantes.

5.1.33. Todos os equipamentos de processamento de informações devem ser protegidos contra ameaças físicas e ambientais. Controles de segurança para proteger equipamentos em Data Centers, devem ser implementados para reduzir o risco de acesso não autorizado, perda ou dano. Os controles também devem ser implementados para garantir a continuidade de quaisquer utilitários de suporte, como energia e tecnologia HVAC, considerando a orientação global.

5.1.34. Um processo formal de controle de mudança e procedimentos, deve ser implementado para gerenciar mudanças nos sistemas de informação que transformam, alteram ou modificam o ambiente operacional ou procedimentos operacionais padrão de qualquer sistema ou serviço que tem o potencial de afetar a estabilidade e confiabilidade da infraestrutura ou perturbar os negócios da Empresa.

- P-15 - Política de Gestão de Mudanças

5.1.35. Processos de gerenciamento de capacidade, incluindo: planejamento, monitoramento, avaliação, controle, orçamento e implementação da capacidade necessária para entrega de negócios ininterrupta e responsiva, devem ser implementados e mantidos para gerenciar o tamanho, quantidade, carga e escalabilidade dos sistemas de informação e recursos.

5.1.36. Onde for prático, os ambientes operacionais (de produção) devem ser separados dos ambientes de teste e desenvolvimento e seguir as seguintes diretrizes:

- É proibido o uso de identidades e credenciais de teste e desenvolvimento para sistemas de informações operacionais;
- O código-fonte (ou equivalente) deve ser armazenado em um local seguro e certificado pela StoneX, longe do(s) ambiente(s) operacional(is), com acesso restrito a funcionários especificados;
- O acesso a compiladores, editores e outras ferramentas dos sistemas de informação operacional deve ser evitado;
- A promoção de software de desenvolvimento/teste para sistemas de informações operacionais deve seguir os processos de gerenciamento de mudanças aprovados;
- Sempre que possível, o uso de informações pessoais ou sensíveis no desenvolvimento, teste ou treinamento de sistemas de informação deve ser proibido.

5.1.37. Uma solução de software antivírus (AV) aprovada deve ser implantada em todos os sistemas de informação da Empresa, onde os serviços são necessários e suportados. O tráfego de e-mail suspeito (mensagens e anexos) deve ser encaminhado para uma área de armazenamento isolada para análise. Quando o uso de código móvel é necessário para a funcionalidade de negócios ou aplicativos, ele deve ser reconhecido e autorizado. Onde não houver nenhum requisito para permitir que o código móvel seja executado, ele deve ser impedido de executar.

5.1.38. Todos os dados armazenados nos servidores de arquivos da Empresa, servidores de e-mail, servidores de rede, servidores web, servidores de banco de dados, controladores de domínio, firewalls e servidores de acesso remoto devem ser submetidos a backup regularmente. Todas as mídias de backup devem ser armazenadas com segurança e estarão disponíveis apenas para pessoas autorizadas. As restaurações de backup devem ser testadas em intervalos regulares para garantir a integridade dos backups em caso de crise.

5.1.39. Todos os eventos de segurança relevantes devem ser monitorados e registrados, conforme estabelecido na (P-34 - Política de Registro e Auditoria), considerando que os logs de auditoria registrarão as atividades do usuário, exceções e

eventos de segurança da informação. Os registros devem ser retidos por um período mínimo de 3 meses para auxiliar no monitoramento do controle de acesso e quaisquer investigações de segurança necessárias. Os usuários devem estar cientes de que, suas ações enquanto estiverem nos sistemas de informação da Empresa, serão monitoradas e registradas para garantir que os sistemas estejam sendo usados de maneira autorizada. Os registros administrativos e de falhas do sistema também devem ser monitorados para fornecer uma visão sobre possíveis falhas ou problemas de segurança. Todo o relógio do(s) sistema(s) de informação deve(m) ser sincronizado(s) com uma única fonte de tempo de referência. Violações reais ou suspeitas de segurança da informação devem ser relatadas para investigação e, quando aplicável, para reguladores externos e clientes. O processo deve incluir procedimentos para:

