1 INTRODUÇÃO

A determinação por se estabelecer um fluxo padronizado para o processo de gestão de incidentes visa manter esse fluxo dentro das conformidades formalmente estabelecidas nas regras internas, buscando também garantir que todos os envolvidos tenham conhecimento dos requisitos descritos nos documentos aprovados, uniformizando o entendimento, contribuindo para a efetiva padronização de ações e atingimento os resultados esperados;

Vale lembrar, que os passos seguintes à aprovação de um documento do sistema geral de qualidade, para que ele possa realmente se tornar efetivo, é o treinamento de todos os envolvidos direta ou indiretamente na execução das atividades descritas neste documento;

2 OBJETIVO

Este documento tem por objetivo estabelecer os controles para assegurar que os incidentes de segurança de informação e potenciais incidentes sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os ativos de rede e sistemas de informação (tanto físicos como lógicos).

3 ABRANGÊNCIA

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores, parceiros e fornecedores do BESTCRED;

4 DEFINIÇÕES

CÓPIA CONTROLADA

I. Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano.

II. Ativo: É qualquer coisa que tenha valor e precisa ser adequadamente protegido.

III. Evento: é qualquer ocorrência visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa um arquivo compartilhado, um servidor que recebe uma solicitação para uma página da Web, um usuário que envia um e-mail ou um firewall que faz um bloqueio de uma tentativa de conexão, entre outros.

IV. Evento adverso (ou ofensivo): é um evento com consequências negativas. Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou execução de malware que destrói dados, entre outros

V. Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

VI. Informação: É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

VII. Risco: combinação dos impactos advindos da ocorrência de um evento indesejado relacionado à segurança da informação e da probabilidade de sua ocorrência

5 SÍMBOLOS E ABREVIATURAS

CÓPIA CONTROLADA

- Não se aplica no momento

6 PROCEDIMENTO

6.1 Gestão de Incidentes

- A gestão dos incidentes de segurança da informação deve ser realizada com base nas seguintes etapas:

6.1.a IDENTIFICAÇÃO DO INCIDENTE

a.1 Consiste em detectar ou identificar de fato a existência de um incidente de segurança. A Gestão de Crise baseia-se na identificação de incidentes internos ou externos, seja na detecção de alertas provenientes dos sistemas de monitoramento do BESTCRED ou por notificações realizadas por qualquer pessoa relatando ser de seu conhecimento ou mesmo vítima de atividade suspeita ou em desacordo com a Política de Segurança da Informação.

a.2 As notificações internas ou externas devem ser realizadas:

I. Pelo sistema oficial de atendimento do ti: TOMTICKET

II. Em caso de impossibilidade de uso do TOMTICKET, enviar e-mail para o endereço: ti-helpdesk@bestcredsp.com.br

CÓPIA CONTROLADA

a.3 Toda notificação ou denúncia deve ser formalmente registrada. Este registro receberá um número de identificação gerado automaticamente pelo #TomTicket, para que possa ser gerenciado pelos responsáveis da Gestão de Crise.

6.1.b TRIAGEM DO INCIDENTE

b.1 Etapa onde a Gestão de Crise deve realizar a análise inicial do evento, notificação ou denúncia visando a sua confirmação como incidente e classificando a sua relevância sobre as atividades do BESTCRED. Nesta Etapa deve ser identificados os sintomas do evento, suas características e os potenciais danos causados.

b.2 Deve-se preencher o formulário ANEXO 1 - Formulário de Registro do Incidente de Segurança da Informação.

Confirmado que um incidente foi detectado, ele deve ser analisado antes de qualquer ação seja tomada, principalmente para confirmar se é um incidente válido.

b.3 A análise realizada pela Gestão de Crise consiste na coleta, aquisição e análise de dados, informações e demais evidências sobre o incidente para investigar o ativo de rede ou sistema de informação que gerou o incidente detectado ou denunciado.

b.4 Essa investigação passa pela identificação de ativos compreendendo endereços IP, endereços MAC da interface de rede, nomes, switches e portas de acesso, bem como prédio, departamento, salas e usuários. Essas informações devem ser levantadas pelas trilhas de auditoria dos diversos sistemas e serviços disponíveis pelo BESTCRED.

