POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SECURITYBOX SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO LTDA.
CNPJ: 11.928.104/0001-87
End: R. Emanuel Kant, 60 Sala 609
Curitiba – PR Telefone: 41 2170-0770

Controle de Versão

Data	Ação	Autor	Empresa	Versão
20/01/2024	Criação	Jean Ricardo Lacerda Santos	BOX GROUP	1.0
13/03/2024	Revisão	Anderson Santos	SECURITYBOX	2.0

Classificação de Confidencialidade

Classificação	Nível	Características
Público	0	Documento que pode ser compartilhado com qualquer pessoa ou empresa.
Interno	1	Documento restrito, não se recomenda compartilhar com pessoas físicas ou outras empresas.
Restrito	2	Documento deve ser compartilhado apenas entre as empresas que foram endereçadas no cabeçalho do documento.
Confidencial	3	Documento não deve ser compartilhado com outras pessoas além das pessoas permitidas e listadas no quadro abaixo.

Pessoas restritas que terão acesso ao documento

Empresa	Cargo	Nome completo
SECURITYBOX	Gerência / Diretoria	Qualquer pessoa

Participação

Empresa	Nome	Papel
SECURITYBOX	George Silverio da Silva	Consultor em LGPD e Especialista em Segurança
BOX GROUP	Jean Ricardo Lacerda Santos	Analista de SOC
SECURITYBOX	Anderson Santos	Analista de Segurança

Sumário

1. OBJETIVO

A Política de Segurança da Informação é o documento que estabelece conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética e segurança da informação, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações sob gestão da SECURITYBOX, definindo os princípios fundamentais que formam a base da Política de Segurança da Informação, norteando a elaboração de normas, processos, padrões e procedimentos.

1. ABRANGÊNCIA

A Política de Segurança da Informação tem abrangência corporativa na SECURITYBOX, ou seja, afeta todas as suas áreas de negócio, filiais, escritórios e demais operações no que se refere a ocorrência de incidentes de segurança da informação.

2. CONCEITOS E DEFINIÇÕES

Os termos a seguir fazem referência a conceitos e definições que poderão ser utilizados ao longo do documento e cabe uma explanação para que não haja qualquer diferença de interpretação.

a) **Recursos**: qualquer ativo, tangível ou intangível, pertencentes, a serviço ou sob responsabilidade da SECURITYBOX, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados em nuvem, sistemas e processos;

b) **Ameaça**: qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais;

c) **Boas Práticas de Segurança da Informação**: são consideradas boas práticas de segurança da informação as recomendações contidas em normas e instituições como: ISO/IEC 27001, ISO/IEC

31000, OWASP (www.owasp.org), NIST (www.nist.gov), ISACA (www.isaca.com.br), SANS (www.sans.org) e outras internacionalmente reconhecidas;

d) **Colaborador**: entende-se como colaborador qualquer pessoa que trabalhe para a SECURITYBOX, quer seja: empregado com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee;

e) **Controle**: qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware, entre outros;

f) **Gestor**: Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de área;

g) **Informação**: qualquer conjunto organizado de dados que possua algum propósito e valor para a SECURITYBOX, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem;

h) **Princípios de "Least Privilege" e "Need to Know"**: estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (Least Privilege) a quem realmente tenha a necessidade de acesso (Need to Know);

i) **Política de Segurança da Informação**: estrutura de documentos formada pela política, normas e padrões de segurança cibernética e segurança da informação;

j) **Risco**: qualquer evento que possa afetar a capacidade da companhia de atingir seus objetivos e sua estratégia de negócios ou conforme a ISO 31000, o efeito da incerteza nos objetivos;

k) **Segurança da Informação (SI)**: é a proteção das informações, sendo caracterizada pela preservação de:

I. Confidencialidade: garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;

II. Integridade: garantia de que o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade;

III. Disponibilidade: garantia de que os Colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa;

IV. Conformidade: garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

l) **Segurança Cibernética**: conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acessos não autorizados. Também conhecida como Segurança de TI, visa proteger somente assuntos relacionados ao digital;

m) **Recursos Críticos**: recursos essenciais para o funcionamento da operação da SECURITYBOX e que possuem informações críticas ou sensíveis;

n) **Baselines**: requisitos, recomendações e melhores práticas de configurações de segurança da informação para os ativos;

o) **Nuvem (Cloud)**: infraestrutura, plataforma, aplicação ou serviço localizado na internet. A nuvem pode ser pública com acesso a todos, privada, com acesso restrito ou híbrido, com parte restrita e parte irrestrita;

p) **IoT (Internet of Things – Internet das coisas)**: conexão de dispositivos eletrônicos, como aparelhos eletrodomésticos, eletroportáteis, máquinas industriais, dentre outros utilizados no dia a dia à internet;

q) **DPO (Data Protection Officer ou Encarregado de Dados)**: pessoa indicada pela SECURITYBOX para atuar como canal de comunicação entre a SECURITYBOX, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

r) **Coordenação administrativa:** pessoa ou área indicada pela SECURITYBOX para atuar como responsável em adquirir, inventariar e repassar os equipamentos, sistemas ou recursos de trabalho necessários para a coordenação de infraestrutura;

s) **Coordenação de infraestrutura**: pessoa ou área indicada pela SECURITYBOX para atuar como responsável por configurar, preparar e liberar os recursos tecnológicos aos colaboradores, bem como promover as condições técnicas e estrutura tecnológica para o desenvolvidos das atividades no ambiente corporativo ou remoto.

3. DIRETRIZES

Por definição, diretrizes podem ser caracterizadas como orientações que definem e regulam planos estabelecidos e ações necessárias, para a normatização de processos e procedimentos. A seguir estão definidas algumas diretrizes para orientar a tomada de decisões da SECURITYBOX, no que tange segurança da informação:

a) A informação é um ativo essencial para os negócios da SECURITYBOX e sendo assim deve ser adequadamente protegida;

b) A segurança da informação visa proteger as informações contra diversos tipos de ameaças, para minimizar a exposição da empresa a riscos, garantindo que as características fundamentais da

informação sejam preservadas, sendo elas: confidencialidade, integridade, disponibilidade e conformidade;

c) A SECURITYBOX em alinhamento com os objetivos e requisitos de negócio, estabelece nesta Política de Segurança da Informação, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações da SECURITYBOX, de seus clientes, fornecedores e parceiros de negócios;

d) Seguir as diretrizes desta política, significa proteger a empresa contra o vazamento de informações, contra fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e da marca da SECURITYBOX;

e) A SecurityBox está comprometida com a melhoria contínua da segurança da informação, adotando práticas rigorosas para proteger os dados e ativos de informação contra ameaças e vulnerabilidades. Em conformidade com os princípios estabelecidos pela norma ISO 27001, nossa política de segurança da informação é revisada regularmente para assegurar que todas as medidas de segurança sejam eficazes e atualizadas, promovendo um ambiente seguro e resiliente. Este compromisso e as estratégias específicas que implementamos para garantir a proteção da informação estão detalhados no documento POP2024-001.

