POLÍTICA DE GESTÃO E RESPOSTA A INCIDENTES

1. OBJETO

O presente Procedimento de Gestão de Incidentes visa estabelecer os formatos e padrões sobre o processo de gerenciamento de incidentes de Tecnologia da Informação da CREDFRANCO.

2. ABRANGÊNCIA

O Procedimento de Gestão de Incidentes tem abrangência corporativa em toda estrutura da CREDFRANCO.

3. OBJETIVOS

O presente Procedimento visa:

i. O integral e rápido atendimento em situações de incidentes de segurança, sejam estas envolvendo ou não dados pessoais;
ii. Restaurar o serviço à sua situação normal de operação, o mais rápido possível;
iii. Minimizar os impactos negativos nas operações da CREDFRANCO;
iv. Certificar que métodos e procedimentos padronizados sejam utilizados para uma rápida e eficaz resposta aos Incidentes;
v. Melhorar a percepção do uso dos bens/ meios relacionados à Tecnologia da Informação, por meio da utilização de uma abordagem profissional, com a finalidade de rápida resolução do incidente, bem como seu registro e comunicação, quando aplicável.

4. DO MONITORAMENTO DE POSSÍVEIS INCIDENTES

A detecção dos incidentes de segurança é de suma importância para uma rápida e eficaz resposta destes, considerando que sem a identificação de tais eventos, não é possível tratá-los, mitigando a ocorrência de danos maiores.

Ademais, o monitoramento enquadra-se como uma das medidas técnicas e administrativas aptas a proteger os dados pessoais a acessos não autorizados, conforme preconiza o art. 46 da Lei Geral de Proteção de Dados (LGPD).

O monitoramento ocorre através do sistema de chamados GLPI e a plataforma **Gurucul Risk Analytics (UEBA/SIEM)** como ferramenta central para apoio à identificação, correlação, análise e reporte de incidentes de segurança da informação.

5. DO REPORT DOS INCIDENTES

O *report* dos Incidentes pelos usuários poderá ser realizado via Chamado, através da ferramenta GLPI, da qual cada colaborador possui cadastro prévio. As demandas também poderão ser enviadas ao e-mail gsi@credifranco.com.br, o qual é gerenciado pela equipe de Tecnologia da Informação da CREDFRANCO.

O Gurucul atua por meio da coleta contínua de logs e eventos provenientes de diferentes fontes tecnológicas, incluindo, mas não se limitando a: servidores, sistemas operacionais, aplicações, bancos de dados, serviços em nuvem, firewalls, soluções de identidade e demais ativos críticos do ambiente corporativo.

A partir desses dados, a ferramenta aplica mecanismos avançados de **User and Entity Behavior Analytics (UEBA)**, inteligência artificial e correlação de eventos, permitindo a detecção de comportamentos anômalos, atividades suspeitas, desvios de padrão, tentativas de acesso não autorizado, movimentações laterais, uso indevido de credenciais e outras situações que possam caracterizar incidentes de segurança.

Tratando-se de incidentes que possam envolver dados pessoais e sensíveis, deverá haver o *report* ao Encarregado (privacidade@credifranco.com.br), que deverá participar de todas as etapas do incidente, ainda que se conclua que não houve impacto a dados pessoais.

Caso o incidente envolve dados relacionados ao Grupo Santander, o mesmo deve ser reportado pelo canal de comunicação (csirt@santander.com.br).

Utilizamos a Plataforma “RunRun It” no caso de atendimento do Sistema de Gestão de Crédito Consignado (Jarvis) ou equipe de Desenvolvimento e Tecnologia, é uma plataforma de gerenciamento de solicitações de suporte ou mudanças que permite que as organizações gerenciem solicitações de usuários de forma eficiente. É utilizado tanto pelo usuário quanto pelo agente:

Caso o incidente envolva suspeita ou real violação de dados de Clientes vinculados aos Bancos parceiros da CREDFRANCO, esta reportará, através do seu Encarregado, o incidente a estes, conforme canais de comunicação específicos.

6. DA ANÁLISE DOS INCIDENTES

6.1 GLPI

Os Incidentes deverão ser reportados, via Chamado (GLPI), pelos Usuários. Após o recebimento do Chamado, este será classificado pela área de Tecnologia da Informação conforme Grau de Prioridade do Incidente, e será direcionado para o técnico responsável, o qual analisará precisamente o problema.

Como método de resolução do Incidente, o técnico responsável valer-se-á de sua base de conhecimento, chamados e/ou incidentes anteriores e similares, visando sempre a melhor e mais rápida resolução.

Após a resolução do Incidente, o Chamado será encerrado, devendo constar neste explicações da resolução do problema.