CÓPIA CONTROLADA

b.5 Confirmado o incidente, a Gestão de Crise deve categorizar e priorizar com base: (i) no impacto potencial conforme avaliação de risco em segurança da informação realizada em conjunto com a Classificação de Severidade de Incidente de Segurança (capítulo 12); (ii) no tempo e recursos necessários para recuperar ativos impactados.

b.6 Todo incidente categorizado como sendo de severidade ALTA deve ser notificado imediatamente ao responsável pelo setor de Tecnologia da BESTCRED, que pode realizar a escalação deste incidente e realizar a alocação dos profissionais necessários para resolução do incidente.

b.7 Caso o incidente detectado envolva ou tenha a suspeita de envolver o tratamento não autorizado de dados pessoais, a Gestão de Crise deve notificar imediatamente o Encarregado pelo Tratamento de Dados Pessoais ou Conselho de Proteção de Dados Pessoais, para avaliarem se o incidente informado se trata de uma violação de dados pessoais.

b.8 Confirmado que o incidente é uma violação de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais ou Conselho de Proteção de Dados Pessoais devem ser adicionados na Gestão de Crise para orientar e acompanhar as medidas a serem tomadas.

b.9 Se mais de um incidente estiver ocorrendo ao mesmo tempo, os incidentes devem ser priorizados, pois não haverá o tempo e recursos para atuar simultaneamente.

b.10 Nesta etapa, a Gestão de Crise deve apresentar as ações que serão priorizadas com base na categoria e no impacto do cenário encontrado e realizar as comunicações necessárias.

CÓPIA CONTROLADA

6.1.c MITIGAÇÃO DO INCIDENTE

c.1 Etapa que busca a solução do incidente por meio de um ciclo básico composto pelas seguintes fases: (i) análise dos dados, (ii) pesquisa de solução, (iii) ação proposta ou contenção realizada, (iv) comunicação, (v) solução efetiva e (vi) recuperação do ambiente.

c.2 Devem ser realizados procedimentos iniciais para contenção do incidente visando evitar a sua propagação e posteriormente em restabelecer o ativo, mesmo que com uma solução temporária, até que a solução definitiva seja implementada.

c.3 A Gestão de Crise deve assegurar que as comunicações com Partes Internas e Externas Interessadas ocorram no momento oportuno e estejam coordenadas de acordo com as diretrizes de gestão de crises do BESTCRED. As Partes Interessadas Internas devem ser informadas sobre as ações que precisam ser realizadas durante o estágio de recuperação.

c.4 A Gestão de Crises deve buscar a solução definitiva, ou seja, identificar a causa raiz de um incidente e eliminá-lo para assegurar que o ativo esteja seguro e confiável para que os procedimentos de recuperação sejam iniciados. A Gestão de Crise pode solicitar o envolvimento e suporte das demais Áreas do BESTCRED afetadas para assegurar que os vetores do incidente sejam solucionados.

c.5 A Gestão de Crise deve acompanhar os processos de recuperação dos ativos até o pleno funcionamento.

c.6 Os sistemas relevantes do BESTCRED devem retomar a funcionalidade básica de modo prioritário. As interdependências sistêmicas

CÓPIA CONTROLADA

também devem ser conhecidas, já que alguns sistemas só podem ser recuperados após outros.

c.7 Durante a recuperação, os sistemas devem ser reconstruídos, reinstalados ou restaurados pela Área de Tecnologia da Informação, ou prestador responsável, usando dados de backup e sistemas e patches atualizados, se necessário com apoio da Gestão de Crise. Os sistemas recuperados devem ser testados e monitorados para assegurar que não ocorra novamente o incidente e que os ativos estejam funcionando de modo adequado.

C.1.d RESPOSTA AO INCIDENTE

d.1 Os responsáveis pela Gestão de Crise devem documentar e arquivar as conclusões do tratamento do incidente, descrevendo:

I. o que aconteceu;
II. como o incidente foi detectado, ou seja, foi relatado por pessoal natural ou por um alerta de sistema automatizado;
III. as etapas tomadas pela Equipe de Resposta ao Incidente, a partir da detecção do evento até o estágio de recuperação dos ativos;
IV. o status do incidente à medida que ele se move ao longo do processo de solução;
V. qualquer dado que seja coletado durante o processo de solução que possa ser usado como evidência;
VI. definir a categorização final do incidente;
VII. comentários e sugestões dos responsáveis pela Gestão de Crise.

d.2 Esta documentação deve servir como referência para pós-incidente.

