POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Diretoria Responsável: Tecnologia da Informação
Gerência Responsável: Gerente de Infra CloudOps & Infra IT
Gerência Responsável: Gerente de Governança de TI
Criação: Henry Wood
Atualizado por: Henry Wood

O que você encontra nesse documento:
As diretrizes que regem os processos de segurança da informação de acordo com a Política de Governança da PayBrokers e suas estratégias.

1. OBJETIVO

A Política de Segurança da Informação (PSI) tem como objetivo proteger a confidencialidade, integridade e disponibilidade das informações de acordo com as melhores práticas adotadas pela empresa e diretrizes da Política de Governança de TI.

2. ABRANGÊNCIA

Esta PSI abrange integralmente todas as operações de Tecnologia da Informação da PayBrokers e seu conglomerado. Estabelece diretrizes e regras que devem ser seguidas por todos os colaboradores, incluindo alta administração, usuários finais, parceiros de negócios e quaisquer indivíduos que utilizem os recursos tecnológicos da empresa.
Esta política baseia-se nas diretrizes da:

- Política de Governança de TI (GTI);

Complementa:

- Norma de Cibersegurança (NCSEC);
- Norma de Segurança da Informação (NSI);

Apoia a:

- Política de Governança de Dados (PGD);
- Norma de Gestão de Dados (NGD);
- Norma de Gestão de Riscos (NGR-TI).

Parceiros de negócios e terceiros, terão acesso a um manual de utilização dos recursos oferecidos pela PayBrokers.

3. REFERÊNCIAS NORMATIVAS

Esta política está baseada nas melhores práticas:

- ISO/IEC 27001: Sistemas de Gestão de Segurança da Informação (SGSI);
- ISO/IEC 27002: Sistemas de Gestão de Segurança da Informação (SGSI);
- ISO/IEC 27701: Sistemas de Gestão de Informações de Privacidade;
- ITIL (Information Technology Infrastructure Library);
- COBIT (Control Objectives for Information and Related Technologies);
- Framework NIST: NIST SP 800-53
- Lei nº 12.965 de 23 de abril de 2014 – Marco Civil da Internet;
- Lei nº 13.709 de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD);
- Portaria SPA/MF nº 722/2024
- Resolução BCB n° 85 de 08/04/2021

Todos os pontos descritos neste tópico, orientam a criação desta PSI, assim como as normas e estruturas utilizadas estão em conformidade com as resoluções e leis exigidas.

4. DEFINIÇÕES RELEVANTES

Esta política está definida organizacionalmente de acordo com a relevância dos tópicos apresentados abaixo:

- Controle de Acesso;
- Gestão de Identidade e Acesso (IAM);
- Testes de Intrusão;
- Implementação de Processos de Criptografia;
- Monitoramento e Respostas a Incidentes;
- Gestão de Vulnerabilidades e Riscos;
- Regras de Uso;
- Estabelecimento de Processos;
- Classificação da Informação;
- Proteção de Dados;
- Conformidade e Regulamentações;
- Treinamentos e Conscientização de Usuários;
- Documentação e Revisão.

As definições relacionadas a este tópico, estão descritas no final deste documento no tópico 19. Glossário.

5. CONTROLE DE ACESSO

Este tópico visa estabelecer controles de acesso rigorosos, garantindo que o acesso aos sistemas e dados críticos seja concedido apenas a pessoal autorizado, consolidando uma abordagem eficaz na defesa em profundidade da segurança da informação.

Princípios Gerais de Controle de Acesso:

Defesa em Profundidade:
A segurança é uma soma de controles complementares, não dependendo de um único controle. Podemos assim definir em **6** principais aspectos:

- Camadas de Segurança

  A defesa deve incluir diversas camadas, como controles físicos (ex.: acesso restrito às instalações), controles técnicos (ex.: firewalls, antivírus) e controles administrativos (ex.: políticas de acesso). Cada camada atua como uma barreira adicional contra invasões.
- Redundância

  A implementação de várias defesas cria redundância. Se uma camada falhar, outras continuarão a proteger os ativos, minimizando o risco de uma violação completa. Isso é crucial em um cenário onde as ameaças estão em constante evolução.
- Monitoramento e Resposta

Sistemas de monitoramento devem ser integrados para detectar atividades suspeitas em tempo real. A capacidade de resposta rápida a incidentes é fundamental para mitigar danos e restaurar a segurança rapidamente.
- Cofre de Senhas

Deverá ser adotado uma ferramenta para gerenciamento de senhas. Esta ferramenta deverá ser capaz de armazenar e gerenciar senhas de forma segura, criptografando as informações, permitindo que os usuários acessem suas credenciais de login de maneira prática e protegida. Além de senhas, esta ferramenta deverá guardar dados confidenciais, como notas e informações de cartões de crédito.
- Treinamento e Conscientização

Os funcionários devem ser treinados regularmente sobre práticas seguras e a importância da defesa em profundidade. A conscientização é uma linha de defesa crítica, pois muitos incidentes de segurança resultam de erro humano.
- Avaliação Contínua

É necessário realizar avaliações regulares das camadas de segurança para identificar vulnerabilidades e garantir que as defesas sejam atualizadas e eficazes contra novas ameaças.