- Planejamento e preparação de resposta a incidentes;
- Monitorar, detectar, analisar e relatar incidentes de segurança da informação;
- Registrar atividades de gerenciamento de incidentes e,
- Ação imediata para contenção, escalonamento de resposta e planejamento de contingência.
- Embasar procedimentos em diretrizes globais, tais como:
    - P-37 - Política de Gestão de Incidentes de Segurança
- A instalação de softwares e aplicativos deve seguir a P-15 - Política de Gestão de Mudanças

- e ser planejada, aprovada, os impactos avaliados, testados e ter um plano de reversão. Todos os softwares e aplicativos fornecidos pelo fornecedor devem ser avaliados (de acordo com a Política de Gestão de Risco) e mantidos. Quaisquer alterações no software devem seguir o processo de controle de alterações e considerar as implicações de segurança da(s) atualização.

5.1.40. Os processos de patch de segurança e gerenciamento de vulnerabilidade devem estar em vigor para identificar, priorizar e corrigir quaisquer vulnerabilidades de segurança dos sistemas de informação, seguindo as seguintes diretrizes:

- As avaliações de vulnerabilidade interna devem ser realizadas mensalmente;
- O teste de penetração externa deve ser realizado pelo menos uma vez por ano;

- Um programa formal de gerenciamento de patch deve ser estabelecido para manter a segurança do(s) sistema(s) de informação;
- Todas as atividades de remediação devem ser registradas, aprovadas e monitoradas para conclusão.
- PS-35-2 – Patch Management Standard

5.1.41. As auditorias do sistema de informação devem ser programadas e planejadas de forma que o impacto nos sistemas operacionais seja mínimo. Convém que os controles sejam implementados para proteger os sistemas de informação e as próprias ferramentas de auditoria durante o processo de auditoria. O controle de acesso deve ser aplicado para evitar o uso indevido de ferramentas de auditoria e para fornecer integridade de ambas as ferramentas e logs e dados associados. Todas as verificações de auditoria devem ser limitadas ao acesso somente leitura. Os trabalhos de auditoria devem ser suportados pelos seguintes procedimentos globais:

- ITG-034 - Controle de aplicativos
- P-01 - Política de Governança de Segurança da Informação
- P-02 - Política do Programa de Segurança da Informação
- P-03 - Política de Segurança da Informação
- P-04 - Política de Gerenciamento de Riscos da Informação
- P-05 - Política de Uso Aceitável
- P-11 - Política de Gestão de Hardware
- P-15 - Política de Gestão de Mudanças
- P-38 - Malware Protection Policy
- PS-21-5 – Data Backup Standard
- PS-35-1 Padrão de gerenciamento de vulnerabilidade
- PS-35-2 – Patch Management Standard

5.1.42. Controles de infraestrutura e sistemas de gestão adequados serão implementados e mantidos para garantir a proteção da informação e dos sistemas de informação.

5.1.43. As redes devem ser gerenciadas e controladas a fim de proteger contra o acesso não autorizado, modificação, uso indevido ou perda, para:

- Informações armazenadas;
- Informações em trânsito;
- Infraestrutura de rede;
- Informações de configuração de rede, incluindo configuração de dispositivo, definições de controle de acesso, informações de roteamento, senhas e chaves criptográficas;
- Informações de gerenciamento de rede;
- Caminhos e rotas de rede;
- Recursos de rede, como largura de banda;
- Limites e perímetros de segurança de rede; e,
- Interfaces de sistemas de informação para redes.

