BRINKS PAY

POLÍTICA DE GESTÃO DE INCIDENTES

Data: 23/09/2024 – Versão: 01

Nome do Documento:	BP-SEG-POL-0002
Versão:	01
Fase:	Vigente
Classificação:	Confidencial
Área Gestora:	Segurança da Informação
Responsável:	Guilherme do Carmo Jose
Revisor:	Carlos Eduardo Jacinto da Silva
Aprovador:	Fabricio Anselmo da Silva
Aprovador:	Ádrili Sato
Aprovador:	Alexandre Bertoli da Costa
Áreas abrangentes:	Brink’s Pay

Sumário

1. Objetivo

O presente documento, Política de Gestão de Incidentes, foi elaborado com o objetivo de estabelecer diretrizes que permitem à BRINK'S PAY garantir que os incidentes sejam tratados em tempo hábil de modo a minimizar o impacto aos negócios.

2. Abrangência e Aplicação

Os princípios de ética e os valores declarados pela direção da BRINK'S PAY devem reger os relacionamentos e negócios da Companhia, assegurando a correta gestão dos incidentes para mitigar eventuais riscos de paralisação dos serviços em decorrência da ausência de um gerenciamento adequado.

A área de Segurança da Informação é responsável pela elaboração, atualização e aprovação deste documento, bem como acompanhar a resposta aos incidentes, gestão de incidentes, definição de métricas, coleta de evidências e elaboração de plano de ação para tratativa de incidentes.

A Diretoria de Tecnologia da Informação é responsável pelo acompanhamento e gestão, a fim de garantir que o plano de ação seja executado de acordo com o planejado e seus resultados sejam atingidos.

3. Definições

Incidente: é aquele que ameaça ou afeta a confidencialidade, integridade ou disponibilidade de sistemas, equipamentos, infraestrutura e pode causar impactos negativos, operacionais, risco ao negócio ou comprometer a imagem da Companhia.

ITSM: sigla para *Information Technology Service Management*, que significa Gerenciamento de Serviços de TI.

Causa raiz: origem do incidente.

Escalonamento: processo de elevar o nível de acionamento do incidente não resolvido na primeira etapa, para que sejam tratados por equipes especificas.

DPO: sigla para *data protection officer*, que significa encarregado de proteção de dados.

4. Gerenciamento de Incidentes

O gerenciamento de incidentes é um processo que tem como objetivo principal restaurar a operação normal dos serviços afetados em tempo hábil, minimizando os impactos e prejuízos as operações do negócio e garantindo assim o melhor nível de serviço e disponibilidade.

- Os incidentes devem ser analisados e registrados com base nas informações fornecidas no momento em que foram relatados ou identificados;
- Os incidentes devem ser registrados de acordo com a sua severidade e prioridade através da ferramenta ITSM da Companhia;
- Os incidentes devem ser atribuídos as equipes responsáveis pelas tratativas através da ferramenta ITSM;
- Os incidentes deverão ser escalonados para outras equipes sempre que a equipe atual não conseguir solucionar os problemas ou quando não for a equipe responsável pelas tratativas.
- São responsabilidades dos gerentes de TI garantir a plena execução do gerenciamento e tratativas dos incidentes por suas respectivas equipes;

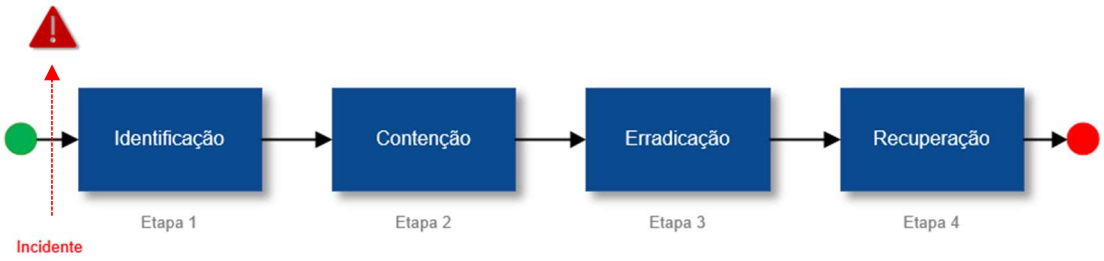
- Os incidentes envolvendo dados pessoais devem ser registrados na ferramenta ITSM e reportados de forma tempestiva ao DPO da Companhia.

Tabela de Classificação de Incidentes

Severidade e Prioridade	Descrição
Prioridade 1 Crítico	São incidentes que causam interrupção completa ou degradação extrema dos sistemas, afetando a prestação de serviços aos clientes, operações de negócios e ou divulgação pública não autorizada de dados.
Prioridade 2 Alto	São incidentes que causam interrupção significativa na prestação dos serviços, afetando clientes e operações de negócios e ou divulgação pública não autorizada de dados.
Prioridade 3 Médio	São incidentes que causam interrupção ou deterioração mínima nos serviços afetando clientes e operações de negócios.
Prioridade 4 Baixo	São incidentes que não causam interrupção ou degradação nos serviços.