Privilégio Mínimo:
Essa abordagem visa garantir que os usuários tenham acesso apenas às informações e recursos necessários para desempenhar suas funções, minimizando assim o risco de vazamentos e abusos.

- Acesso Restrito

  Cada colaborador deve ter permissões limitadas, baseadas em suas responsabilidades. Isso significa que, mesmo que um usuário tenha acesso a um sistema, ele poderá visualizar ou modificar informações relevantes ao seu trabalho.
- Revisão de Acesso

É essencial realizar revisões periódicas das permissões concedidas. Isso ajuda a identificar e revogar acessos desnecessários, especialmente quando colaboradores mudam de função ou permitem a organização.
- Autenticação Rigorosa

Implementar métodos robustos de autenticação, como autenticação multifator (MFA), para garantir que apenas usuários autorizados possam acessar sistemas críticos.

- Monitoramento de Atividades

Estabelecer um sistema de monitoramento para registrar e auditar acessos e atividades dos usuários. Isso permite identificar comportamentos suspeitos e responder rapidamente a incidentes.

- Educação e Conscientização

Promover treinamentos regulares sobre a importância do privilégio mínimo e práticas seguras de acesso à informação, garantindo que todos os colaboradores compreendam suas responsabilidades.

Necessidade de Saber:

O acesso é concedido apenas às informações essenciais para o desempenho de uma função, nada além disso.

- Acesso Baseado em Funções (RBAC)

O acesso a informações deve ser determinado com base nas responsabilidades e funções específicas de cada colaborador. Apenas aqueles cuja atividade requer acesso a dados sensíveis devem tê-lo.

- Avaliação de Necessidade

Antes de conceder acesso, você deve realizar uma avaliação rigorosa para determinar se o colaborador realmente precisa das informações para suas atividades diárias.

- Documentação e Justificativa

Manter registros documentados que justifiquem as concessões de acesso, incluindo a razão pela qual o acesso foi necessário e por quanto tempo.

- Revisão Contínua

Implementar revisões periódicas dos acessos concedidos, garantindo que os direitos de acesso sejam atualizados ou revogados conforme alterações nas funções ou na estrutura organizacional.

- Treinamento e Conscientização

Promover treinamentos sobre a importância do princípio da Necessidade de Saber, ajudando os colaboradores a entender suas responsabilidades no fornecidas com informações sensíveis.

Necessidade de Usar:

Garante que o acesso a recursos e informações seja concedido apenas quando necessário para a execução de tarefas específicas.

- Acesso Condicional

O acesso a sistemas e dados deve ser permitido somente quando houver uma necessidade clara e justificada para o uso, garantindo que os recursos não sejam acessados sem propósito.

- Definição de Escopos

Definir claramente quais informações e recursos são necessários para cada função ou tarefa, evitando acessos desnecessários que podem comprometer a segurança.

- Controle de Acesso Temporário

Implementa mecanismos que permitem acessos temporários a informações ou sistemas, limitando o tempo em que um usuário pode acessar dados sensíveis, conforme a necessidade.

- Monitoramento de Uso

Realizar auditorias e monitoramento contínuo das atividades dos usuários para garantir que o acesso seja utilizado de acordo com as diretrizes condicionais e identificar comportamentos inadequados.

- Treinamento e Conscientização

Promover treinamentos sobre a importância do princípio da Necessidade de Usar, ajudando os colaboradores a compreender quando e como devem acessar informações e recursos.

Registro de Requisição de Acessos:

Garante um controle rigoroso sobre quem pode acessar informações e recursos dentro da organização.

- Documentação das Solicitações

Todas as requisições de acesso devem ser formalmente documentadas, incluindo detalhes como o nome do solicitante, os dados da solicitação, o tipo de acesso exigido e a justificativa para o acesso. Isso fornece um histórico claro e auditável.

- Aprovação Hierárquica

As concessões devem ser submetidas a um processo de aprovação que envolve supervisores ou responsáveis gestores. Isso garante que o acesso seja concedido apenas com base na necessidade e relevância para as funções do colaborador.

- Registro de Concessões e Revogações

É essencial manter registros não apenas das concessões de acesso, mas também das revogações. Isso inclui documentar quando um

acesso é removido e os motivos para tal ação, garantindo uma trilha auditável.

- Auditorias Regulares

Realizar auditorias periódicas nos registros de requisição de acessos para verificar a conformidade com as políticas, e identificar possíveis irregularidades ou acessos não autorizados.

- Treinamento e Conscientização

Promover treinamentos para os colaboradores sobre a importância do registro de requisições de acessos, enfatizando a responsabilidade de cada um em solicitar acessos adequados e reportar quaisquer anomalias.

Identificação e Autenticação:

Garantir que apenas usuários autorizados tenham acesso a sistemas e informações sensíveis, sendo atribuído uma identificação exclusiva (ID) a cada pessoa com acesso a sistemas ou software críticos. Essa prática assegura que cada indivíduo seja unicamente responsável por suas ações.

- Identificação Única

Cada usuário deve possuir um identificador único (como um nome de usuário) que permita rastrear suas atividades dentro dos sistemas. Isso facilita a responsabilização e o monitoramento das ações realizadas.