CÓPIA CONTROLADA

d.3 A coleta e preservação de provas, sejam digitais ou não, na etapa de solução do incidente, bem como dados e informações que possibilitaram a identificação do incidente são importantes e devem ser documentadas no registro final do incidente. A coleta de provas deve ser avaliada conforme a necessidade pela Gestão de Crise, devendo acionar a Área jurídica em caso de dúvidas quanto à sua necessidade.

d.4 Quando um incidente for categorizado como severidade ALTA, deve ser realizada a coleta e preservação das provas envolvidas.

C.1.e PÓS INCIDENTE

e.1 A etapa de pós incidente tem o seu início após a resolução e encerramento do incidente, onde serão analisadas pela Gestão de Crise as causas que motivaram a sua ocorrência e quais são as medidas que podem ser tomadas com objetivo que o fato não ocorra novamente.

e.2 O objetivo desta etapa é melhorar os procedimentos realizada na etapa de resposta e aprimorar os ativos para protegê-los de futuros incidentes.

e.3 A Gestão de Crise deve comunicar as partes interessadas do resultado da análise.

e.4 Os incidentes ocorridos devem ser analisados em conjunto com os procedimentos de continuidade de negócio e governança de dados pessoais do BESTCRED. Esta análise visa identificar aprimoramento dos indicadores de probabilidade e consequência dos incidentes previstos e as ocorrências reais de incidentes.

e.5 Com base no relatório e nas informações obtidas durante a solução do incidente, a Gestão de Crise deve criar um plano de ação que incluam os

CÓPIA CONTROLADA

responsáveis, datas de vencimento e entregas para garantir que todas as partes interessadas saibam o que se espera delas. As ações devem ser categorizadas como curto ou longo prazo.

7 RESPONSABILIDADES

Departamento de tecnologia e segurança da informação

I. Auxiliar na análise dos incidentes de segurança por meio da apresentação das trilhas de auditoria dos sistemas sob sua gestão;

II. Caso o tratamento do incidente envolva impactos no ambiente de produção a equipe de gerenciamento de mudanças deve ser comunicada para notificar os gestores e usuários do recurso em questão sobre o ocorrido.

Conselho e encarregado pelo tratamento de dados pessoais

III. Analisar os incidentes de segurança da informação que possivelmente envolvam dados pessoais e dados pessoais sensíveis;

IV. Liderar as salas de crise e indicar processo de gestão de incidentes que envolvam dados pessoais.

V. Conduzir em paralelo a este documento os procedimentos indicados na Norma de Gestão de Incidentes de Violação de Dados Pessoais.

Juridico

VI. Se o incidente tiver consequências legais deve ser estabelecido um contato com os órgãos responsáveis pela apuração e aplicação de penalidades (Agências Reguladoras e/ou Delegacias, se for o caso) para relato dos fatos e a apresentação de indícios relativos ao incidente.

CÓPIA CONTROLADA

Departamento de RH

VII. Para os incidentes de segurança da informação que envolva desvio de conduta do colaborador ou em desacordo com o código de ética, o mesmo será encaminhado para Gestão de Crise, sendo que o gestor da área de recurso humanos poderá se aprofundar na investigação.

Departamento de marketing

VIII. No caso de incidentes que tiverem desdobramentos para fora da Empresa e que envolvam a imprensa ou comunidade externa.

Área de auditoria

IX. Para os incidentes de segurança da informação que envolvam indícios de fraude ou vazamento de informação, o mesmo será encaminhado para área de auditoria, a qual poderá se aprofundar na investigação.

Gestores

X. Garantir e gerenciar o cumprimento desta Norma e demais documentos complementares pelos seus colaboradores.

XI. PENALIDADES

Violações: Qualquer atividade que desrespeite as disposições estabelecidas nesta Norma ou em quaisquer dos documentos complementares do BESTCRED deve ser considerada como uma violação e tratada pelo BESTCRED a fim de apurar as responsabilidades dos envolvidos de acordo com as “Medidas Disciplinares” do BESTCRED visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

CÓPIA CONTROLADA

8 SISTEMAS OFICIAIS DA BESTCRED

Os Sistemas Vitais da BESTCRED, devem estar cobertos por essa política são:

- Rede de Arquivos departamentais, e individuais (Servidor de Rede)
- Rede de Gestão de Acessos (AD - Active Directory)
- Pasta em Nuvem (Sharepoint, Onedrive)
- Sistema de E-Mails e Colaboração (Office 365, Teams)
- Sistemas de Atendimento dos Clientes (CRM)
- Telefonia (Sistema de Gravação de Ligações)

9 ACORDOS DE NÍVEIS DE SERVIÇOS (SLA)

a. De acordo com a severidade do incidente de segurança da informação, o mesmo terá um prazo para o seu tratamento.

