Política de Segurança da Informação

2023

Folha de Controle

Informações Gerais

Título	Político de Segurança da Informação
Código de referência e nº da versão	SI – POL - 104
Status	
Aprovador	Kleber Tolezani
Data de Aprovação	17/07/2023
Publicidade	
Área Proprietária da Política	Segurança da Informação
Políticas e outros documentos relacionados	
Palavras-chave	

Histórico de Versões

Versão	Motivo	Data	Autor
1.0	Elaboração do documento	10/01/2022	Equipe técnica
1.1	Revisão do documento	14/12/2022	Equipe técnica
1.2	Mesa limpa e violação	14/04/2023	Equipe técnica
1.3	Software não autorizado	21/04/2023	Equipe técnica
1.4	Controle de ativos e antivírus	10/07/2023	Equipe técnica

SUMÁRIO

1. INTRODUÇÃO

O objetivo da Política de Segurança da Informação é estabelecer diretrizes de alto nível abrangendo crenças, metas e objetivos de toda a empresa projetados para atender todos os requisitos de segurança da informação exigidos pelas leis aplicáveis, regulamentos e padrões da indústria.

As diretivas da Política são projetadas para fornecer uma visão geral de como a Entrepay mantém um ambiente que seja controlado, consistente, seguro e projetado para aumentar a produtividade dos membros da Entrepay e parceiros.

1.1. Ciclo de vida

Esta Política é projetada para:

● Proteger a segurança e a confidencialidade dos ativos de informações da Entrepay;

● Proteger contra quaisquer ameaças ou perigos antecipados à segurança ou integridade de tais ativos de informação;

● Proteger contra qualquer acesso não autorizado ou uso de ativos de informação. O acesso não autorizado pode resultar em dano substancial ou inconveniência a qualquer cliente, titular dos dados ou à empresa;

● Gerenciar adequadamente os riscos identificáveis relacionados aos ativos de informações da Entrepay;

● Responder adequadamente e minimizar os riscos relacionados a qualquer Incidente de Segurança da Informação;

● Atender aos requisitos regulatórios e contratuais com relação à Segurança da Informação;

● Conscientizar todos os membros da equipe e contratados da Entrepay sobre suas obrigações e responsabilidades com respeito à Segurança da Informação;

● Estabelecer protocolos projetados para proteger a Entrepay e seus ativos de informação, incluindo informações, software, hardware e equipamentos de infraestrutura de rede.

Esta política se aplica ao tratamento por todos os membros da equipe da Entrepay, contratados, terceiros e fornecedores com relação aos seus ativos de informação, incluindo qualquer informação, hardware, equipamento ou dispositivo usado para armazenar, processar ou comunicar tais informações em todos os estágios e processos ao longo do ciclo de vida da informação,

Incluindo:

● Criação/Coleção

● Divulgação

● Armazenamento

● Distribuição

● Disposição

● Destruição

2. ESTRUTURA

Este documento está organizado em cinco domínios de segurança da informação:

1. Identificar: Desenvolver o entendimento organizacional para gerenciar riscos para sistemas, dados e capacidades.

2. Proteger: Desenvolver e implementar salvaguardas apropriadas para garantir a entrega de serviços de informação.

3. Detectar: Desenvolver e implementar atividades apropriadas para identificar eventos de Segurança da Informação.

4. Responder: Desenvolver e implementar ações apropriadas em relação aos eventos de Segurança da Informação detectados.

5. Recuperar: Desenvolver e implementar planos apropriados para resiliência em torno de quaisquer recursos ou serviços que podem ser prejudicados devido a eventos de Segurança da Informação.

3. EXPECTATIVAS

A segurança é responsabilidade de todos os membros da equipe e indivíduos envolvidos com a Entrepay. Portanto, os indivíduos com acesso às instalações e ativos de informações do Entrepay devem cumprir os requisitos definidos neste documento de política, bem como em qualquer documentação de padrão(ões) de Segurança da Informação associado(s).

A segurança é uma responsabilidade de trabalho fundamental para todos os membros da equipe e faz parte dos termos e condições de trabalho.