- Métodos de Autenticação

Implementar mecanismos de autenticação robustos, como senhas complexas, autenticação multifator (MFA) e biometria, para garantir que apenas usuários autorizados possam acessar informações confidenciais.

- Políticas de Senhas

Estabelece diretrizes claras sobre a criação, uso e troca de senhas, incluindo requisitos de complexidade, periodicidade de troca e classificação de compartilhamento.

- Registro de Acesso

Manter registros detalhados de tentativas de acesso, tanto bem-sucedidas quanto malsucedidas. Esses registros são essenciais para auditorias e investigações em caso de incidentes de segurança.

- Treinamento e Conscientização

Promover treinamentos regulares para os colaboradores sobre práticas seguras de identificação e autenticação, enfatizando a importância da proteção das credenciais de acesso.

A implementação de cada item descrito neste tópico está detalhadamente explanada na Norma de Segurança da Informação (NSI).

6. GESTÃO DE IDENTIDADE (IAM)

O gerenciamento de identidade e acesso (IAM) é um conjunto de processos e tecnologias que definem quem é um usuário e quais permissões e privilégios ele possui dentro de um sistema. O controle de acesso deve ser implementado para garantir que apenas usuários autorizados possam acessar dados e sistemas, isso inclui:

- Definição de Papéis e Responsabilidades

Estabelecer claramente quem é responsável pela gestão de identidades e acessos, incluindo a definição de papéis para administradores, usuários e auditores.

- Processos de Identificação e Autenticação

Implemente métodos robustos de identificação e autenticação, como autenticação multifatorial (MFA), para garantir que apenas usuários autorizados tenham acesso a sistemas críticos.

- Controle de Acesso Baseado em Necessidade

Adotar o princípio da Necessidade de Saber, permitindo que os usuários acessem apenas as informações permitidas para suas funções, minimizando os riscos associados a acessos não autorizados.

- Provisionamento e Desprovisionamento

Definir processos claros para o provisionamento (concessão) e desprovisionamento (revogação) de acessos, garantindo que as permissões sejam atualizadas conforme mudanças nas funções ou desligamentos.

- Monitoramento e Auditoria

Estabelecer práticas de monitoramento contínuo das atividades dos usuários e auditorias regulares para verificar a conformidade com as políticas de acesso, identificando comportamentos suspeitos.

- Treinamento e Conscientização

Promover treinamentos regulares sobre práticas seguras de IAM enfatizando a importância da proteção das credenciais e do uso responsável dos acessos.

- Conformidade com Normas e Regulamentações

Garantir que a gestão do IAM esteja conforme as normas relevantes, como a ISO 27001, e as disposições de proteção de dados, assegurando a conformidade legal.

- Classificação e Mapeamento de Recursos

Realizar o mapeamento e classificação dos recursos que necessitam ser protegidos, garantindo que as políticas de acesso sejam aplicadas especificamente.

- Resposta a Incidentes Relacionados ao Acesso

Protocolos para resposta a incidentes relacionados ao acesso não autorizado, incluindo definição de procedimentos para investigação e remediação.
Inclui-se, conforme aplicabilidade, a:

- Autenticação multifator.
- Revisões regulares de acesso.
- Registro de atividades de acesso.

A implementação e procedimentos de cada item descrito neste tópico está detalhadamente explanada na Norma de Segurança da Informação (NSI).

7. SIMULAÇÃO DE ATAQUES

A realização de testes de intrusão é fundamental para avaliar a resiliência dos sistemas e processos de segurança da informação da PayBrokers. Esses testes visam identificar vulnerabilidades e fortalecer as defesas contra possíveis ameaças. As simulações serão conduzidas nos seguintes aspectos:

- Teste de Intrusão em Infraestrutura Física:
  Avaliação da segurança física das instalações, incluindo acesso não autorizado a áreas restritas e proteção de equipamentos críticos.
- Teste de Intrusão em Infraestrutura em Nuvem:
  Análise da segurança dos serviços em nuvem utilizados pela organização, garantindo que as configurações estejam adequadas e que não haja brechas que possam ser exploradas.
- Teste de Intrusão em Aplicações Web:
  Realização de testes em aplicações web utilizando as abordagens Black Box, Grey Box e White Box para identificar vulnerabilidades em diferentes níveis de acesso e conhecimento sobre o sistema.
- Engenharia Social e Phishing:
  Simulações para avaliar a suscetibilidade dos colaboradores a ataques de engenharia social, incluindo tentativas de phishing, para reforçar a conscientização sobre práticas seguras.

Os testes e simulações serão coordenados pelo Gerente de CloudOps, preferencialmente em parceria com empresas especializadas em segurança da informação. Essas parcerias podem incluir tanto empresas contratadas para serviços contínuos quanto consultorias temporárias para avaliações específicas. Após conclusão dos testes, um relatório detalhado será elaborado, contendo as vulnerabilidades identificadas, as recomendações para mitigação e um plano de ação para implementar melhorias na segurança. A execução regular dessas simulações garantirá que a PayBrokers esteja sempre preparada para enfrentar novas ameaças e proteger suas informações críticas. Essa versão é mais clara e estruturada, enfatizando a importância dos testes de intrusão e detalhando os diferentes tipos de simulações realizadas.

A Norma de Segurança da Informação (NSI) detalha como se darão os procedimentos para simulação de ataques, ferramentas e parceiros que a PayBrokers poderá utilizar.