f) A SecurityBox estabeleceu um plano de comunicação abrangente com autoridades e grupos especiais, conforme exigido pela ISO 27001:2022. Este plano visa fornecer orientação clara sobre como a empresa se comunicará com as autoridades relevantes e grupos especiais em situações relacionadas à segurança da informação e à conformidade com a norma. Os detalhes específicos deste plano estão descritos no documento PCA2024-001

g) Esta política será analisada em período não superior a um ano, a partir da data de última publicação, ou sempre que houver mudança significativa no ambiente tecnológico da

SECURITYBOX. Quando atualizada, será publicada uma nova versão, caso haja necessidade de ajustes que a administração entender cabível ou necessárias;

4. PAPÉIS E RESPONSABILIDADES

Todo colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações da SECURITYBOX e deve cumprir as determinações da política, normas e padrões de segurança da informação.

Premissas de segregação de funções, não devem ser executadas pela mesma pessoa as seguintes ações dentro do mesmo contexto:

i. Iniciar, aprovar ou executar dentro do contexto de mudança;
ii. Solicitar, aprovar e implementar dentro do contexto de direitos de acesso;
iii. Utilizar e administrar dentro do contexto de aplicações;
iv. Projetar, auditar e garantir dentro do contexto, os controles de segurança de informação.

a) As responsabilidades da Alta Direção são:

I. Garantir os resultados da SGSI, assegurando recursos para a implementação, manutenção e melhoria contínua do Sistema de Gestão da Segurança da Informação;
II. Prover comprometimento e assegurar apoio à aderência a Política de Segurança da Informação de acordo com os objetivos e estratégias de negócio estabelecidas para a organização;
III. Fornecer à área de segurança da informação claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário, garantindo que se alcance os resultados esperados;
IV. Apoiar outros papéis relevantes à Segurança Cibernética e da Informação.

b) As responsabilidades do Colaborador são:

I. Notificar a coordenação de infraestrutura sobre as violações da política de segurança da informação e sobre os incidentes de segurança que venha a tomar conhecimento;

II. Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI;

c) As responsabilidades do Gestor são:

I. Apoiar e incentivar o estabelecimento da Política de Segurança da Informação da SECURITYBOX;

II. Garantir que seus subordinados tenham acesso e conhecimento desta política e demais normas e padrões de segurança da informação vigentes;

III. Fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações da SECURITYBOX;

IV. Avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;

V. Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;

VI. Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos Colaboradores que violarem o código de ética e conduta, a política de segurança da informação e as normas da SECURITYBOX;

VII. Autorizar acessos de seus colaboradores apenas quando forem realmente necessários e seguindo os conceitos de “need to know” e “least privilege".

d) As responsabilidades da coordenação de infraestrutura são:

I. Orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;

II. Desenvolver e estabelecer programas de conscientização e divulgação da política de segurança da informação;

III. Conduzir o processo de gestão de riscos de segurança da informação;

IV. Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

V. Conduzir a definição controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;

VI. Propor projetos e iniciativas para melhoria do nível de segurança das informações da SECURITYBOX.

VII. Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software;

VIII. Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia, sempre alinhados com o DPO;

IX. Conduzir a gestão dos acessos a sistemas e informações da SECURITYBOX;

X. Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;

XI. Informar imediatamente a área de gestão de riscos, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da SECURTIYBOX;

XII. Controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação da empresa ou em sua segurança;

XIII. Garantir a continuidade dos serviços tecnológicos de maneira a atender aos requisitos essenciais do negócio;

XIV. Garantir que todos os ativos críticos de tecnologia da informação devam ser instalados em ambientes especializados e adequados. Estes devem conter todas as proteções e contingências necessárias para a sua respectiva proteção.

e) As responsabilidades da Área de Recursos Humanos são:

I. Verificar o histórico de candidatos a emprego, de acordo com a ética e leis vigentes;

II. Garantir que a política, normas e procedimentos da política de segurança da informação sejam divulgados no processo de admissão/integração de novos colaboradores.

f) As responsabilidades da Área Jurídica são:

I. Apoiar a aplicação de medidas disciplinares referente a violações da política de segurança da informação;

II. Identificar e monitorar requisitos legais pertinentes à segurança da informação;

III. Garantir a adoção de cláusulas pertinente à segurança das informações nos contratos estabelecidos com a SECURITYBOX.

g) As responsabilidades de Fornecedores e Parceiros de Negócios são:

I. Cumprir as determinações da política, normas e procedimentos publicados pela SECURITYBOX;

II. Orientar os empregados da empresa sobre o cumprimento das determinações da política, normas e procedimentos publicados pela SECURITYBOX;

III. Cumprir com o acordo de confidencialidade e determinações da ANPD e Lei 13.709/18.

5. DIRETRIZES PARA TRATAMENTO DAS INFORMAÇÕES

As diretrizes para realização do tratamento de informações devem observar um propósito legítimo, específico, explicito e deve ser informado ao titular dos dados, conforme POP2024-003.

a) Toda informação deve ter regras claramente definidas pelo seu proprietário para proteção contra perda, alteração e acesso, seja ela armazenada em meio eletrônico (computador central, servidores de rede, microcomputadores, pen drive, e-mail, etc), em papel (correspondências, atas, relatórios, manuscritos, etc.) ou outros meios;

b) Toda informação deve ter usuários explicitamente definidos (instituições, áreas, pessoas) e os tipos de direitos que cada um terá para acessá-la;

c) Toda informação deverá ter procedimentos para protegê-la do acesso de pessoas não autorizadas;

d) Toda informação que garanta a continuidade das atividades da SECURITYBOX, deverá ter cópia de segurança em local distinto, devidamente protegido para essa finalidade ou outro meio eficiente para permitir sua pronta recuperação em caso de perda ou danos;

e) As informações contidas em material que se tornar disponível para descarte (papel, pen drives, CD, etc) deverão ser destruídas ou mantidas em locais fechados, protegidas do acesso de pessoas não autorizadas;

f) Todo colaborador da SECURITYBOX, é responsável pela segurança da informação a que tem acesso;

g) Toda informação encontrada extraviada deverá ser, imediatamente, devolvida a sua origem;

h) Os equipamentos que contiverem informações da SECURITYBOX, somente poderão ser deslocados para venda, manutenção, etc, quando certificado de que as informações neles contidos estejam completamente eliminadas.