A violação dessas expectativas de segurança, intencional ou não, é motivo para ação disciplinar consistente com a gravidade da violação. Espera-se que todos os membros da equipe relatem casos de outros que não seguem essas expectativas.

4. PRINCÍPIOS

A Entrepay deve proteger seus ativos de informação, infraestrutura e sistemas contra destruição, perda, danos técnicos erros, falsificação, roubo ou uso não autorizado, seja intencional ou acidental.

A Entrepay deve proteger contra ações não autorizadas, incluindo modificação, cópia, acesso ou outras em processamento.

A Entrepay deve fornecer orientação estabelecendo uma política de Segurança da Informação, aprovando funções e responsabilidades e fornecendo coordenação consistente dos esforços de segurança em toda a empresa.

Os seguintes princípios orientadores fundamentais devem sustentar quaisquer políticas, padrões, e procedimentos usados no Entrepay:

Princípio 1. A Entrepay utiliza um processo baseado em padrões de mercado (ISO 27001) para identificar, avaliar e tratar informações de segurança aplicáveis aos ambientes Entrepay.

Princípio 2. A informação é um ativo comercial crítico e deve ser protegida em relação à sua importância e valor.

Princípio 3. Os controles são necessários para proteger a confidencialidade, integridade e disponibilidade das informações bens.

Princípio 4. A Entrepay investe em controles comprovados com base no ciclo de vida, avaliação de custo-benefício e risco análise. O objetivo não é necessariamente eliminar os riscos, mas minimizá-los da forma mais custo-benefício, compensando o custo dos controles contra a redução antecipada de perdas devido a evitar ou mitigar Incidentes de segurança.

Princípio 5. A segurança da informação é uma parte inerente da arquitetura de informações da Entrepay e processos operacionais e de gestão. Todos os membros da equipe são responsáveis pelas informações Segurança.

Princípio 6. A segurança da informação é um elemento central da governança corporativa da Entrepay.

Princípio 7. A segurança da informação é um facilitador de negócios que permite que a Entrepay entre com mais confiança em relações comerciais, mercados e situações com risco aceitável.

Princípio 8. A liderança do segmento tem a responsabilidade de garantir que suas áreas permaneçam em conformidade com a Política de Segurança de Informação da Entrepay.

5. REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação da Entrepay é avaliada pelo menos anualmente, e ajustado, conforme apropriado, considerando mudanças nos requisitos de negócios, tecnologia e ameaças.

As mudanças na política de Segurança da Informação Entrepay são revisadas e aprovadas anualmente.

A Política de Segurança da Informação é divulgada e publicada.

6. IMPLEMENTAÇÃO DE CONTROLES

6.1. IDENTIFICAR

Gestão de ativos

Fornecer dados valiosos para as equipes de segurança responsáveis por tecnologias defensivas e resposta a Incidentes, o estado esperado de ativos físicos e lógicos associados a informações e instalações de processamento de informações devem ser identificados e esses dados armazenados em um inventário de ativos mantido. Os recursos de computação devem ser contabilizados através de seus ciclos de vida, por exemplo, criação, acesso, responsabilidade, backup, armazenamento, realocação e descarte. Inventários precisos e detalhados são essenciais para proteger esses ativos de informação, detectando perda ou uso indevido e respondendo a possíveis incidentes. Membros da equipe autorizados para levar dispositivos e sistemas físicos de uma instalação da Entrepay são responsáveis por proteger tais ativos.

A rede Entrepay deve ser identificada e os dados armazenados nela dentro de um inventário de ativos de software mantido.

Cada Unidade de Negócios é responsável por manter um inventário de ativos de software que lista todos os aplicativos aprovados junto com seus elementos de dados necessários. O software deve ser contabilizado durante todo o seu ciclo de vida. Isso inclui a criação, acesso, propriedade, backup, armazenamento, realocação e descarte. Os dados desses sistemas de inventário são usados por Segurança da Informação para fins de defesa em profundidade, auditoria, conformidade e resposta a Incidentes.

Os sistemas de informação são frequentemente revisados em auditorias de conformidade. Também são informações importantes para resposta a incidentes, já que um comprometimento de sistema externo pode ameaçar os ativos da Entrepay.