8. IMPLEMENTAÇÃO DE PROCESSOS DE CRIPTOGRAFIA

Esta política estabelece diretrizes de criptografia para a proteção de informações e dados considerados como (sensíveis) de acordo com o negócio da PayBrokers e as legislações vigentes. A criptografia deve ser usada para garantir a confidencialidade, autenticidade e integridade dos dados, sendo regrada pelo time de CloudOps. As medidas de proteção de dados incluem:

- Deveres do Usuário de Rede:

O uso de senhas e chaves de criptografia é estritamente pessoal e intransferível. Em caso de comprometimento do sigilo de senhas ou chaves de acesso, é imperativo notificar imediatamente a equipe de CloudOps da PayBrokers para ações imediatas.

- Usuários devem evitar:

Transmitir anexos de arquivos contendo dados pessoais sem criptografia por e-mail. Utilizar sistemas de proxy, tunelamento, criptografia sem a devida autorização para conexões ou qualquer ferramenta que possibilite acesso não autorizado ao tráfego.

- Requisito de Algoritmo:

As soluções de criptografia aprovadas são padrões reconhecidos internacionalmente, como AES e sua análise e aplicação devem ser analisadas individualmente pelo Gerente de CloudOps. As soluções de criptografia atendem minimamente aos seguintes critérios:

- As soluções de criptografia simétrica utilizam chaves iguais ou superiores a 128 bits;
- As soluções de criptografia assimétrica utilizam chaves iguais ou superiores a 2048 bits;
- Solução de autenticação assimétrica como OpenSSH utilizam chaves iguais ou maiores que 1024 bits.
- Os algoritmos de hash aprovados para uso são SHA3 e SHA2.

- As chaves de criptografia são classificadas e tratadas como "Restritas e confidenciais".

A implementação, procedimentos, ferramentas e quais tipos de dados devem ser criptografados, estão descritos detalhadamente na Norma de Segurança da Informação (NSI).

9. MONITORAMENTO E REPOSTAS A INCIDENTES

Monitoramento

O monitoramento contínuo é um componente crítico para a proteção dos ativos de informação da PayBrokers, cuja premissa é identificar atividades anômalas ou não autorizadas em tempo real, permitindo uma resposta rápida a possíveis incidentes de segurança. Seus princípios são:

- Detecção Proativa

Implementar e manter sistemas robustos para monitorar redes e sistemas, detectando incidentes antes que causem danos significativos. Isso inclui a análise constante de logs e o uso de sistemas de detecção de intrusões (IDS).

- Análise e Investigação

Quando um incidente é detectado, uma investigação detalhada é realizada para compreender a natureza do evento, suas causas e o impacto nas ações da organização. Esta análise é fundamental para desenvolver estratégias de contenção e recuperação.

Respostas a Incidentes

A resposta a incidentes deve ser planejada e estruturada, garantindo que todos os membros da equipe de SI saibam suas responsabilidades durante um evento de segurança. As principais etapas incluem:

- Identificação

A partir da identificação de um incidente, é imperativo que os colaboradores comuniquem imediatamente à equipe de CloudOps sobre quaisquer incidentes de (SI) ou comportamentos suspeitos.

- Canal de Comunicação

A partir da identificação de um incidente ou comportamento que suscite suspeitas deve ser comunicada imediatamente ao CloudOps, utilizando qualquer canal de comunicação disponível. É fundamental que essa comunicação ocorra de forma rápida, a fim de garantir a adoção das ações necessárias.

- Plano de Ação de Respostas a Incidentes

O Plano de Ação de Respostas a Incidentes estabelece diretrizes essenciais para a identificação, contenção, erradicação e recuperação de incidentes de segurança da informação. Este plano apresenta as etapas principais, garantindo que as informações mínimas necessárias estejam claramente definidas.

Preparação

- Treinamento: Realização de treinamentos regulares para todos os colaboradores sobre identificação e relato de incidentes.
- Definição de Papéis: Estabelecimento de uma equipe de resposta a incidentes com funções específicas.

Identificação

- Monitoramento Contínuo: Implementação de sistemas para detectar atividades suspeitas em tempo real.
- Relato de Incidentes: Canal claro para que colaboradores relatem incidentes, com um formulário padrão.

Contenção

- Ações Imediatas: Medidas para limitar o impacto do incidente, como isolar sistemas afetados.

Erradicação

- Análise da Causa Raiz: Identificação da origem do incidente e remoção das ameaças detectadas.

Recuperação

- Restauração de Sistemas: Restauração dos sistemas afetados a partir de backups seguros e monitoramento pós-incidente.

Análise Pós-Incidente

- Relatório Detalhado: Elaboração de um relatório que documenta o incidente, as ações tomadas e as lições aprendidas.
- Revisão do Plano: Atualização do plano com base nas lições aprendidas e melhorias necessárias.

Comunicação

- Interna e Externa: Manutenção da comunicação clara com todos os stakeholders sobre o progresso na resolução do incidente.

Treinamento Contínuo

- Revisão Regular: Revisão e atualização do plano anualmente ou após um incidente significativo, incluindo simulações regulares.