6. RECOMENDAÇÕES PARA O TRATAMENTO DA INFORMAÇÃO

A seguir estão indicadas recomendações no que tange o tratamento de informações.

a) Os colaboradores não devem efetuar tentativas de obter acesso às informações que não lhe são permitidos, devendo solicitá-las ao respectivo proprietário da informação, pasta ou arquivo;

b) A elaboração das normas e procedimentos de acesso deverá levar em consideração os riscos do acesso e alteração não autorizados, divulgação indevida e indisponibilidade dos dados, que tem por consequência às fraudes, problemas legais, perdas de negócios, danos à imagem e dificuldade na recuperação da informação.

c) A SecurityBox está comprometida em manter os padrões de segurança da informação em todas as suas operações. Como parte desse compromisso, implementamos e integramos de forma eficaz a segurança da informação ao gerenciamento de projetos. Isso garantirá que os riscos de segurança sejam identificados, avaliados e tratados desde as fases iniciais de cada projeto, independentemente de sua natureza ou escopo. A integração da segurança da informação ao gerenciamento de projetos fortalecerá nossa capacidade de proteger os dados sensíveis da empresa e garantir a confidencialidade, integridade e disponibilidade das informações em todas as etapas do ciclo de vida do projeto.

7. OBJETIVO E DIRETRIZES PARA CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação tem o objetivo de proporcionar ao usuário a possibilidade de analisar suas informações, facilitando a definição do seu nível de acesso e condições de armazenamento, considerando sua confidencialidade, integridade e disponibilidade.

a) Todas as informações devem ser classificadas;

b) Toda a informação deverá ser considerada sigilosa e de alto risco até que se tenha estabelecido sua classificação;

c) A proteção proporcionada à informação, tanto em termos de acesso quanto de conservação, deve estar de acordo com sua classificação;

d) Quando em um mesmo meio físico existirem informações classificadas de maneiras diferentes, deve-se adotar, para fins de segurança, a classificação mais restrita;

e) Sempre que forem efetuadas alterações significativas em um sistema informatizado, ou nas características de uma informação, deverá ser comunicado aos usuários com antecedência e efetuada uma revisão de classificação.

8. CONCEITOS DE CONFIDENCIALIDADE

Em segurança da informação, confidencialidade é o ato ou esforço de uma organização para garantir que as informações e dados sejam mantidos em segredo ou privados. A seguir estão indicados os tipos de informações e suas características:

I. Informações Sigilosas: Informações extremamente restritas quanto a sua divulgação. São de alto valor por motivos estratégicos e/ou com grande possibilidade de provocar prejuízos, razão pela qual seu nível de proteção deve ser o mais alto possível;

II. Informações Confidenciais: Informações de caráter setorial e para divulgação a um reduzido grupo de pessoas de uma área ou setor de atividade;

III. Informações Internas: São aquelas que têm sua circulação restrita ao âmbito interno da SECURITYBOX, divulgadas a clientes e fornecedores;

IV. Informações Públicas: São aquelas que circulam livremente, interna e externamente, não havendo interesse em controlar sua divulgação e acesso.

9. CONCEITOS DE RESTRIÇÃO AO ACESSO

A informação de acesso restrito, é toda aquela que deve ser divulgada apenas a quem de direito compete, cabendo análise individual para cada caso e as restrições ao acesso podem ser:

I. Controlado: O acesso às informações sigilosas, confidenciais e internas deverá ser determinado pelo comitê diretivo, que estabelecerá as áreas, pessoas e o nível desse acesso;

II. Não Controlado: As informações públicas não estarão sujeitas ao controle de acesso.

10. CONCEITOS DE NÍVEIS DE ACESSO

O conceito de níveis de acesso, remete à possibilidade da visualização das informações ou da capacidade e permissão de alterações das mesmas. Os níveis de acesso podem ser:

I. Somente para consulta: Nível de acesso do usuário, permite somente a leitura das informações;

II. Consulta e alteração: Nível de acesso do usuário, permite efetuar mudanças nas informações disponibilizadas, como inclusão de pareceres, informações complementares, valores, etc.

11. CONCEITOS DE INTEGRIDADE E DISPONIBILIDADE

Conceitualmente, a integridade significa manter as informações em seu formato original e verdadeiro, enquanto a disponibilidade, se refere ao acesso dos dados por seu titular sempre que for necessário. A integridade e disponibilidade podem ser:

I. De Alto Risco: Informações cuja indisponibilidade e/ou inexatidão poderão causar prejuízos à continuidade dos negócios;

II. De Médio Risco: Informações que impõem ao negócio problemas de disponibilidade e dificuldade na recuperação. O proprietário da informação e os usuários aceitam a disponibilidade limitada e a existência de um determinado tempo para recuperação;

III. De Baixo Risco: Informações cuja exatidão e acessibilidade apresentam pouco ou nenhum risco ao negócio. Os usuários aceitam eventuais indisponibilidades e longos períodos para recuperação das informações.

12. CONCEITO DE SENHA FORTE

Uma senha considerada forte é aquela que foge da obviedade e que por sua maior complexidade, torna-se mais difícil de ser explorada e descoberta. As senhas consideradas fortes devem considerar as seguintes características:

I. Devem possuir um misto de letras maiúsculas e minúsculas, números, pontuação e caracteres especiais como “@”, “#”, “$” etc.;

II. Devem possuir no mínimo 8 caracteres de comprimento;

III. Não devem ser baseadas em informações pessoais óbvias, como por exemplo, nome ou sobrenome, data de nascimento, nome dos pais ou dos filhos, número do CPF ou RG, endereço de e-mail etc.;

IV. Não podem conter palavras simples contidas em dicionário;

V. Não devem ser sequencias simples de letras e números, como por exemplo “11111111” ou “12345678” ou “aaaaaaaa” ou “abcdefgh”;

VI. Nunca reutilizar senhas recentes nem que tenham pequenas alterações;

VII. Use senhas diferentes para cada sistema.

VIII. A validade da senha é de 45 dias

13. ADMINISTRAÇÃO DE ACESSO DE USUÁRIOS

A função desempenhada pela coordenação de infraestrutura e que visa garantir a correta gestão de acessos ao ambiente e aos diversos sistemas da SECURITYBOX, deve ser considerada no que tange à administração de acesso de usuários. As principais recomendações para este tema e que estão cobertos pela Política, são:

a) A área de TI, responsável pela execução do controle de acesso aos sistemas e subordinada às determinações de concessões pelas gerências das áreas clientes, deverá manter procedimentos formais que contemplem desde o registro inicial para um novo usuário à administração de privilégios e senhas e o registro de cancelamento de autorizações;

b) A área responsável pelo controle de acessos, deverá garantir a prevenção de acessos não autorizados;

c) Cada usuário deverá gravar os arquivos de sua competência em pasta própria, ficando assim, responsável pelo conteúdo de sua pasta;

d) Cada usuário terá acesso apenas ao seu núcleo de informações concernentes à sua alçada. Em caso de necessidades de informações que fogem da mesma, deverá ser autorizado pela gerência o acesso a tais informações;

e) Todos os acessos, alterações, exclusões, efetuados pelos usuários nos diretórios compartilhados, será registrado em um Log para fins de auditoria.