A Entrepay deve empregar medidas para garantir que as informações, independentemente do meio (eletrônico ou papel), sejam classificados de acordo

com sua sensibilidade e o impacto potencial para os negócios de divulgação inadequada ou uso indevido.

A Entrepay deve garantir que aqueles com acesso aos Ativos de Informação protejam tais Ativos de Informação, física e logicamente, de qualquer alteração, roubo, destruição, uso ou acesso ilegal ou não autorizado, ou outros perda. A Entrepay deve definir papéis e responsabilidades com separação apropriada de deveres para apoiar o Programa.

Os fornecedores de produtos e/ou serviços representam um risco para os sistemas e dados da Entrepay. Para mitigar e/ou reduzir esse risco, a Entrepay exige que seus contratos com fornecedores incluam cláusulas que tratem de qualquer Riscos de Segurança da Informação associados à Gestão da Informação e aos serviços de comunicação. Para garantir esses requisitos são atendidos, à medida que os serviços são entregues e as necessidades de negócios mudam, a Entrepay monitora e audita a prestação de serviços do fornecedor.

O setor da indústria da Entrepay é regulamentado. Como tal, a Entrepay é obrigada a elaborar estratégias de proteção que estejam alinhados e que priorizem ações com base em leis federais, ordens executivas, diretivas, políticas, regulamentos e documentos de orientação. Assim, como a Entrepay se envolve no desenvolvimento, documentação, e atualização da infraestrutura crítica, questões de Segurança da Informação relacionadas a sistemas e recursos-chave devem ser identificados dentro dos processos de design e implementação, procedimentos operacionais e tecnologias específicas planos de recuperação de desastres e continuidade de negócios.

A Entrepay deve participar de organizações específicas do setor para se manter informado sobre os desenvolvimentos atuais em Segurança da Informação para o setor industrial, tanto sob a perspectiva arquitetônica quanto de gerenciamento de riscos.

A Entrepay deve definir os objetivos de Segurança da Informação de acordo com seus outros objetivos organizacionais, operacionais e prioridades técnicas.

Os serviços de missão crítica devem ser definidos e bem compreendidos pelas equipes que dão suporte ao negócio. Proteção física, práticas operacionais e estruturas organizacionais resilientes devem ser estabelecidas e documentadas para manter a postura de segurança da Entrepay durante as atividades habituais, bem como na recuperação de desastres operações.

A infraestrutura de serviço crítico que transporta dados ou suporta serviços de informação deve ser projetada para resiliência e protegido contra interrupção, interceptação, interferência ou dano de partes externas ou atores internos. Arquitetando resiliência no projeto da infraestrutura crítica da Entrepay é importante para permitir que a Entrepay continuar a fornecer serviços diante de desastres naturais, ataques maliciosos ou acidentes.

A fim de proteger sua infraestrutura e sistemas contra inúmeros eventos, incluindo, entre outros, acessos não autorizados ou destruição acidental, modificação, cópia, acesso, perda e uso, bem como erros técnicos, falsificação e roubo, a Entrepay deve fornecer orientação para essa proteção, estabelecendo uma política de segurança, aprovando funções e responsabilidades e coordenação consistente dos esforços de segurança em toda a empresa, e é divulgada a todos os membros da equipe da empresa e Terceiros relevantes.

Todas as Unidades de Negócios devem auxiliar no cumprimento das responsabilidades de segurança dentro de suas áreas funcionais e são responsáveis por garantir a Confidencialidade, Integridade e Disponibilidade das Informações, em todas as suas formas, dentro de suas áreas funcionais de acordo com as políticas e padrões de segurança estabelecidos.

Os gerentes das unidades de negócios devem entender e empregar técnicas apropriadas de avaliação e análise de riscos para garantir controles apropriados de segurança cibernética estão em vigor em suas áreas de responsabilidade.

A Segurança da Informação deve estabelecer um programa e práticas para a identificação e categorização eficazes de vulnerabilidades associadas aos ativos gerenciados da Entrepay. O programa deve ser baseado em riscos e levar em consideração conta o apetite de risco corporativo, bem como ameaças a sistemas e dados protegidos.