As prioridades dos incidentes são definidas com base no impacto e urgência dos incidentes.

5. Etapas do Gerenciamento de Incidentes.



Macrofluxo das etapas do gerenciamento de incidente

Identificação

Na etapa de identificação, os incidentes reportados são analisados e registrados na ferramenta ITSM com base nas informações fornecidas ou obtidas através de análises. Todos os incidentes são classificados de acordo com sua prioridade e severidade.

Contenção

O processo de contenção é realizado o mais rápido possível para minimizar o impacto nos serviços. Ações de maior abrangência são adotadas em caso de incidentes Críticos e Altos para evitar a propagação do incidente e possível paralisação de serviços que possam causar impactos negativos, operacionais ou comprometer a imagem da Companhia. O envolvimento da liderança dos times de TI se faz necessário para tomada de decisões estratégicas dentro do processo de contenção.

Erradicação

Durante o processo de erradicação, os times designados para atuar nas tratativas de cada incidente devem eliminar a causa raiz. Nesta etapa são realizadas análises e testes para garantir a mitigação por completo e evitar reincidência do incidente.

Recuperação

Etapa no qual todos os sistemas, serviços, operações de negócio e/ou dispositivos afetados voltam a operar em sua normalidade. Os times envolvidos devem assegurar que não houve perda de dados relevantes. Nos casos de ocorrência de perda de informações, as áreas de negócio afetadas deverão ser notificadas e a equipe de TI deverá iniciar o processo de recuperação de dados através da restauração de backups. Nesta fase é necessário realizar testes e validação dos dados restaurados para garantir a integridade das informações. Após a conclusão de todas atividades o incidente deve ser encerrado na ferramenta ITSM.

Melhoria Contínua

Este processo tem como objetivo otimizar os procedimentos adotados e melhorar a efetividade da resposta aos incidentes. As áreas envolvidas nas tratativas dos incidentes devem reunir evidências, artefatos, documentos, relatórios para debater sobre todo o processo, desde a identificação até a recuperação e propor melhorias.

6. Histórico de Versionamento

Autor	Motivo Principal	Data	Versão
Carlos Eduardo Jacinto da Silva	Versão inicial	13/06/2022	1.0
Helio Holsback Serejo	Versão inicial	13/06/2022	1.0
Aloysio Regis Gouveia Filho	Revisão Anual	19/04/2023	1.0
Guilherme do Carmo Jose	Revisão Anual	23/09/2024	1.0

7. Revisores

Área	Nome	Cargo
Segurança da Informação	Guilherme do Carmo Jose	Especialista de Segurança da Informação

8. Aprovadores

Área	Nome	Cargo
Segurança da Informação	Carlos Eduardo Jacinto da Silva	Gerente de Segurança da Informação
Tecnologia da Informação	Fabricio Anselmo da Silva	Gerente de sistemas e Projetos
Novos Negócios	Ádrili Sato	Diretora de Desenvolvimento de Negócios
Tecnologia da Informação	Alexandre Bertoli da Costa	Diretor de TI América Latina

Autenticação da assinatura

ENVELOPE

953a3d39-9bc6-4e2e-acc9-a1f5924f9832

Enviado em 04/10/2024 14:16:20 (UTC-3)

DOCUMENTO

f859f6af-4acc-411e-af3a-1a446d71fc3a

BrinksPay - Política de Gestão de Incidentes.pdf.pdf

unico idtech

DOCUMENTO CERTIFICADO

Fotografe o QR Code para validar a autenticidade desse documento

Remetente do documento

BRINKS Segurança e Transporte de Valores LTDA.

60.860.087/0012-51

1º ASSINANTE - Própria

Carlos Eduardo Jacinto da Silva
***.775.698-**

car********rdo@brinks.com.br

Assinado em: 07/10/2024 09:44:03 (UTC-3)
Métodos de autenticação: E-mail + CPF

2º ASSINANTE - Própria

Fabricio Anselmo da Silva
***.337.558-**

fab**********lmo@brinks.com.br

Assinado em: 07/10/2024 10:26:52 (UTC-3)
Métodos de autenticação: E-mail + CPF

3º ASSINANTE - Própria

Alexandre Bertoli da Costa
***.775.818-**

ale**********oli@brinks.com.br

Assinado em: 25/10/2024 10:02:47 (UTC-3)
Métodos de autenticação: E-mail + CPF

4º ASSINANTE - Própria

ADRILI MARIA SATO
***.473.688-**

adr*****ato@brinks.com.br

Assinado em: 29/10/2024 17:13:21 (UTC-3)
Métodos de autenticação: E-mail + CPF