Papeis e responsabilidades:

Função	Responsabilidade
Gerente de CloudOps	**Responsabilidade:** Coordena todas as atividades de resposta a incidentes e garante a comunicação entre as partes envolvidas.
Especialista CloudOps	**Responsabilidade:** Realiza monitoramento contínuo, investiga incidentes, analisa vulnerabilidades, implementa medidas corretivas e participa na elaboração de relatórios pós-incidente.
Analista de Infra IT	**Responsabilidade:** Implementa soluções técnicas para contenção e erradicação de incidentes, de acordo com o parecer e orientação do Analista de CloudOps, além de restaurar sistemas afetados.
Gerente de Governança de TI	**Responsabilidade:** Supervisiona a implementação das políticas de segurança da informação, assegura a conformidade com normas e regulamentações, e fornece diretrizes estratégicas para a gestão de riscos.
Departamento de Gestão e Riscos	**Responsabilidade:** Avalia os riscos associados à segurança da informação, desenvolve estratégias para mitigação, realiza análises de impacto e garante que as políticas estejam alinhadas com os objetivos organizacionais.
Departamento Jurídico	**Responsabilidade:** Recebe relatórios técnicos sobre incidentes, elabora comunicações para entidades reguladoras e garante que todas as ações estejam em conformidade com as leis e regulamentações aplicáveis.

Esta é a forma resumida do Plano de Ação de Respostas a Incidentes. Sua íntegra está descrita de forma detalhada na Norma de Gestão de Riscos de TI (NGR-TI) da PayBrokers.

10. GESTÃO DE VULNERABILIDADES E RISCOS

Este item é tratado em maior abrangência na Norma de Gestão de Riscos de TI, assim como a sua implementação, contudo no intuito de garantir que todas as operações de TI estejam em conformidade com as legislações e normas aplicáveis, a PSI direciona os pilares que serão abordados na NGR-TI.

- Avaliação de Vulnerabilidades

É essencial realizar avaliações regulares para identificar vulnerabilidades em sistemas, redes e processos de organização. Isso inclui a análise de potenciais ameaças, como ataques cibernéticos, malware e engenharia social.

- Gestão de Riscos

A PSI inclui um processo sistemático para avaliação e gestão de riscos, considerando a probabilidade de ocorrência e o impacto potencial das vulnerabilidades identificadas. Essa abordagem permite priorizar ações corretivas e alocar recursos específicos.

- Mitigação de Riscos

Com base nas avaliações realizadas, devem ser adotadas medidas de mitigação para reduzir os riscos a níveis aceitáveis. Isso pode envolver a aplicação de controles técnicos, como firewalls e sistemas de detecção de intrusões, bem como práticas administrativas, como treinamentos regulares para os colaboradores.

- Aplicação sistêmica de patches e correções

A aplicação de patches e correções é uma prática essencial para manter a segurança dos sistemas e reduzir a exposição a vulnerabilidades. Esse processo garante que todos os sistemas da organização estejam atualizados contra ameaças conhecidas, minimizando riscos de exploração.

- Monitoramento Contínuo

A vigilância constante é crucial para identificar novas vulnerabilidades e avaliar a eficácia das medidas inovadoras. Ferramentas de monitoramento devem ser utilizadas para detectar atividades suspeitas em tempo real.

- Contenção

Implementação imediata de medidas para limitar o impacto do incidente, evitando sua propagação.

- Erradicação

Remoção da causa raiz do incidente, garantindo que a vulnerabilidade não persista.

- Recuperação

Restauração dos sistemas afetados ao seu estado normal de operação, acompanhada por avaliações para prevenir recorrências.

- Refinamento

Após a resolução do incidente, a equipe deve analisar o que aconteceu e identificar melhorias para o processo.

- Cultura de Segurança

Fomentar uma cultura organizacional que valorize a segurança da informação é vital. Todos os colaboradores devem ser incentivados a reportar vulnerabilidades e participar ativamente na proteção dos ativos da empresa.

11. REGRAS DE USO

Este tópico estabelece diretrizes claras para o acesso aos recursos e informações da PayBrokers garantindo a utilização correta dos recursos de TI. A observância e cumprimento dessas regras são fundamentais para proteger a organização contra riscos

e ameaças. A implementação desse tema está descrita na NSI (Norma de Segurança da Informação).

Uso Adequado dos Recursos

- Finalidade Profissional

Os recursos tecnológicos disponibilizados pela PayBrokers aos seus colabores incluindo computadores, celulares, tablets ou quaisquer outros recursos/equipamentos, devem ser utilizados exclusivamente para fins profissionais. Terceiros e prestadores de serviços deverão ser informados sobre a utilização desses recursos.

- Parceiros de negócios

Parceiros de negócios da PayBrokers que utilizam os aplicativos/softwares fornecidos pela empresa, devem estar cientes do uso correto desses recursos.

- Utilização de Senhas

As senhas de acesso aos sistemas da PayBrokers deverão ser criadas a partir de requisitos de segurança sendo, no mínimo 8 caracteres com o uso de letras maiúsculas e minúsculas assim como caracteres especiais. As senhas serão substituídas periodicamente em um intervalo de 90 dias.