Os dados dos fóruns de compartilhamento de informações e fontes relacionadas são essenciais para a Entrepay manter uma forte segurança postura. Esses dados permitem que a Segurança da Informação aprimore o conhecimento interno sobre práticas de segurança, novas tecnologias, ameaças e vulnerabilidades.

Para apoiar esse esforço, os membros da equipe de Segurança da Informação e Tecnologia da Informação manterão contatos com grupos de interesse especiais ou outros fóruns especializados em segurança, feeds de dados e associações profissionais.

As comunicações entre a Entrepay e esses Terceiros devem ser mantidas em sigilo.

As ameaças têm o potencial de prejudicar dados, sistemas e membros da equipe da Entrepay. As ameaças podem ser naturais ou origem humana, acidental ou deliberada, interna ou externa. Para apoiar o programa geral de gerenciamento de riscos, as ameaças devem ser identificados e documentados por classe geral e, se mais detalhes estiverem disponíveis, por tipo específico dentro dessa aula.

Para ajudar as equipes de Segurança da Informação a alocar recursos adequadamente, a Entrepay deve avaliar os impacto que pode resultar de potenciais incidentes de segurança. Esta avaliação deve considerar a

Confidencialidade, Integridade e Disponibilidade de todos os ativos dentro de cada cenário de Incidente, bem como a probabilidade do próprio cenário.

Para facilitar as comparações de risco ano a ano, a Entrepay usa uma abordagem de análise de risco baseada em cenários. O nível de análise pode variar com base na criticidade dos ativos, extensão das vulnerabilidades conhecidas, incidentes anteriores correspondentes ao tipo de cenário e a profundidade da análise.

As respostas aos riscos identificados devem ser baseadas nos critérios de avaliação e aceitação de riscos que são usados para garantir que as decisões sejam consistentes e considerar os objetivos organizacionais, as opiniões das partes interessadas, etc. Embora esses critérios são baseados principalmente em níveis aceitáveis de risco, os membros da equipe devem criar uma lista de respostas razoáveis para o risco levando em consideração as consequências potenciais, o nível de confiança nos dados de entrada de critérios e similares preocupações.

A Entrepay deve estabelecer um processo pelo qual os Terceiros são avaliados, classificados e gerenciados.

A Entrepay deve estabelecer uma estrutura e executar um processo que avalia e avalia fornecedores e incluir riscos de segurança cibernética de acordo com a classificação do Terceiro.

A Entrepay deve garantir que os interesses e riscos legais corporativos sejam atendidos na criação e execução de contratos de fornecedores e parceiros.

A Entrepay deve estabelecer uma estrutura e um processo para monitorar os riscos associados a fornecedores e parceiros em conjunto com suas práticas de classificação e risco empresarial.

A Entrepay deve estabelecer uma estrutura e processos para planejar e executar atividades relacionadas à resiliência com fornecedores e/ou parceiros críticos.

6.2. PROTEGER

Controle de acesso

A Entrepay deve estabelecer padrões, processos e procedimentos de gerenciamento de identidade e acesso que concedem acesso de maneira controlada, de acordo com os requisitos comerciais e regulamentares.

A Entrepay deve empregar medidas que restrinjam o acesso físico às instalações ao pessoal de acordo com a finalidade das instalações, conteúdo e necessidade de negócios do pessoal.

A Entrepay deve garantir que o acesso remoto (por exemplo, via VPN) é feito de forma segura, utilizando tecnologias que preservam o Confidencialidade, Integridade e Disponibilidade de suas redes ou Ativos de Informação.

A Entrepay deve estabelecer e comunicar padrões de controle de acesso que facilitem a compreensão e execução dos princípios de menor privilégio e separação de funções.

A integridade das redes da Entrepay deve ser mantida estabelecendo segmentação e acesso apropriados estratégias de controle de acordo com o risco dos sistemas e dados que protege. A infraestrutura de rede deve ser gerenciada e controlada de forma a preservar a confidencialidade, integridade e/ou disponibilidade da rede.

O acesso à rede não deve comprometer a Confidencialidade, Integridade e/ou Disponibilidade dos Ativos de Informação.