14. SEGURANÇA DA INFORMAÇÃO - MESA E TELA LIMPAS

A política de mesa limpa e tela limpa, é uma prática de segurança recomendada, que visa reduzir o risco de acesso não autorizado, exposição de dados considerados sensíveis, bem como a perda ou dano da informação durante o período de trabalho normal ou mesmo fora dele. Os tópicos a seguir devem ser considerados para esta tratativa interna:

a) Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não;

b) Os princípios da política de mesa limpa e tela limpa:

I. Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancadas, quando não estiverem em uso, especialmente fora do horário do expediente;

II. Informações sensíveis ou críticas para o negócio da organização, devem ser trancadas em local separado e seguro (um armário ou cofre à prova de fogo por exemplo);

III. Anotações, recados e lembretes não devem ser deixados amostra sobre a mesa ou colados em paredes, divisórias ou no monitor da estação de trabalho;

IV. Não anotar informações sensíveis em quadros brancos;

V. Não guardar pastas com documentos sensíveis em prateleiras de fácil acesso;

VI. Destruir documento impressos antes de jogá-los fora. Sempre que possível utilizar máquinas desfragmentadoras;

VII. Não imprimir documentos apenas para lê-los. Leia-os na tela do computador, se possível;

VIII. Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;

IX. Sempre que possível, utilizar senhas individualizadas nas impressoras para permitir que o documento seja impresso mediante autorização pessoal;

X. Fotocopiadoras devem ser protegidas contra uso não autorizado;

XI. Bloquear sessão do computador sempre que se ausentar do posto de trabalho;

XII. Efetuar bloqueio de sessão automatizado nos computadores após 2 minutos de inatividade;

XIII. A utilização de crachá de identificação é obrigatória para todos os colaboradores, no exercício de suas atividades;

XIV. Nunca deixe o crachá de identificação ou chaves em qualquer lugar; mantenha-as junto a você;

XV. Em caso de perda do crachá de identificação ou chaves de acessos, comunicar imediatamente a coordenação administrativa e o departamento de RH.

15. CONTROLE DE ACESSO A COMPUTADORES E REDE

O controle de acesso a computadores e rede visa manter os registros de acesso e contar com mecanismos de proteção e segurança devidamente padronizados e instalados nos equipamentos, bem como procedimentos de autorização e controles, são essenciais para garantir maior segurança no ambiente e informações manipuladas. As seguintes diretrizes devem ser seguidas como forma de abrangência para este tópico:

a. O controle de acesso deverá assegurar que os usuários de computadores, conectados à rede corporativa da SECURITYBOX, não comprometam a segurança de qualquer sistema operacional ou produto. Para isso toda estrutura da SECURITYBOX, deverá possuir servidores controladores de domínio que garantam que o usuário não efetue alterações indevidas na estação de trabalho. Além disso, todos os computadores devem estar com antivírus corporativo devidamente instalados e ativados;

b. A inserção de qualquer nova informação, realizada por meio de dispositivos removíveis só será liberada mediante autorização do gerente ou gestor do setor responsável. Antes de efetuar a liberação, deverá ser verificado se a estação de trabalho realmente possui antivírus instalado e atualizado;

c. O acesso a serviços computacionais deverá sempre ocorrer através de um procedimento seguro, no qual o usuário conecta-se a um sistema de controle utilizando seu usuário e senha, devendo ser planejado para minimizar os riscos de acesso não autorizados;

d. O acesso às estações de trabalho de forma remota, deverá ocorrer somente mediante autorização do próprio usuário responsável pela estação de trabalho;

e. O acesso ocorrerá através de programa adquirido e licenciado para a SECURITYBOX. Para isso, o setor de operações deverá instalar o programa cliente nas estações de trabalho, proporcionando assim o acesso remoto seguro;

f. Qualquer acesso remoto, que seja efetuado por terceiros, deverá ter o aval e acompanhamento da área de TI da SECURITYBOX;

g. Redes WIFI específicas para navegação internet, denominadas “visitantes” devem estar completamente segregadas da rede interna corporativa, além da aplicação dos devidos controles de acesso e monitoramento.

16. SEGURANÇA FÍSICA DE COMPUTADORES E SERVIDORES

Estabelecer padrões de segurança e procedimentos para avaliar e manter organizados e protegidos computadores e servidores, ampliará a capacidade de gestão, visibilidade e controle da infraestrutura da SECURITYBOX. As seguintes diretrizes devem ser seguidas como forma de abrangência para este tema:

a) Todos os equipamentos deverão ser configurados conforme padrões estipulados pela SECURITYBOX, mais especificamente pelo setor de operações, tanto para computadores, como para os servidores;
b) A estrutura para manter a segurança física dos equipamentos de rede e computadores, devem obedecer aos padrões de segurança gerais da SECURITYBOX e adequar-se, no mínimo, às especificações dispostas neste item;

17. ESTRUTURA FÍSICA (SALA)

Possuir instalações compatíveis e capazes de acondicionar corretamente os equipamentos, é determinante para evitar problemas como interrupções de serviços indispensáveis e garantir a segurança de equipamentos e informações da SECURITYBOX. As seguintes diretrizes devem ser seguidas como forma de abrangência para este tópico:

a) As dimensões do local devem ser suficientes para a instalação dos equipamentos de rede e servidores;

b) No caso dos servidores de rede, a sala deve ser fechada com uso de chaves ou fechaduras eletrônicas, restringindo o acesso ao ambiente;

c) A disposição dos cabos lógicos e de energia devem ser instalados em canaletas específicas para que não haja interferência na rede e deve ser adequada para que as pessoas possam transitar livremente;

d) As entradas de ar (ventilação) dos equipamentos devem estar desobstruídas;

e) As estações de trabalho e os servidores, devem estar instalados em locais firmes, que evitem trepidações.

18. REFRIGERAÇÃO E QUALIDADE DO AR

Ter um ambiente climatizado e controlado, garantirá a máxima eficiência e preservação dos equipamentos instalados, promovendo assim menor índice de falhas e manutenções. As seguintes diretrizes devem ser seguidas como forma de abrangência para este tema:

a) A climatização deve obedecer aos padrões especificados pelo fabricante, quando aplicável;

b) O ambiente deve estar livre de poluição por poeira, gases ou fumaça, evitando que a poluição danifique os equipamentos, possibilitando a quebra dos mesmos ou falhas de processamento.