Uso de Dispositivos e Internet

- Dispositivos Permitidos

É permitido o uso apenas de equipamentos fornecidos pela PayBrokers, devidamente configurados pela equipe de Infra IT. Caso haja necessidade de uso de equipamento pessoal por qualquer motivo, essa autorização deverá ser solicitada através de chamado efetuado na plataforma GLPI. A solicitação será avaliada junto ao gestor/diretor direto do colaborador, e avaliado pelo gerente de Infra IT.

- Uso Responsável da Internet

É vedado o uso de sites inadequados ou potencialmente perigosos através dos recursos fornecidos pela empresa como: rede wi-fi, rede física, vpn, computadores, notebooks, celulares corporativos ou qualquer outro recurso tecnológico fornecido pela PayBrokers. A não observância destas regras será captada por monitoramento e poderá ocasionar sanções administrativas.

Compartilhamento Seguro

- Compartilhamento seguro

O uso de informações deve seguir nosso conjunto de ferramentas corporativas, sobre as quais temos domínio e monitoramento. Caso haja demanda para trâmite de informações críticas e/ou sigilosas (como credenciais bancárias, por exemplo), deve-se tratar o caso com a excepcionalidade devida, com análise final do gerente de CloudOps e apreciação/aprovação do CTO através da abertura de chamado pelo portal GLPI.

12. ESTABELECIMENTO DE PROCESSOS

Estabelecer e documentar os processos de segurança da informação mantendo-os atualizados como: inventários, riscos e vulnerabilidades, avaliação e mitigação de riscos e resposta a incidentes.

Definição de Processos

- Documentação Padronizada

Políticas e Normas deverão seguir o padrão estabelecido conforme o documento de interno intitulado (Regras para Criação de Políticas e Normas) descrevendo cada processo, incluindo responsabilidades e etapas a serem seguidas.

- Aprovação e Revisão

Garantir que todos os processos sejam aprovados pela alta administração e revisados anualmente para manter sua relevância.

- Treinamento

Implementar treinamentos para todos os colaboradores sobre os processos estabelecidos, garantindo que saibam como aplicá-los.

- Integração

Os processos de segurança da informação estarão alinhados com outras políticas e normas de TI.

13. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação é o processo de retenção de níveis de sensibilidade a conjuntos de dados, considerando fatores como valor, confidencialidade, integridade e disponibilidade. Essa prática é fundamental para garantir que as informações sejam tratadas e protegidas, protegidas. Esta PSI direciona os pilares da Classificação da Informação, contudo este tema será desdobrado mais amplamente na Política de Governança de Dados (PDG) e na norma de Governança de Dados (NGD).

Níveis de Classificação

As informações na organização são segmentadas em níveis de classificação específicas, conforme a criticidade e o acesso permitido, incluindo:

- Dados Públicos

Informações disponíveis para acesso irrestrito, podendo ser visualizadas por qualquer indivíduo sem necessidade de autenticação ou autorização específica.

- Dados Internos

Informações destinadas exclusivamente ao uso interno da organização. Esse nível de classificação limita o compartilhamento externo e exige autorização formal para divulgação fora do ambiente corporativo.

- Dados Confidenciais

Informações de caráter sensível, que requerem medidas de proteção robustas. O acesso a esses dados é restrito a indivíduos com permissões específicas e deve seguir diretrizes de controle rigorosas para prevenir exposição indevida.

- Dados Restritos

Dados com alto grau de sensibilidade e criticidade, acessíveis apenas a um grupo extremamente limitado dentro da organização. Esse nível de classificação impõe os controles de acesso mais rígidos, assegurando que apenas indivíduos essenciais tenham visibilidade sobre essas informações.

Fatores motivadores à Classificação da Informação

- Identificação de Dados Sensíveis

Permite à organização identificar quais dados são críticos e precisam de proteção especial.

- Aplicação de Controles de Acesso

Facilita a implementação de políticas de controle de acesso, garantindo que apenas usuários autorizados possam acessar informações sensíveis.

- Conformidade Legal

Ajuda a atender requisitos legais e regulatórios, como os estabelecidos pela LGPD (Lei Geral de Proteção de Dados).

- Implementação da Classificação

Para implementar uma estratégia eficaz de classificação da informação, as organizações devem seguir algumas etapas.

- Mapeamento de Dados

identificar e catalogar todos os dados armazenados na organização.

- Definição de Políticas

Estabelecer políticas claras sobre como os dados devem ser classificados e protegidos.

- Treinamento e Conscientização

Educar os colaboradores sobre a importância da classificação e como aplicar as políticas definidas,

14. PROTEÇÃO DE DADOS

Este item será abordado em maior profundidade na Política de Governança de Dados PGD e na norma de governança de dados NGD.

A proteção de dados é um processo que engloba um conjunto de práticas e políticas destinadas a garantir a segurança, integridade e privacidade das informações pessoais e sensíveis sob a responsabilidade da PayBrokers.

Sua execução é fundamental para:

- **Garantir a Privacidade**
  Protege as informações pessoais dos colaboradores, clientes e parceiros.
- **Conformidade Legal**
  Atende às exigências da legislação vigente, como a Lei Geral de Proteção de Dados (LGPD).
- **Manter a Confiança**
  Fortalecer a relação com clientes e partes interessadas por meio de práticas transparentes.
- **Mitigar Riscos**
  Reduzir a probabilidade de vazamentos e incidentes de segurança.