A estratégia de segurança de rede da Entrepay utiliza os princípios de Controle de Perímetro, Listas de Controle de Acesso e Segregação.

● O controle de perímetro concentra-se nos serviços normalmente fornecidos por firewalls, e outros controles que restringem o fluxo de dados entre as redes.

● Listas de controle de acesso são usadas para controlar o acesso a recursos específicos com base na fonte de rede e destinos, sistemas que solicitam acesso e os protocolos usados para a conexão de rede.

● A segregação restringe o tráfego de rede entre zonas de segurança ou grupos de dispositivos de rede que são diferenciados por classificação de dados, confiança e/ou níveis de risco, muitas vezes aproveitando os dois primeiros princípios.

A Entrepay deve garantir que todas as identidades de usuário sejam devidamente atribuídas e validadas.

A Entrepay deve estabelecer um programa de conscientização e treinamento que avalie as necessidades e executa um plano para a melhoria contínua da conscientização sobre segurança cibernética em toda a organização. Conhecimento e o treinamento deve começar com as novas contratações, fornecer educação contínua para todos e considerar funções especializadas e responsabilidades por oportunidades específicas de treinamento.

A Entrepay deve garantir que os executivos seniores e o Conselho de Administração sejam mantidos informados/supervisionados e uma compreensão de suas funções e responsabilidades em relação à Confidencialidade, Integridade e Disponibilidade de ativos/recursos de informação.

A Entrepay providenciará treinamento para os membros de sua equipe de forma base necessária para garantir o conhecimento dos tópicos regulamentares e de segurança aplicáveis.

Segurança de dados

Para garantir o nível de proteção compatível com a classificação dos próprios dados, a Entrepay deve estabelecer padrões que definam controles para a proteção de dados em repouso.

Para garantir o nível de proteção compatível com a classificação dos próprios dados, a Entrepay deve estabelecer normas que definam controles para a proteção de dados em trânsito.

A Segurança da Informação da Entrepay deve definir padrões relacionados à segurança cibernética a serem incluídos nos processos e programas que executam a destruição, descarte ou reutilização de equipamentos ou destruição lógica de dados.

Os membros da equipe devem garantir que os ativos de dados sejam protegidos e tratados de acordo com os dados da Entrepay padrões de classificação e manuseio.

A Entrepay deve documentar e implementar medidas para garantir a configuração segura de aplicativos, hospedar sistemas e dispositivos de rede.

Para proteger contra perda de dados devido à corrupção ou perda da fonte primária, os Proprietários da Informação devem garantir que existem processos de backup para todas as suas coletas de dados de acordo com as necessidades e requisitos do sistema e/ou tipo de dados.

A Política de Segurança Física permite que o Programa defina os controles físicos que ajudam a proteger os Ativos de Informação contra acesso não autorizado, roubo, uso indevido, perda e ameaças ambientais e garantir a confidencialidade, integridade e Disponibilidade de Ativos de Informação. A Entrepay deve empregar medidas que restrinjam o acesso a instalações que contenham Ativos de informação apenas para pessoal autorizado que tenha uma necessidade comercial legítima de acesso.

Espera-se que os Proprietários de Informações da Entrepay assegurem que os mecanismos apropriados de sanitização de Informações quando as informações devem ser destruídas.

A Entrepay deve estabelecer medidas para garantir que os controles e medidas de segurança sejam continuamente monitorados e avaliados quanto à eficácia.

A Entrepay deve avaliar e monitorar os controles e riscos de segurança com uma frequência suficiente para apoiar decisões baseadas em risco (diferentes tipos de controles podem exigir diferentes frequências de monitoramento).

Com base nos resultados da avaliação, os controles devem ser aprimorados ou substituídos.

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação.

A Entrepay deve manter um plano de resposta a incidentes de segurança para identificar, mitigar e remediar adequadamente incidentes. A Entrepay deve relatar Incidentes à aplicação da lei ou outras autoridades reguladoras conforme apropriado para as circunstâncias ou quando necessário.

Além disso, a Entrepay deve manter planos de continuidade de negócios para sistemas de segurança críticos.

A Entrepay deve realizar testes periódicos de sua resposta a incidentes de segurança e planos de continuidade de negócios.