19. REDE ELÉTRICA

É fundamental garantir uma rede elétrica eficiente, segura e contando com equipamentos para proteção dos equipamentos instalados e a segurança de equipamentos e estrutura física do próprio ambiente físico da SECURITYBOX. Para tanto, as seguintes diretrizes devem ser seguidas como forma de cumprimento para este tópico:

a) É necessário que exista aterramento exclusivo para os equipamentos e estabilização dos pontos de energia elétrica. Os equipamentos de estabilização de energia (Nobreaks) deverão ter uma autonomia mínima de 60 minutos (para evitar a parada da operação) ou de 20 minutos (para que os equipamentos sejam devidamente desligados, sem oscilações de tensão que possam danificá-los);

b) O uso de tomadas compartilhadas através de duplicadores (benjamins ou similares) deverá ser autorizado pelo setor de operações e obedecido os padrões de segurança determinados pelo fornecedor (no caso, optar sempre por filtros de linha com certificado);

c) Os equipamentos devem ser instalados em uma rede elétrica exclusiva, conforme os padrões recomendados pelos fabricantes, e a voltagem das tomadas devidamente identificadas;

d) As instalações elétricas devem sofrer revisões preventivas periódicas a cada 180 dias ou de acordo à disponibilidade e planejamento da área de coordenação de infraestrutura da SECURITYBOX.

20. EQUIPAMENTOS CONTRA INCÊNDIO

Possuir uma estrutura de contingência contra incêndios, revisada, compatíveis com os tipos de materiais existentes no ambiente e com uma equipe capacitada para atuar em caso de emergências, é uma medida de segurança muito importante e que deve ser observada. Assim, para atendimento a esta diretriz da política, as seguintes premissas devem ser atendidas:

a) Devem existir equipamentos de combate a incêndios adequados para materiais eletrônicos, tais como extintores de CO2, e estes devem estar em local visível, sinalizado e desobstruído, e ser de conhecimento de todos os funcionários;

b) Os equipamentos de combate a incêndios deverão sofrer revisões preventivas periódicas de equipe especializada conforme norma ABNT NBR 12962.

21. CUIDADOS COM EQUIPAMENTOS QUE ARMAZENAM DADOS E INFORMAÇÕES

Garantir que as informações estão seguras e que não são mais acessíveis, é um cuidado que necessita ser aplicado inclusive para efetuar o correto descarte, descontinuação ou manutenção de equipamentos de armazenamento de dados da SECURITYBOX. Para que essas diretrizes sejam atendidas, as seguintes medidas devem estar cobertas:

a) Quando os equipamentos que armazenam dados e informações forem vendidos, devolvidos ao fabricante, enviados para manutenção ou doados para instituições e outras finalidades do tipo, as informações neles contidas devem ser destruídas antes de deixar as dependências da SECURITYBOX;

b) É importante ressaltar que para esse equipamento, não é suficiente apenas apagar os dados. Deve-se executar um programa de formatação que realmente os destrua (Wipe);

c) As manutenções dos equipamentos que armazenam dados e informações realizadas no próprio local, devem ser acompanhadas pelo responsável da área (coordenação de infraestrutura) ou de um colaborador designado. É de fundamental importância que a manutenção seja solicitada através de chamado ao Help Desk e o atendimento seja previamente acordado com o solicitante. No caso da presença física de colaborador da área de TI ou de terceiros, os mesmos devem ser identificados e portar crachá/identificação. Caso haja qualquer dúvida, não permitir o atendimento e acionar a coordenação de infraestrutura da SECURITYBOX para confirmação.

22. LICENCIAMENTO DE SOFTWARES

Utilizar sistemas e softwares licenciados é fundamental para um ambiente seguro, atualizado e controlado. As seguintes diretrizes devem ser seguidas como forma de abrangência para este tema:

a) Todo equipamento deverá ter o seu sistema operacional devidamente licenciado obedecendo os termos de utilização do fabricante;

b) Softwares de uso diário, que não possuírem licenças gratuitas, também deverão obedecer às regras de licenciamento do fabricante;

c) Todo e qualquer software utilizado nas estações de trabalho ou servidores, que não esteja devidamente licenciado nos termos definidos pelo padrão da SECURITYBOX e que não obedeçam às regras de licenciamento do fabricante, será de total responsabilidade do colaborador, assim como instalações futuras de softwares ou sistemas operacionais não licenciados;

d) O setor de operações não tem autorização para efetuar instalações de softwares não licenciados. Se o colaborador optar pela instalação de um software não licenciado, o mesmo estará se responsabilizando pelas penalidades/multas que tal ação poderá acarretar.

23. DIRETRIZES PARA SEGURANÇA FÍSICA DE EQUIPAMENTOS

O objetivo das diretrizes de segurança física dos equipamentos é garantir à SECURITYBOX, a administração e utilização correta dos recursos e dados armazenados nos servidores de maneira segura. Para tal, medidas adequadas deverão ser tomadas respeitando os princípios de confidencialidade,

integridade e disponibilidade das informações que são armazenadas e manipuladas através desses equipamentos:

a) Todos os equipamentos que armazenam informações e dados, que são essenciais para o funcionamento da empresa, deverão estar armazenados em locais devidamente protegidos contra o acesso de pessoas não autorizadas;

b) Os equipamentos não ligados à rede (“stand-by”) e que armazenam informações de alto e médio risco, deverão estar instalados em locais que garantam a segurança física desses equipamentos, incluindo sistemas que mantenham o fornecimento de energia elétrica e a recuperação dos dados caso haja necessidade de utilizar esse equipamento em algum momento;

c) Os equipamentos que estejam ligados a uma rede, deverão manter as informações classificadas como de alto e médio risco no servidor;

d) Todas as pessoas que estiverem autorizadas a utilizar informações da SECURITYBOX fora de suas dependências físicas, deverão obedecer às mesmas diretrizes estabelecidas para os equipamentos instalados internamente;

e) Todos os equipamentos portáteis que tenham capacidade de armazenamento de dados, devem ser protegidos conforme especificação da SECURITYBOX. Quando estes equipamentos contiverem informações que não possam ser de conhecimento público, devem ter seu acesso protegido por senha e utilizada algum recurso de criptografia de dados;

f) A responsabilidade sobre os equipamentos localizados nas diversas áreas integrantes da rede da SECURITYBOX compete à coordenação de infraestrutura, com apoio da coordenação administrativa, que deverá manter registros atualizados sobre cada equipamento disponibilizado e seus respectivos receptores.