5.1.44. A troca de informações entre a Empresa e qualquer parte externa deve ser protegida contra interceptação, cópia, desvio e descarte quando transmitida eletronicamente. As informações trocadas entre sistemas ou serviços de mensagens eletrônicas devem ser gerenciadas para proteger a integridade e a confidencialidade da mensagem. A mídia, incluindo e-mail, dispositivos móveis, mensagens instantâneas e transferência eletrônica de arquivos (FTP etc.) contendo informações da Empresa, deve ser protegida contra acesso não autorizado, uso indevido ou corrupção durante o transporte além dos limites físicos da Empresa. Os termos e condições para a troca segura de informações com partes externas devem ser documentados em um contrato.

5.1.45. O uso de serviços de mídia social e outros serviços de mensagens eletrônicas não aprovados pela empresa deve ser proibido; a menos que seja explicitamente aprovado pela Assessoria de Imprensa.

5.1.46. Todas as mensagens eletrônicas criadas, compiladas, enviadas ou recebidas nos sistemas de informação da Empresa são registros da Empresa, os funcionários devem ser informados e concordar com sua obrigação de manter a confidencialidade das informações, conforme diretrizes globais a saber:

- P-31 - Política de Gestão de Segurança de Rede
- P-40 - Cloud Security Policy
- P-21 - Política de Dados

5.1.47. Convém que os controles de segurança sejam identificados e verificados como parte dos requisitos de negócios para novos sistemas de informação ou melhorias nos sistemas de informação existentes. Uma Avaliação de Risco e/ou uma Avaliação de Impacto de Privacidade deve ser realizada durante o desenvolvimento, implementação de grandes mudanças ou aquisição de sistemas de informação. O desenvolvimento de sistemas de informação ou atividades de aquisição seguirão procedimentos padrão para teste e controle de mudanças. Os Proprietários de Ativos de Informação (IAO) em parceria com a Segurança de Negócios de TI garantirão que controles suficientes estejam em vigor para mitigar o risco de perda de informações, erro ou uso indevido de sistemas de informação. Antes da implementação, os sistemas de informação devem ser avaliados para verificar a adequação dos controles de segurança usados.

5.1.48. O software e os sistemas desenvolvidos internamente seguirão as políticas, padrões e melhores práticas estabelecidas para um desenvolvimento seguro. As políticas e padrões estabelecidos devem ser aplicados de forma consistente ao longo do ciclo de vida do desenvolvimento, independentemente da localização. Se o desenvolvimento for terceirizado, a garantia deve ser obtida de que a parte externa está em conformidade com as políticas e padrões da Empresa para desenvolvimento seguro.

5.1.49. Procedimentos devem ser implementados para garantir que os dados de teste dos sistemas de informações operacionais sejam autorizados, registrados, protegidos e removidos do ambiente de teste assim que o teste for concluído. Quando dados pessoais ou confidenciais são usados para fins de teste, os detalhes e conteúdos confidenciais devem ser despersonalizados ou desidentificados. Os Proprietários de Ativos de Informação (IAOs) devem garantir que o uso de informações pessoais para fins de teste não infrinja os requisitos das leis de Proteção de Dados e Privacidade, estabelecidos na POL-054 e orientados pelas diretrizes globais:

- P-03 - Política de Segurança da Informação
- P-25 - Política de Gerenciamento Ágil do Ciclo de Vida do Desenvolvimento de Software (SDLC)
- P-30 - Política de Arquitetura
- P-21 - Política de Dados

5.1.50. Todos os fornecedores/vendedores de serviços de informação críticos devem ser examinados e aprovados antes de os serviços serem adquiridos ou contratados, ou o acesso a informações ou sistemas de informação concedido, para garantir que os fornecedores/vendedores atendam aos padrões de segurança da informação exigidos. Os requisitos de segurança da informação serão considerados ao estabelecer relacionamentos com fornecedores/fornecedores, e os riscos avaliados para garantir que as informações da empresa e os sistemas de informação permanecerão protegidos e seguros. Convém que o acesso à informação ou aos sistemas de informação seja baseado em um contrato formal contendo os arranjos necessários de segurança da informação.