15. CONFORMIDADE E REGULAMENTAÇÕES

Esta PSI deve cumprir todas as leis aplicáveis, como a Lei Geral de Proteção de Dados (LGPD), que regula o tratamento de dados pessoais.

- Normas

Adotar normas reconhecidas, como ISO/IEC 27001, 27002 e 27701 para estabelecer controles de segurança da informação.

- Auditorias

Realizar auditorias internas e externas regularmente para verificar a conformidade com a PSI e identificar áreas de melhoria.

- Treinamento

Fornecer treinamento regular aos colaboradores sobre regulamentações e políticas de segurança, garantindo que todos conheçam suas responsabilidades.

- Documentação

Manter registros detalhados de incidentes, avaliações de risco e auditorias para demonstrar a conformidade.

- Responsabilidade Legal

Definir claramente as responsabilidades legais da organização em caso de violação de dados ou não conformidade.

- Atualizações

Revisar o PSI periodicamente para incorporar alterações na legislação e nas normas de segurança.

16. TREINAMENTOS E CONSCIENTIZAÇÃO DE USUÁRIOS

A capacitação contínua dos colaboradores é essencial para garantir a segurança da informação e a conformidade com as normas vigentes, incluindo a Lei Geral de Proteção de Dados (LGPD). Para isso, a PayBrokers implementará as seguintes diretrizes de treinamento e conscientização:

Treinamentos Regulares

- Todos os colaboradores participarão de treinamentos periódicos sobre segurança da informação, que incluirão tópicos como:
- Práticas seguras no tratamento de dados pessoais.
- Identificação e prevenção de ameaças cibernéticas, como phishing e engenharia social.
- Uso adequado de senhas e autenticação multifator (MFA).
- Conformidade com a LGPD e outras regulamentações aplicáveis.

Campanhas de Conscientização

- Serão realizadas campanhas internas para promover a conscientização sobre a importância da segurança da informação. Isso incluirá:
- Materiais informativos, como cartazes e newsletters.
- Workshops interativos que abordem cenários práticos de segurança.

Avaliação de Conhecimento

- Após cada treinamento, avaliações serão aplicadas para medir o entendimento dos colaboradores sobre os conteúdos abordados. Essas avaliações ajudarão a identificar áreas que necessitam de reforço.
- Simulações Práticas:
- Serão realizadas simulações periódicas para treinar os colaboradores na identificação e resposta a incidentes de segurança, como tentativas de phishing. Isso permitirá que os colaboradores pratiquem suas habilidades em um ambiente controlado.

Feedback Contínuo

- Os colaboradores serão incentivados a fornecer feedback sobre os treinamentos e as práticas de segurança, permitindo melhorias contínuas nas iniciativas de capacitação.

Atualizações Regulares:

- Os materiais utilizados nos treinamentos serão revisados e atualizados regularmente para refletir novas ameaças, mudanças nas regulamentações e melhores práticas em segurança da informação.

Envolvimento da Gestão

- Garantir que líderes e gestores participem dos treinamentos, reforçando a importância da segurança da informação em toda a organização.

Essas iniciativas visam garantir que todos os colaboradores estejam bem-informados e preparados para proteger as informações sensíveis da organização, contribuindo assim para um ambiente seguro e em conformidade com as exigências legais. Esse texto é claro e abrangente, enfatizando a importância dos treinamentos e da

17. DEFINIÇÕES DE PAPÉIS E RESPONSABILIDADES

Pode-se definir os papeis e responsabilidades da seguinte forma:

CTO	**Responsabilidade:** Definir a estratégia tecnológica, orientar o Gerente de Infra Cloud e Infra IT na implementação e operação de projetos e busca por inovações, além de gerenciar orçamentos e investimentos e o estabelecimento de metas.
Gerente de CloudOps & TI	**Responsabilidade:** Liderar equipes de infraestrutura e operações em nuvem, garantir a disponibilidade e a estabilidade da plataforma, a escalabilidade dos sistemas, gerenciar fornecedores e implantar políticas de otimização, segurança e conformidade.
Analista de Infraestrutura	**Responsabilidade:** Manutenção e otimização de servidores, redes e serviços de TI *on-premise*, inventário de ativos de infraestrutura e provisão de acessos, garantindo a estabilidade e o desempenho da infraestrutura corporativa.

Analista de CloudOps	**Responsabilidade: G**erencia e otimiza operações em ambientes de computação em nuvem, incluindo implantação, monitoramento e manutenção de serviços, automatiza processos, implementa práticas de segurança e controla custos, garantindo eficiência e alinhamento com as necessidades do negócio.
Gerente de Governança de TI	**Responsabilidade:** Criação em conjunto desta PSI, garantindo a sua implementação, atualização e revisão e aprovação.

18. DOCUMENTAÇÃO E COMUNICAÇÃO

A documentação e a revisão da Política de Segurança da Informação (PSI) são fundamentais para garantir a eficácia contínua das diretrizes estabelecidas e a conformidade com as normas regulatórias. As seguintes práticas serão adotadas:

Documentação Completa

Todos os procedimentos, normas e diretrizes relacionados à segurança da informação devem ser documentados de forma clara e acessível conforme a diretriz da Política de Governança de TI (PGTI). Isso inclui registros de incidentes, resultados de auditorias, treinamentos realizados e quaisquer alterações na política.