24. SEGURANÇA FÍSICA DOS SERVIDORES

Para proteger e restringir acesso aos servidores, é fundamental ampliar as ações de segurança para proteger as informações e a infraestrutura para a SECURITYBOX, de acordo com as seguintes premissas:

a) O acesso físico aos equipamentos que armazenam dados e informações essenciais para o funcionamento dos sistemas, deverão estar alocados em uma sala reservada e o acesso deverá ser rigorosamente restrito às pessoas autorizadas;

b) Os servidores deverão estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica estabilizada e recuperação de dados;

25. CONCEITOS PARA ELABORAÇÃO DO PLANO “BACKUP”

Todas as informações e sistemas considerados como imprescindíveis, devem estar contemplados nas rotinas de backup operacional/contingencial, considerando aspectos como a periodicidade da atualização dos dados e as particularidades inerentes à operação da SECURITYBOX. Para tanto, as seguintes considerações devem ser atendidas para este requisito:

a) “Backup” contingencial é a cópia das informações sensíveis, “software” e sistemas vitais à continuidade dos negócios da SECURITYBOX e deve ser guardado em duas cópias, sendo que uma, obrigatoriamente, deve ser guardada em local externo, seja em estrutura física ou em cloud (nuvem). Destina-se a permitir a recuperação em situações catastróficas;

b) Os procedimentos, prazos e quantidade de cópias de “backup” / “restore” deverão ser formalmente documentados de forma a permitir sua execução, manutenção e auditoria. Tais procedimentos devem também ser referenciados no plano de recuperação de desastres (DRP);

c) As cópias de segurança deverão ser identificadas, catalogadas e registradas, de forma única e padronizadas, de maneira a permitir sua fácil localização e utilização;

d) A elaboração do Plano backup/*restore* deve conter:

I. Abrangência: Relação dos arquivos e diretórios a serem copiados no processo de "backup";

II. Periodicidade: Intervalo de tempo no qual o sistema é submetido à rotina de "backup";

III. Retenção: Prazo pelo qual os arquivos de "backup" devem ser mantidos;

IV. Procedimentos: Descrição dos procedimentos de "backup";

V. Quantidade de cópias: Número de cópias de "backup", locais e meios de armazenamento;

VI. Identificação dos meios de armazenamento: Os meios de armazenamento devem estar devidamente identificados;

VII. Registro do uso das cópias de "backup": A manipulação dos meios de armazenamento deve ser registrada e controlada. Estes registros devem ser guardados por 90 (noventa) dias para futuras verificações;

VIII. Manutenção das cópias "backup": Quando o prazo de retenção for superior ao especificado pelo fabricante para tempo de vida útil do meio de armazenamento, deve-se adotar um procedimento de regravação dos dados em nova unidade do meio de armazenamento, periodicamente, respeitando o tempo de vida útil do mesmo.

26. CONSCIENTIZAÇÃO E DIVULGAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Esta premissa visa garantir que a segurança da informação não seja apenas conhecida, mas que seja compreendida por todos os colaboradores, orientando sobre as melhores práticas, requisitos mínimos de segurança, quais os riscos e responsabilidades existentes e quais são as implicações e medidas que serão aplicadas em caso de incidentes de segurança da informação.

a) Os recursos e as informações de propriedade ou sob custódia da SECURITYBOX devem ser utilizados de acordo com os interesses da organização, para prestação dos seus serviços, atendendo aos requisitos e respeitando as regras estabelecidas;

b) A política de segurança da informação, normas e padrões de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos colaboradores, tanto pelas equipes de recursos humanos quanto pelos gestores das áreas;

c) Programas de conscientização, divulgação e reciclagem do conhecimento da política de segurança da Informação devem ser estabelecidos e praticados regularmente para garantir que todos os colaboradores e terceiros conheçam as diretrizes e responsabilidades relacionadas à segurança das informações.

27. PLANO DE CONTINUIDADE DE NEGÓCIO

O Plano de Continuidade de Negócio (PCN) é um processo que visa garantir a recuperação dos processos críticos da SECURITYBOX em casos de indisponibilidade do ambiente ou de quaisquer recursos que impossibilitem o desenvolvimento ou as operações de cada área de negócio. O PCN deve contemplar minimamente os seguintes requisitos:

a) Deve-se estabelecer, documentar, implantar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para os serviços e processos de negócio da SECURITYBOX, durante situações adversas. O modelo a ser adotado para a Gestão de Continuidade de Negócios (PCN) deverá ser baseado na Norma ISO/IEC 22301;

b) Deve-se efetuar uma revisão periódica do PCN, anualmente, a fim de identificar pontos que estejam em desacordo com a situação atual, observando pontos como troca de fornecedores, alterações de sistemas, mudanças em procedimentos, entre outros.

28. GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

A gestão de riscos de segurança da informação, segundo a ISO/IEC 27005:2008, é o processo sistemático de gestão organizacional que determina a aplicação equilibrada de controles de segurança, baseado no perfil de riscos de segurança conhecido. Portanto, é fundamental que haja uma Gestão e análise de riscos de acordo com as seguintes premissas:

a) A gestão de riscos de segurança da informação deve ser realizada através de um processo estruturado que contemple a identificação, análise, avaliação, priorização, comunicação, tratamento e monitoração dos riscos que podem afetar negativamente os negócios da SECURITYBOX;

b) O processo de gestão de riscos deve contemplar novos ativos, sistemas ou processos, quer sejam eles internos, em nuvem ou conduzidos por parceiros;

c) Os planos de ação devem ser considerados para o planejamento estratégico organizacional, conforme as prioridades.

29. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Um incidente de segurança da informação, é um evento adverso confirmado, que comprometa a confidencialidade, integridade ou a disponibilidade de dados afetados. As referências acerca deste tema devem atender aos seguintes requisitos:

a) São considerados incidentes de segurança da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de SI: confidencialidade, integridade, disponibilidade, conformidade e não-repúdio, colocando o negócio em risco;

b) Violações ou tentativas de violação desta política, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança;

d) Colaboradores devem informar imediatamente à coordenação de infraestrutura todas as violações à política de segurança da informação, normas, padrões incidentes ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento;

e) A identificação de incidentes de segurança pode ocasionar o bloqueio imediato dos acessos dos colaboradores envolvidos até que sejam concluídas as investigações necessárias;

f) O processo de gestão de incidentes deve estar documentado, institucionalizado e deve ser seguido por toda a SECURITYBOX.

30. SEGURANÇA EM REDES

Segura em redes remete a qualquer atividade projetada com a finalidade de proteger o acesso, o uso e a integridade da rede corporativa e os dados que nela trafegam.

a) Devem existir controles tecnológicos para proteger o acesso entre redes (incluindo Internet, redes públicas, extranets, acesso remoto, wireless e as diferentes redes de usuários);

b) Equipamentos com diferentes requerimentos de segurança devem ser segregados em redes diferentes;

c) Além do controle de acesso entre as redes, deve ser protegida a informação em trânsito, seguindo os requerimentos da classificação da informação;

d) O acesso remoto somente será permitido para situações em que for indispensável e esteja documentado e com mecanismos de autenticação de múltiplos fatores;

e) Os níveis de segurança (confidencialidade, integridade e disponibilidade) esperados dos serviços de comunicações, devem ser estabelecidos nos contratos firmados com os fornecedores desses serviços;

f) Deve ser implementado controle tecnológico de Firewall para a proteção das redes mais críticas;

g) Controles criptográficos devem ser solicitados, estabelecidos e/ou desenvolvidos, para garantir os níveis de confidencialidade das informações trafegadas, segundo a sua classificação (definido pelo proprietário da informação).