A Entrepay deve garantir que o Departamento de Recursos Humanos (RH) trabalhe com a Segurança da Informação para educar os membros da equipe e as partes apropriadas no emprego inicial ou engajamento em relação

às suas responsabilidades para proteger a segurança dos Ativos de Informação da Entrepay.

Antes da contratação, o departamento de RH deve realizar verificações de antecedentes (dentro das restrições das leis locais) sobre potenciais pessoais que pode ter acesso aos ativos de informações da Entrepay.

A Entrepay deve estabelecer medidas para identificar, rastrear e remediar vulnerabilidades encontradas durante a vulnerabilidade varreduras, avaliações e/ou testes de penetração.

Os administradores de sistemas e dispositivos devem garantir que correções, patches e service packs essenciais sejam implantados corretamente aos dispositivos aplicáveis. Onde as vulnerabilidades são descobertas e os patches não estão disponíveis, a reconfiguração e/ou controles de compensação devem ser utilizados.

Manutenção

A Entrepay deve garantir que a manutenção e/ou reparo das redes, sistemas ou aplicativos da Empresa sejam concluídos de acordo com os objetivos de tempo acordados e as atividades usando métodos e ferramentas apropriados/aprovados são rastreados até a conclusão.

Para minimizar o impacto de ameaças externas, a Entrepay, por política, não permite que fornecedores realizem manutenção remota autônoma e atividades de diagnóstico de fora da rede Entrepay.

A Entrepay deve estabelecer requisitos para gerenciamento de log de auditoria, sincronização de tempo e integridade de arquivo monitoramento de seus Ativos de Informação.

A Entrepay permite o uso de dispositivos de mídia removíveis (pendrive, CD, etc.) quando aprovado e usado de acordo com os procedimentos da Entrepay.

O acesso aos Sistemas de Informação da Entrepay deve ser concedido de forma controlada de acordo com requisitos de negócio. Não há direito implícito de acesso. O acesso é estritamente proibido, a menos que explicitamente concedido.

Tráfego dentro e entre os ambientes de rede da Entrepay e tráfego entre a Entrepay e terceiros, devem ser protegidas por meio de separação em nível de rede, restrições aos direitos de acesso e, sempre que possível, criptografia de protocolo.

6.3. DETECTAR

Anomalias e Eventos

A gerência e/ou os patrocinadores do projeto são responsáveis por notificar a Segurança da Informação sobre novos ou existentes sistemas ou aplicativos onde são necessários controles de acesso ou controles de fluxo de dados. A Segurança da Informação ajudará na analisar os fluxos de dados esperados e exigir ou recomendar alterações no projeto ou engenharia para dar suporte Padrões, Procedimentos e melhores práticas com base na Classificação de Dados e outros fatores de risco.

A Entrepay deve garantir que métodos de detecção e resposta a ameaças sejam usados para preservar o Confidencialidade, Integridade e Disponibilidade dos Ativos de Informação da Entrepay contra invasores, uso não autorizado, e ataques cibernéticos.

A Entrepay deve alavancar amplos controles de detecção para identificar e analisar eventos de segurança e ameaças. Esses controles são revisados como parte do processo periódico de avaliação de riscos e como parte de avaliações internas ou processos de auditoria externa.

Monitoramento Contínuo de Segurança

A Entrepay deve garantir que as ferramentas de monitoramento apropriadas sejam instaladas e configuradas adequadamente para registrar a rede atividade que pode impactar a Segurança da Informação, bem como violações de segurança contra dados críticos de produção. Apenas equipe os membros aprovados pela administração podem usar software ou hardware de monitoramento de rede ou tela.

Revisões periódicas do ambiente físico devem ser realizadas pela Segurança da Informação.

A Entrepay deve garantir que as ferramentas de monitoramento apropriadas sejam instaladas e configuradas adequadamente para registrar qualquer usuário atividade que pode impactar a Segurança da Informação, bem como violações de segurança contra dados críticos de produção.

Todos os ativos de informação que são suscetíveis a códigos maliciosos conhecidos devem ter detecção atual mecanismos implementados para detectar e, sempre que possível, impedir que esse código seja introduzido ou executado.