CLASSIFICAÇÃO	PRAZO PARA TRATAMENTO
ALTA	Até 8hrs
MÉDIA	Três dias úteis
BAIXA	Cinco dias úteis

Será de **Alta** criticidade quando implicar em:

a. Infração à legislação ou regulamentação brasileira;

b. Infração aos documentos normativos do BESTCRED com consequência para os ativos intangíveis da empresa ou reincidência de um incidente de criticidade Média;

CÓPIA CONTROLADA

c. Imputação de responsabilidades criminais e sanções administrativas ao BESTCRED ou seus colaboradores;

d. Paralisação definitiva, de longa duração ou de larga escala de processos de negócios do BESTCRED;

e. Graves danos aos ativos intangíveis ou ao patrimônio da empresa;

f. Acessos, alterações, reproduções, usos, revelações, compartilhamentos e perdas indevidas ou não autorizadas de informações críticas ou sigilosas de propriedade ou sob a responsabilidade do BESTCRED;

g. Perdas financeiras ou aplicação de multas contratuais de valor elevado;

h. Perda de fornecedores, contratados ou parceiros.

Será de criticidade **Média** quando implicar em:

a. Infração aos documentos normativos do BESTCRED;

b. Comprometimento do relacionamento com fornecedores, contratados ou parceiros;

c. Perdas financeiras de valor mediano ou aplicação de multas contratuais de qualquer valor;

d. Danos sensíveis ou contornáveis aos ativos intangíveis ou ao patrimônio do BESTCRED;

e. Paralisação de duração acima do aceitável ou perda significativa de desempenho de processos de negócios do BESTCRED;

f. Situação que, caso não controlada a tempo, possa levar a paralisação de serviços críticos do BESTCRED.

Será de criticidade **Baixa** quando implicar em:

CÓPIA CONTROLADA

a. Infração ética;

b. Tentativa de acesso indevido às informações, sistemas e ambientes do BESTCRED, que não contenham informações críticas ou sigilosas para a empresa;

c. Perdas financeiras de valor mínimo;

d. Paralisação dentro do período aceitável ou perda inexpressiva de desempenho de processos de negócios do BESTCRED;

e. Situação que, caso não controlada a tempo, possa levar a paralisação de serviços não críticos do BESTCRED ou a ocorrência de prejuízos de forma geral.

Os limites de criticidade previstos pelos itens acima podem ser alterados de acordo com os impactos ao negócio aferidos pelas Áreas de Segurança da Informação e Conselho de Proteção de Dados Pessoais.

10 PENALIDADES

Todos os incidentes implicam em consequências de acordo com o seu nível de criticidade (**Alta**, **Média** e **Baixa**) e a extensão dos danos ocorridos. Conforme sua classificação, as responsabilidades dos colaboradores envolvidos serão apuradas pelo RH e Diretoria, procedimento administrativo interno e poderão alcançar as seguintes medidas:

a. **Alta**: Demissão por justa causa ou rescisão de contrato;

b. **Média**: Suspensão ou advertência;

c. **Baixa**: Advertência verbal para retratação e retificação.

CÓPIA CONTROLADA

11 DISPOSIÇÕES FINAIS

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com a Política, normas e procedimentos aplicáveis pela BESTCRED.

Este plano, bem como os demais documentos que o complementa encontram-se disponíveis na REDE e na INTRANET corporativa.

Este plano entra em vigor na data de sua publicação.

12 ANEXOS

Os seguintes anexos devem ser utilizados conforme necessidade:

ANEXO 1 - Formulário de Registro do Incidente de Segurança da Informação

ANEXO 2 - NOTIFICAÇÃO AO TITULAR

ANEXO 3 - Relatório padrão para ANPD

NATUREZA DA REVISÃO

Revisão	Data	Descrição da Revisão
1	02.05.22	Criação do Documento
2	29.05.23	Atualização e adequação de Formato
3	17.05.24	Atualização da Política

CÓPIA CONTROLADA