31. REGISTROS DE AUDITORIA

Os registros de auditoria devem ser gerados para possibilitar o rastreamento cronológico e detalhado de todas as alterações em sistemas, aplicações, redes e dispositivos utilizados. As seguintes premissas devem ser consideradas para atendimento a este item da política:

a) Todas as ações de usuários, sistemas e qualquer evento de segurança da informação devem gerar trilhas de auditoria (logs), que deverão ser mantidos por um período mínimo de 1 ano, em local centralizado e protegido contra acessos não autorizados;

b) Não deve haver nenhuma modificação na integridade das trilhas de auditoria (logs), ou seja, não pode haver usuários com permissão de alteração;

c) Todo acesso de consulta, cópia ou tentativa de modificação e exclusão as trilhas de auditoria (logs) devem ser registradas;

d) As falhas nos registros das trilhas de auditoria (logs) devem ser registradas, analisadas e devem ser tomadas providencias para corrigir o erro de forma imediata.

e) O relógio de todos os equipamentos e softwares devem estar sincronizados com os servidores de horas do Brasil (NTP.br) com intuito de facilitar o correlacionamento de eventos e rastreamento de transações.

32. ANÁLISE DE VULNERABILIDADES TÉCNICAS

A análise de vulnerabilidades em sistemas, equipamentos e infraestrutura é fundamental para ampliar a maturidade e capacidade da gestão de incidentes de segurança, permitindo ainda atuar de maneira proativa para mitigar problemas que possam impactar informações e operações da SECURITYBOX. Os seguintes itens devem ser atendidos para a cobertura deste tema:

a) Periodicamente devem ser realizados testes de vulnerabilidades técnicas dos equipamentos críticos da infraestrutura de acordo com o procedimento operacional padrão para este processo;

b) Após os levantamentos, as comparações e identificações dos riscos devem ser executadas, possibilitando o tratamento dos riscos de acordo com seus níveis;

c) Nos casos em que não for possível a eliminação total da vulnerabilidade, deve ser apresentada aceitação do risco ou a determinação de falso positivo;

d) Verificações ou auditorias regulares devem verificar a conformidade com as exigências técnicas dos sistemas e das redes;

e) As auditorias realizadas por terceiros devem identificar claramente as interações com os sistemas em operação;

f) As auditorias técnicas dos sistemas e das redes, devem respeitar as práticas estabelecidas e devem ser realizadas de acordo com as recomendações da organização. Estas auditorias devem ser realizadas por fornecedores reconhecidos e competentes.

33. PREVENÇÃO E DETECÇÃO DE INTRUSÃO

Os sistemas de detecção de invasões (IDS) e prevenção de intrusão (IPS) auxiliam na identificação, registro e interrupções de tentativas de invasão, além de alertar e comunicar aos administradores do ambiente sobre possíveis ameaças. Para que este item seja coberto pela política, as seguintes diretrizes devem ser seguidas:

a) Todos os recursos do sistema de informação expostos à Internet devem ser acompanhados e protegidos por um IDS / IPS;

b) Sempre que o IDS / IPS detecta ou responde a uma tentativa externa mal-intencionada suficientemente grave para ameaçar os recursos do sistema de informações protegidas, uma análise estruturada e procedimento de resposta deve ser executado.

34. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

Para que a proteção contra códigos maliciosos, é fundamental utilizar uma ferramenta de proteção contra vírus e execução de códigos maliciosos, atualizada e corretamente configurada, pois trata-se de uma camada importante para ampliar a segurança contra ameaças no ambiente da SECURITYBOX, conforme disposições abaixo:

a) Deverão ser implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final, como em servidores) para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos;

b) Deve ser verificada a atualização das ferramentas de proteção baseadas em assinaturas, para que estejam nas últimas atualizações disponíveis;

c) Deve ser estabelecida uma frequência de verificação de códigos maliciosos em todos as estações de trabalho, servidores e dispositivos de armazenamento de informações corporativas.

35. CONTROLES CRIPTOGRÁFICOS

Os controles criptográficos são utilizados com o objetivo de proteger a confidencialidade e integridade dos dados manipulados e armazenados, e devem seguir as seguintes recomendações para atendimento à política:

a) Deverão ser utilizados controles criptográficos para proteger as informações segundo os requerimentos da sua classificação;

b) Somente algoritmos de criptografia aprovados pela coordenação de infraestrutura podem ser utilizados para esta finalidade na SECURITYBOX;

c) O gerenciamento das chaves de criptografia deve prever mecanismos para o armazenamento seguro, geração segura da chave e inutilização das chaves gerenciadas;

d) Deverá existir um mecanismo de recuperação da informação caso seja perdida uma chave de criptografia;

e) As chaves de criptografia devem ser trocadas periodicamente, dependendo da sua frequência de utilização;

f) Caso seja comprometida uma chave criptográfica, está deve ser revogada imediatamente. Se for uma chave para criptografia de arquivos, deve ser prontamente substituída;

g) Mecanismos de autenticação e auditoria devem ser estabelecidos para garantir a segurança do acesso às chaves.

Todos os demais controles de segurança relacionados com criptografia de dados, seja em repouso ou em trânsito, estão descritos, especificados e detalhados na política ***58 - POL2024-021 - Política para uso de criptografia - SecurityBox.***

36. SERVIÇO DE NUVEM

Contratar sistemas ou infraestruturas na nuvem (Cloud) é um alterativa cada dia mais utilizada, porém, é de suma importância, considerar todas as condições de segurança oferecidas, conforme:

a) A possibilidade de utilização de uma solução de hospedagem externa, e, mais especificamente, uma solução de 'cloud computing', depende do nível de sensibilidade dos dados e os processos relacionados. Esta escolha deve ser feita com base na execução de uma análise de riscos;

b) Toda e qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, deverá ser previamente comunicada à coordenação de infraestrutura da SECURITYBOX e deve ter a aprovação desta;

c) Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles software como serviço (SaaS) ou armazenamento de base de dados, devem possuir acesso seguro através de interfaces HTTPS no mínimo, bem como a autenticação segura e em ambientes segregados;

d) Os acessos devem ser controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada colaborador/terceiro ou administrador,

possuindo também tais acessos e ações, registrados em trilhas de auditorias específicos para essa finalidade.