A Segurança da Informação orienta a implementação e monitoramento de sistemas que podem detectar códigos maliciosos e responder aos Incidentes de acordo.

A Entrepay deve implementar medidas para garantir o uso apropriado de dispositivos de computação móvel.

Espera-se que qualquer membro da equipe que trabalhe com terceiros relate violações de segurança conhecidas e suspeitas.

Proprietários de informações que gerenciam provedores de serviços externos são responsáveis por fornecer dados de log para ações que afetam a Segurança da Informação.

A Entrepay deve implementar medidas que irão identificar, rastrear e corrigir as vulnerabilidades encontradas durante as varreduras, avaliações e testes de penetração.

Processos de Detecção

A Entrepay deve garantir que aqueles com acesso aos Ativos de Informação protejam tais Ativos de Informação, física e logicamente, de qualquer alteração, roubo, destruição, uso ou acesso ilegal ou não autorizado, ou outros perda. A Entrepay deve definir papéis e responsabilidades com separação apropriada de deveres para apoiar o Programa.

Os membros da equipe da Entrepay e, quando aplicável, Terceiros devem cumprir as Políticas e quaisquer Padrões e Procedimentos aplicáveis do Programa.

As ferramentas contínuas de monitoramento e detecção devem ser testadas periodicamente para garantir que os mecanismos estejam funcionando efetivamente.

Minimizar o tempo entre detecção e resolução, caso um Incidente de segurança seja suspeito ou percebido por alguma equipe membro, o membro da equipe deve notificar imediatamente a Segurança da Informação. Entrepay Segurança Corporativa

As ferramentas e processos de detecção devem ser continuamente avaliados e aprimorados para garantir novas ameaças, vulnerabilidades, explorações e o uso malicioso é detectado apropriadamente.

6.4. RESPONDER

Planejamento de resposta

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou

acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança para identificar, mitigar e corrigir incidentes relacionados à segurança. A Entrepay deve relatar os incidentes à lei aplicação ou outras autoridades reguladoras, conforme apropriado nas circunstâncias ou quando necessário.

Os Incidentes Operacionais são gerenciados pela função de Gerenciamento de Incidentes.

Comunicações

A Entrepay mantém processos de resposta a Incidentes dentro de padrões de mercado.

Análise

A Entrepay deve empregar medidas para garantir que incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança para detectar adequadamente incidentes de segurança.

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança para analisar incidentes. A Entrepay deve relatar Incidentes à aplicação da lei ou outras autoridades regulatórias, conforme apropriado nas circunstâncias ou quando necessário.

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um

Plano de Resposta a Incidentes de Segurança que forneça orientação na identificação e coleta apropriadas de evidências forenses digitais. A Entrepay deve relatar os incidentes à lei aplicação ou outras autoridades reguladoras, conforme apropriado nas circunstâncias ou quando necessário.

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança que prescreve a designação de um incidente. A Entrepay deve relatar Incidentes à aplicação da lei ou outras autoridades reguladoras conforme apropriado nas circunstâncias ou quando necessário.

Mitigação

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança para conter incidentes. A Entrepay deve relatar Incidentes à aplicação da lei ou outras autoridades regulatórias, conforme apropriado nas circunstâncias ou quando necessário.

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança para identificar, mitigar e remediar Incidentes. A Entrepay deve relatar os Incidentes às autoridades policiais ou outras autoridades reguladoras, conforme apropriado nas circunstâncias ou quando necessário.

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança para identificar, mitigar e remediar Incidentes. A Entrepay deve relatar os Incidentes às autoridades policiais ou outras autoridades reguladoras, conforme apropriado nas circunstâncias ou quando necessário.

Melhorias

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança que avalia, após o incidente, quaisquer atividades de resposta a incidentes. A Entrepay deve relatar os Incidentes às autoridades policiais ou outras autoridades reguladoras, conforme apropriado nas circunstâncias ou quando necessário.

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança para identificar, mitigar e remediar Incidentes. A Entrepay deve relatar os Incidentes às autoridades policiais ou outras autoridades reguladoras, conforme apropriado nas circunstâncias ou quando necessário.