6.2 Gurucul

Sempre que um evento atingir os critérios definidos de risco ou severidade, o **Gurucul** gera **alertas de segurança**, os quais são classificados conforme o nível de criticidade (baixo, médio, alto ou crítico). Esses alertas constituem o **registro inicial do incidente**, servindo como base formal para o processo de gestão de incidentes.

Os alertas emitidos pelo Gurucul devem ser analisados pela equipe responsável pela Segurança da Informação, que realizará:

- Validação do alerta;
- Classificação do incidente;
- Registro formal do incidente nos controles internos;
- Abertura de tratativa conforme o plano de resposta a incidentes;
- Definição e execução das ações de contenção, erradicação e recuperação;
- Documentação das evidências e lições aprendidas.

6.1 Classificação do Incidente

Os Incidentes serão tratados conforme seu nível de prioridade e tipo, conforme classificação abaixo:

Grau de Prioridade	Definição da Prioridade	SLA
Muito Baixa	O Incidente não afeta o trabalho do usuário.	24 horas
Baixo	O Incidente não afeta o trabalho do usuário de forma significativa.	16 horas
Médio	O Incidente afeta o usuário de maneira significativa.	12 horas
Alto	O Incidente impossibilita o Usuário de executar suas atividades.	8 horas

Critica	O Incidente afeta todo um setor/ área, empresa, como perigo de Spam, Spoofing, vírus ou malware que podem afetar a Rede.	4 horas

7. DOCUMENTAÇÃO DO INCIDENTE

A documentação do incidente é de suma importância para compreensão do problema e busca de soluções e respostas a eventuais demandas judiciais, conforme o princípio da transparência previsto no art. 6º, VI, da Lei Geral de Proteção de Dados.

A documentação deverá contemplar como o incidente foi descoberto, as ações realizadas e como a evidência do incidente está armazenada. Deverão ser descritas todas as informações do

(i) responsável pelo registro do incidente;

(ii) tipo de incidente;

(iii) ativos afetados;

(iv) detalhes técnicos pertinentes.

Referida documentação é importante não apenas para consolidação das provas, mas para que a CREDFRANCO consiga visualizar e determinar melhorias nos procedimentos de Governança e Compliance.

8. DO RELATÓRIO DE IMPACTO À ANPD

No caso de eventuais questionamentos da Autoridade Nacional de Proteção de Dados (ANPD), deverá ser elaborado Relatório de Impacto conforme o art. 48, §1º da LGPD, contendo, no mínimo:

(i) a descrição da natureza dos dados pessoais afetados;

(ii) as informações sobre os titulares envolvidos;

(iii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

(iv) os riscos relacionados ao incidente;

(v) os motivos da demora, no caso da comunicação não ter sido imediata e

(vi) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

O Relatório deverá conter todas as informações sobre o tratamento de dados pessoais bem como do incidente de segurança, o que permitirá a enumeração de riscos não documentados e a identificação da necessidade de revisão do mapeamento pela empresa.

9. REVISÕES E ATUALIZAÇÕES

Visando promover uma melhor experiência aos Colaboradores, Clientes e Parceiros CREDFRANCO, os termos desta Política poderão ser atualizados ou adaptados, anualmente, conforme o início de cada ano, para que reflitam as nossas práticas, bem como estejam sempre em conformidade com a legislação aplicável.

10. CONSIDERAÇÕES FINAIS

Esta Política deverá ser adotada a partir desta data e todas as alterações estruturais que se fizerem necessárias deverão ser previamente aprovadas pela área de Governança e Compliance.

Histórico de Revisões

Versão	Data		Revisões	Aprovador	Área
	Atualização	Aprovação			
01	-	21/03/2021	Emissão da Política	Everton Alves	Tecnologia da Informação
02	18/05/2022	24/06/2022	Atualização do Layout e Revisão do Conteúdo	Bárbara Fideles/ Gustavo Ferreira	Governança e Compliance/ Tecnologia da Informação
03	17/04/2023	17/04/2023	Revisão do Conteúdo	Bárbara Fideles	Governança e Compliance
04	26/05/2023	26/05/2023	Atualização do item 5 e revisão do Conteúdo	Bárbara Fideles/ Gustavo Ferreira	Governança e Compliance/ Tecnologia da Informação
05	22/12/2023	01/03/2024	Atualização do Item 5 OTRS e atualização do item 9	Gustavo Ferreira / Hemerson Deodato	Tecnologia da Informação
06	29/01/2025	06/03/2025	Atualização do Item 5 de OTRS para RunRun	Fernando Bulhões	Desenvolvimento
07	22/01/2026	29/01/2026	Atualização do Item 4 e 5 ferramenta de monitoramento Gurucul Revisão de conteúdo	Hemerson Deodato Lais Cristina Gustavo Ferreira Gabriel Bortoloto	Tecnologia da Informação