Revisões Periódicas

A Política de Segurança da Informação (PSI) será revisada anualmente, com a vigência iniciando em 1º de janeiro de 2025, após aprovação do Comitê de Governança de TI. Após o primeiro ano, as revisões e atualizações ocorrerão a cada dois anos. No entanto, se surgirem necessidades específicas, alterações poderão ser implementadas a qualquer momento para garantir conformidade com legislações vigentes, mudanças na estrutura organizacional ou em resposta a incidentes relevantes. Essas revisões são essenciais para assegurar que a política permaneça atualizada, eficaz e alinhada às melhores práticas de segurança da informação.

Responsabilidade pela Revisão

A responsabilidade pela revisão da PSI ficará a cargo da Gerência de Governança de TI, que deverá envolver as partes interessadas relevantes na avaliação da política. Isso inclui feedback de colaboradores e o gerente de infra IT & CloudOps.

Relatórios Anuais

Serão elaborados relatórios anuais sobre a implementação da PSI, incluindo uma análise dos incidentes de segurança, ações corretivas tomadas e recomendações para melhorias. Esses relatórios serão apresentados à alta administração para revisão e discussão.

Feedback Contínuo

O feedback dos colaboradores sobre a eficácia da política será incentivado, permitindo ajustes contínuos e melhorias nas práticas de segurança. Mecanismos para coleta de feedback serão estabelecidos, como pesquisas internas e reuniões periódicas.

Atualizações Regulares

A documentação será atualizada sempre que novas ameaças forem identificadas ou quando melhores práticas forem estabelecidas no setor. Isso garantirá que a PSI esteja sempre alinhada com as necessidades da organização e as exigências do ambiente regulatório.

Essas diretrizes visam assegurar que a Política de Segurança da Informação não apenas atenda às exigências legais, mas também promova uma cultura organizacional de segurança e responsabilidade em relação à proteção das informações.

19. GLOSSÁRIO

- AUTENTICAÇÃO MULTIFATOR (MFA) – Método de segurança que requer mais de uma forma de verificação para conceder acesso a sistemas ou informações, aumentando a proteção contra acessos não autorizados.
- BLACK BOX - Os testadores não têm conhecimento prévio do sistema, simulando um ataque externo sem informações privilegiadas.
- CLASSIFICAÇÃO DA INFORMAÇÃO – Processo de categorizar dados com base em sua sensibilidade e importância, determinando o nível adequado de proteção necessário.
- CRIPTOGRAFIA – Técnica de proteção de dados que utiliza algoritmos para transformar informações em um formato ilegível para usuários não autorizados, assegurando a confidencialidade.
- ENGENHARIA SOCIAL - Este teste avalia a capacidade da organização em detectar e responder a ataques como phishing.
- GRAY BOX - Combina elementos dos dois anteriores; os testadores têm algum conhecimento do sistema, mas não total acesso.
- GTI – Governança de Tecnologia da Informação.
- IAM – Conjunto de processos e tecnologias que definem e gerenciam quem é um usuário e quais permissões e privilégios ele possui dentro de um sistema.
- LGPD – Lei Geral de Proteção de Dados, é uma legislação brasileira que estabelece diretrizes para a coleta, uso, tratamento, armazenamento e compartilhamento de dados pessoais.
- NCSEC – Norma de Cibersegurança que estabelece requisitos mínimos para a segurança cibernética dentro da organização.
- NGD – Norma de Governança de Dados, conjunto de diretrizes e práticas que asseguram a integridade, segurança e uso adequado dos dados, garantindo sua gestão eficaz em conformidade com normas e regulamentações, como a Lei Geral de Proteção de Dados (LGPD).
- NGR-TI – Norma de Gestão de Riscos de TI, conjunto de diretrizes e práticas que orientam a identificação, avaliação e mitigação dos riscos associados à tecnologia da informação na empresa.
- NSI – Norma de Segurança da Informação, conjunto de diretrizes que
- PROTEÇÃO DE DADOS – Conjunto de práticas destinadas a garantir a segurança e privacidade das informações pessoais e sensíveis contra acesso não autorizado, uso indevido ou divulgação.
- PROXY – servidor intermediário que atua como um gateway entre um usuário e a internet.
- REGRAS DE USO – Diretrizes que definem como os recursos tecnológicos devem ser utilizados pelos colaboradores, promovendo práticas seguras e responsáveis.
- SI – Segurança da Informação.
- TESTE DE INTRUSÃO – Também conhecido como Pen Test, é uma avaliação de segurança cibernética que simula ataques reais para identificar e explorar vulnerabilidades em sistemas.
- TUNELAMENTO – Técnica utilizada em redes de computadores que permite encapsular pacotes de dados dentro de outros pacotes, criando um "túnel" seguro entre dois pontos na rede
- WHITE BOX - Os testadores têm acesso total às informações do sistema, incluindo código-fonte e arquitetura.

20. LINKS DE REFERÊNCIA

Lei nº 12.965 de 23 de abril de 2014 – Marco Civil da Internet;
Lei nº 13.709 de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD);
Portaria SPA/MF nº 722/2024
Resolução BCB n° 85 de 08/04/2021