5.1.51. A atividade do fornecedor/vendedor deve ser monitorada e auditada de acordo com a criticidade do serviço, valor dos ativos e risco(s) associado(s), seguindo a orientação global P-41 - Política de Gestão de Fornecedores.

5.1.52. Devem ser implementadas medidas para proteger processos de negócios críticos dos efeitos de grandes falhas de sistemas de informação ou desastres para garantir sua recuperação oportuna de acordo com as necessidades de negócios. A análise de impacto nos negócios deve ser realizada quanto às consequências de desastres, falhas de segurança, perda de serviço e falta de disponibilidade de serviço. Os planos de continuidade de negócios devem ser mantidos e testados regularmente e devem estar alinhados com a respectiva política e diretriz global P-42 - Business Resiliency Policy.

5.1.53. O projeto, operação, uso e gerenciamento de sistemas de informação devem cumprir todos os requisitos de segurança regulamentares e contratuais. Isso inclui a legislação de proteção de dados, regulamentos do setor financeiro e as obrigações contratuais da Empresa. Uma combinação de auditoria interna e externa, análises de segurança, avaliações, verificações de saúde de TI e análises de lacunas deve ser usada para demonstrar a conformidade com os padrões, regulamentos e melhores práticas escolhidos, incluindo políticas e procedimentos internos. Os relatórios devem ser disponibilizados para a equipe de governança de TI e para o Conselho local, para a Gestão Executiva e para a matriz, seguindo as orientações globais elencadas abaixo:

- P-15 - Política de Gestão de Mudanças
- P-03 - Política de Segurança da Informação
- P-02 - Política do Programa de Segurança da Informação
- P-04 - Política de Gerenciamento de Riscos da Informação
- P-01 - Política de Governança de Segurança da Informação
- P-21 - Política de Dados

5.1.54. Quando os serviços prestados pela Empresa exigem cooperação entre várias partes e, como resultado, as políticas de Segurança da Informação das partes envolvidas se sobrepõem com diferentes níveis de rigor, a disposição mais restritiva será aplicada.

5.1.55. O não cumprimento de quaisquer políticas, padrões de controle ou procedimentos associados pode resultar em ações disciplinares, incluindo a rescisão do contrato de trabalho para funcionários ou rescisão do contrato para contratados, parceiros, consultores ou outras entidades. Ações judiciais também podem ser tomadas por violações das leis e regulamentos aplicáveis.

5.1.56. Os pedidos de isenções a esta política e quaisquer políticas, padrões ou procedimentos associados devem ser submetidos ao departamento de Governança de TI para processamento e revisão. Exceções só serão permitidas após o recebimento da aprovação por escrito tanto da empresa quanto do proprietário do aplicativo ou tecnologia.

5.2. RESPONSABILIDADES

5.2.1. É responsabilidade do comitê local, apoiado pela equipe de Governança de TI:

a. influenciar, supervisionar e promover a segurança da informação e identificar riscos de informação, protocolos, leis, regulamentos e necessidades do(s) cliente(s);
b. garantir que os funcionários, contratados e terceiros entendam suas responsabilidades e sejam adequados para as funções para as quais são considerados para reduzir o risco de fraude, mau uso das instalações da Empresa e roubo de propriedade da Empresa;
c. Aprimorar o conhecimento e atualizar treinamentos com as informações de segurança relevantes, assegurando que o público-alvo seja devidamente treinado;