6.5. RECUPERAR

Planejamento de Recuperação

A Entrepay deve empregar medidas para garantir que Incidentes suspeitos de segurança da informação sejam investigados para mitigar qualquer

dano e evitar alteração, destruição, roubo, uso ilegal ou não intencional ou acesso a, ou outros perda de Ativos de Informação. A Entrepay deve manter um Plano de Resposta a Incidentes de Segurança para recuperar de um incidente. A Entrepay deve relatar Incidentes à aplicação da lei ou outras autoridades reguladoras conforme apropriado nas circunstâncias ou quando necessário.

7. MESA LIMPA

Para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente, a Entrepay considera a adoção de uma política de “mesa limpa”, visando o resguardo e informações constante em documentos e/ou impressos durante a ausência do funcionário do seu local e/ou estação de trabalho.

A política deve considerar as classificações de segurança da informação, os riscos correspondentes e os aspectos culturais da organização. Informações deixadas sobre as mesas de trabalho são passíveis de serem danificadas ou destruídas de diversas formas.

O objetivo da política de “mesa limpa” é definir diretrizes que reduzam o risco de uma violação de segurança, fraudes e roubo de informações causadas por documentos que estão sendo deixados sozinhos nas instalações da empresa.

8. ANTIVÍRUS CORPORATIVO

Todo computador da instituição deve possuir instalado a solução de antivírus corporativo.

Todo e qualquer dispositivo conectado ao equipamento que possui o antivírus instalado será rastreado para verificar se existe alguma vulnerabilidade.

Semanalmente o antivírus fará uma varredura em todos os computadores da instituição procurando por vulnerabilidades. Esta varredura é incremental, monitorando os arquivos modificados desde a última varredura.

A equipe responsável pela manutenção da ferramenta tem autonomia para, caso julguem necessário, tomar medidas pró-ativas para combater ou prevenir uma disseminação de vulnerabilidades.

9. UTILIZAÇÃO DE DESKTOPS E NOTEBOOKS

As estações de trabalho devem ser protegidas contra danos ou perdas, bem como de acesso, uso ou exposição indevidos.

As estações de trabalho devem possuir identificações únicas (hostname/ID).

O acesso à estação de trabalho deverá ser encerrado no final do expediente, desligando-se o equipamento, e durante o uso deverá ocorrer o bloqueio das estações de trabalho (desktops ou notebooks) com senha.

Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo à Entrepay só devem ser utilizadas em equipamentos com controles adequados.

Apenas pessoal autorizado da área de Tecnologia da Informação poderá instalar softwares nas estações de trabalho (desktops ou notebooks), utilizando apenas softwares licenciados e homologados. Em caso de dúvidas, deverá consultar a área de Tecnologia da Informação por meio dos canais de suporte.

A área de Tecnologia de Informação deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

9.1. Fornecimento de ativos

O recebimento de ativos de TI ocorre através do preenchimento de “Termo de Responsabilidade”, que possui referência no contrato de trabalho.

9.2. Devolução de ativos

O encerramento de atividades de colaboradores ou terceiros, deve ser formalizado para contemplar a devolução de todos os ativos de propriedade da Entrepay.

10. SOFTWARE NÃO AUTORIZADO

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

Qualquer software não autorizado baixado poderá ser excluído pela TI.

Os colaboradores não poderão, em hipótese alguma, utilizar os recursos da Entrepay para fazer o download ou distribuição de software ou dados pirateados.

A Política de Segurança da Informação da Entrepay proíbe o uso de softwares e dados não licenciados.

11. VIOLAÇÃO DA POLÍTICA

Todo o trabalhador conhecendo qualquer incidente, desvio, falha ou violação das normas relacionadas a Segurança da Informação, deve notificar imediatamente seu superior e a Equipe de Segurança da Informação. Se há mera possibilidade de impacto a Dados Pessoais, sensíveis ou não, deve ser notificado também o DPO, que de acordo com as leis e regulamentações deve ter condições de verificar a obrigação de comunicar incidentes aos titulares dos dados pessoais envolvidos, autoridades competentes e tomar outras providências.

entrepay