37. GESTÃO DE INCIDENTES DE SEGURANÇA

A gestão de incidentes de segurança da informação, pode ser definida como sendo os procedimentos estabelecidos para identificar, gerenciar, registrar, analisar e comunicar quaisquer incidentes de segurança da informação, a fim de minimizar o impacto negativo causado e permitir o rápido restabelecimento das operações, conforme as seguintes condições:

a) Qualquer evento relacionado a um suposto ou comprovado ataque a segurança de um sistema, deve ser resolvido de acordo com um processo de gerenciamento de incidentes previamente estabelecido;

b) Os procedimentos envolvidos devem descrever o processo de gerenciamento de incidente, o processo de investigação e o processo de recolhimento de provas. O processo de gerenciamento de incidente deve:

I. Permitir a detecção, o mais cedo possível, e a capacidade de responder com a máxima eficácia para limitar os danos causados pelo incidente;
II. Limitar as zonas de vulnerabilidade pela remediação de anomalias identificadas em algum ou todos os sistemas potencialmente afetados;
III. Reter informações relevantes para posteriores investigações e coleta de provas; compilar um registro de incidentes de segurança e estatísticas para uso na previsão e prevenção de possíveis futuros incidentes;
IV. Identificar pontos de contato apropriados para compreender o nível da severidade do ataque em curso;
V. Caso seja um incidente de segurança que comprometa os dados pessoais de titulares, o DPO deve ser imediatamente comunicado.

c) Uma vez que um incidente mal-intencionado for solucionado, uma análise deve ser efetuada para identificar a origem do ataque e iniciar procedimentos administrativos ou judiciais apropriados.

38. GESTÃO DE FORNECEDORES

As atividades relacionadas com a análise e avaliação de características, requisitos e comprovações técnicas para produtos e serviços prestados para a SECURITYBOX, devem seguir as seguintes condições:

a) O gerenciamento de fornecedores deverá considerar a avaliação de risco e classificação dos fornecedores (estratégico, tático, operacional);
b) O desempenho de fornecedores críticos de ser avaliado em intervalos regulares definidos, com a finalidade de verificar quanto ao cumprimento das metas acordadas e se os resultados estabelecidos foram alcançados. Os resultados devem ser discutidos com o fornecedor para se identificar as necessidades e oportunidades de melhoria;
c) Cada fornecedor deverá ter um gestor designado que acompanha o seu desempenho, tornando-o responsável pela qualidade dos serviços oferecidos para a SECURITYBOX.

39. EXCEÇÕES

Ocorrências relacionadas ao funcionamento da Política da Segurança da Informação, não contempladas neste regulamento, serão levadas para conhecimento e deliberação da Diretoria.

40. PENALIDADES

O colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares cabíveis.

41. REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de Segurança da Informação deverá ser revista e atualizada, ao menos uma vez a cada ano, com vistas a se manter em consonância com as regras de negócio, coerente e aderente com as melhores práticas do mercado, leis, regulamentos e demais aspectos legais aplicáveis.

42. DAS REFERÊNCIAS

Para um entendimento mais abrangente sobre esta política de Segurança da Informação, deve-se consultar os documentos abaixo referenciados:

I. Política de Gestão de Incidentes de Segurança da Informação;

II. NSI 001 Norma de Administração de Ambientes Tecnológicos;

III. NSI 002 Norma de Gestão de Riscos em Segurança da Informação;

IV. ISO 22301

V. ISO/IEC 27.000/2022

VI. Cobit 5 – DS4

VII. NIST 800-30 VIII. NIST 800-39 IX.

VIII. Lei 13.709/18.

43. DAS DÚVIDAS

Em caso de dúvida solicitar esclarecimento a coordenação de infraestrutura da SECURITYBOX.

44. DOS CONTROLES DE REGISTROS

Identificação	Armazenamento	Segurança / Proteção	Recuperação/ Rastreabilidade	Tempo de Retenção	Descarte

45. DAS DISPOSIÇÕES FINAIS

a) Esta Política de Segurança da Informação foi aprovada em reunião de Diretoria realizada em seis de maio de 2024.

TERMO DE CIÊNCIA E CONCORDÂNCIA

Eu, _____,
inscrito na matrícula sob nº _____, declaro que recebi e tenho pleno conhecimento do teor da Política de Segurança da Informação, normas e instruções aqui fornecidas.

Concordo expressamente com todas as regras inerentes à esta Política de Segurança da Informação, normas e instruções e me comprometo em cumprir integralmente todas as regras estabelecidas na política, normas e instruções apresentadas.

Tenho ciência de que o descumprimento da Política de Segurança da Informação e qualquer uma de suas normas e instruções, poderá acarretar a extinção do meu contrato de trabalho firmado com a SECURITYBOX, bem como as consequências jurídicas decorrentes da violação.

Por ser verdade, firmo o presente.

_____, ____ de _____ de _____.

_____

Assinatura do colaborador

46. DOCUMENTOS NORMATIVOS

- Código de Conduta de Colaboradores;
- LGPD - Lei nº 13.709, de 14 de agosto de 2018;
- Norma ISO 27001 Gestão de Segurança da Informação;
- NIST SP 800-161 Rev. 1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

49. RECIBO DE ENTREGA DE EQUIPAMENTOS ELETRÔNICOS

A seguir, modelo de recibo de controle de entrega de equipamentos eletrônicos a ser obrigatoriamente ofertado ao coletor dos equipamentos eletrônicos que estão para descarte, a fim de garantir a ausência de disco rígido ou semelhante que possa conter informações privilegiadas da empresa, estando disponível de maneira avulsa também na documentação interna da SECURITYBOX:

RECIBO DE CONTROLE DE ENTREGA DE EQUIPAMENTOS ELETRÔNICOS

Eu, _____, CPF/CNPJ nº_____, recebi da SECURITYBOX SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO LTDA, os equipamentos abaixo discriminados, destinados a descarte ecológico, reforçando que dentre os equipamentos descartados, não consta nenhum disco rígido ou semelhante que possa conter informações ou dados privilegiados.

Data ___/___/_____

_____

Assinatura do coletor

DATA	QUANTIDADE	EQUIPAMENTO	ASSINATURA

Controle de Aprovação

Data	Ação	Versão	Aprovador	Assinatura
15/06/2024	Aprovação	2.0	George SIlverio da Silva	gov.br Documento assinado digitalmente GEORGE SILVERIO DA SILVA Data: 16/07/2024 19:34:21-0300 Verifique em https://validar.iti.gov.br

SECURITYBOX SEGURANÇA EM TECNOLOGIA A INFORMAÇÃO LTDA.
CNPJ: 11.928.104/0001-87
End: R. Emanuel Kant, 60 Sala 609
Curitiba – PR Telefone: 41 2170-0770