d. Receber avisos e alertas, recomendações e patches relativos a ameaças e vulnerabilidades de segurança;
e. Compartilhar e trocar informações relacionadas a tecnologia, produtos, ameaças ou vulnerabilidades;
f. Fornecer pontos de ligação apropriados ao lidar com incidentes de segurança;
g. garantir que este SGSI e quaisquer políticas e padrões de controle relacionados sejam comunicados e implementados;
h. gerenciar a remoção dos direitos de acesso e a coordenação da devolução de quaisquer ativos de informação (equipamentos de TI, chaves, passes de identificação, etc.);
i. Os procedimentos devem ser identificados e documentados para as principais atividades do sistema associadas aos sistemas de informação da Empresa. Esses procedimentos operacionais e os requisitos de controle documentados para as atividades do sistema serão tratados e registrados como documentos SGSI formais;
j. As políticas de segurança da informação devem ser revisadas e atualizadas a cada ano civil para refletir a evolução do cenário internacional de legislação e padrões relacionados à segurança da informação. Essas atualizações incluirão as últimas descobertas de grupos de pesquisa de informações e os principais desenvolvimentos, incluindo legislação, mudanças na regulamentação e o lançamento de outros padrões relacionados à segurança.

5.2.2. IAO

a. Deve assumir a responsabilidade pelos ativos de informação em sua gestão, que contribuem para o gerenciamento de riscos e apoiam a implementação de controles de segurança.

b. Todas as informações e ativos de informações associados aos recursos de processamento de informações devem pertencer a um indivíduo designado (função) dentro da Empresa. O proprietário do ativo de informação (IAO) será claramente identificado no(s) registro(s) de ativos e riscos e será responsável pela manutenção, proteção e destruição segura do ativo de informação.

5.2.3. GESTORES

a. A gerência direta deve incentivar para que os funcionários apliquem e cumpram a segurança da informação de acordo com a Política de Segurança da Informação (SGSI) e seus padrões de controle de apoio, conforme orientações do CISO, assegurando que suas equipes:

- Sejam devidamente informados sobre suas responsabilidades de segurança da informação antes de terem acesso a quaisquer informações confidenciais ou sistemas de informação;
- São fornecidos com orientações sobre as expectativas de segurança de sua função;
- São motivados a cumprir as políticas de segurança e padrões de controle;
- Alcançar e manter um nível de conscientização de segurança relevante para sua função;
- Cumprir os termos e condições de seu emprego.

b. A Empresa deve manter registros de ativos de ativos de informação chave para fornecer rastreamento de "vida útil" em toda a Empresa. Atualmente, esse é um processo descentralizado e gerenciado por representantes locais de TI.

5.2.4. RECURSOS HUMANOS

a. A equipe de RH é responsável pelo processo de rescisão (incluindo contratados e estagiários) e deve trabalhar com a equipe de Acesso ao Sistema e o gerente direto da pessoa que sai para garantir que todos os aspectos de segurança relevantes sejam aplicados ao processo.

5.2.5. USUÁRIOS

a. Os usuários devem estar cientes de suas responsabilidades em relação ao controle de acesso ao sistema e ao uso de mecanismos de acesso. Os usuários devem seguir as boas práticas em relação à proteção e uso de senhas, frases-senha e qualquer outra informação de autenticação secreta ou método usado para identificar uma pessoa.

b. O equipamento do usuário não deve ser deixado sem supervisão enquanto uma sessão do usuário estiver ativa, a menos que seja protegido por um mecanismo de travamento apropriado. O bloqueio de proteção de tela deve ser usado para ausências curtas de um terminal ativo. Durante longos períodos de ausência e no final do período normal de trabalho, o logout completo dos aplicativos ativos e o desligamento do terminal devem ser concluídos.

c. Ao deixar o escritório no final de cada dia de trabalho, todos os usuários devem:

- Mantenha as mesas longe de documentação sensível;
- Bloqueie todos os documentos confidenciais em um local seguro;
- Certifique-se de que qualquer mídia removível contendo dados confidenciais esteja bloqueada com segurança.

d. Os usuários devem seguir as políticas locais de segurança da informação, bem como orientações globais, a saber:

- P-18 – Política de Gestão de Acesso
- P-20 - Política de senha e token
- P-09 - Política de limpeza de mesa e tela