	SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO **POLÍTICA INSTITUCIONAL DE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS**	**N.º DOCUMENTO** POL.GCE_13.00	**Revisão:** 00

ANÁLISE CRÍTICA DO DOCUMENTO			
STATUS: [√] Aprovado [ ] Reprovado		**DEPTO./SETOR:** ADMINISTRATIVO	**DATA EMISSÃO** 31/08/2021
Verificado: Adlson Ferraz Cordeiro DPO – "Data Protection Officer"	**Data:** 31/08/2021	**Aprovado:** Gustavo de Felippo Gori Diretor	**Data:** 31/08/2021
DOCUMENTO			
Política Institucional de Incidentes de Segurança com Dados Pessoais – Grupo EMPAC			

1. INTRODUÇÃO

Esta Política Institucional de Incidentes de Segurança com Dados Pessoais estabelece o procedimento para a gestão de situações após a identificação da ocorrência, ou mera suspeita, de um incidente de segurança da informação que envolva dados de pessoa natural identificada ou identificável ("Dados Pessoais") que são tratados pelo Grupo **EMPAC,** denominada **"CONTROLADORA"** visando o combate dos riscos e a minimização de eventuais efeitos relacionados a incidentes desta natureza. A presente Política Institucional de Incidentes de Segurança com Dados Pessoais foi elaborada de acordo com a Lei nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais – (LGPD).

2. OBJETIVO

Esta presente Política Institucional de Incidentes de Segurança com Dados Pessoais se aplica a todo o Grupo **EMPAC** (Unidade de Tocantins-MG, Escritório de Belo Horizonte-MG e Unidades de Belo Jardim-PE).

O Grupo **EMPAC** adota medidas de segurança, técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

De toda forma, incidentes podem ocorrer e é fundamental que o Grupo **EMPAC** e seus funcionáriosestejam prontos para agir por meio de ações planejadas e organizadas para detecção, análise e reação em casos efetivos ou suspeitos de incidentes com dados pessoais.

Esta Política visa estabelecer diretrizes para o gerenciamento de resposta a incidente com dados pessoais, possibilitando uma resposta rápida e eficaz, nos termos da legislação aplicável.

3. ABRANGÊNCIA

Esta Política Institucional de Incidentes de Segurança com Dados Pessoais é um documento interno, com valor jurídico e aplicabilidade imediata, plena e indistinta. Ela deve ser de conhecimento e aplicação exclusiva ao Encarregado de Proteção de Dados – "DPO", nomeado pelo Representante Legal – "Gustavo de Felippo Gori".

Esta Política se aplica a todos os funcionparios do Grupo **EMPAC** que recebam, acessam ou dequalquer forma tratem Dados Pessoais.

4. DEFINIÇÕES

Os termos de definições importantes ao Sistema de Gestão da Segurança da informação no Grupo **EMPAC,** se baseiam na **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados – "LGPD".**

- **Incidente:** significa qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos Dados Pessoais;
- **Equipe de Gestão de Incidentes:** Equipe responsável pela adoção de medidas de identificação e ações envolvendo qualquer incidente ocorrido com Dados Pessoais tratados pelo Grupo **EMPAC**, composta necessariamente por membros do Comitê de Privacidade. Qualquer comunicação com o Comitê de Privacidade relacinados a Dados Pesoais deverá ser feita através do e-mail compliance@empac.com.br.

5. DIRETRIZES DA RESPOSTA A INCIDENTE DE DADOS PESSOAIS

5.1. Conhecimento de incidente

Os funcionáros deverão, imediatamente após tomarem conhecimento, notificar qualquer suspeita ou ocorrência efetiva de incidente aos membros do Comitê de Privacidade e ao Encarregado de Dados – 'DPO", por meio do **FOR-GCE-160 – Notificação de incidente com dados pessoais.**

5.2. Avaliação interna do incidente

Ao tomar conhecimento de qualquer incidente, o Comitê de Privacidade deverá entrar em contato com o funcionário que fez a notificação para entender a natureza, categoria e quantidade de Titulares afetados, categoria e quantidade dosDados Pessoais afetados, consequências concretas e prováveis, adotando de imediato as medidas previstas nesta Política de forma a limitar o impacto e a recorrência da violação, nos termos desta política.

O Comitê de Privacidade avaliará os riscos oriundos do incidente, em especial qualquer consequência adversa aos Titulares dos Dados Pessoais.

Ao fazer esta avaliação, é importante considerar a seriedade ou a relevância dos danos em potencial causados aos Titulares afetados. A avaliação de risco inevitavelmente exigirá um entendimento:

1. Da natureza dos Dados Pessoais afetados;
2. Informação sobre os Titulares envolvidos;
3. Verificação das medidas técnicas e de segurança utilizadas para proteção dos dados;
4. Os riscos relacionados ao incidente; e
5. As medidas que serão tomadas para reverter ou mitigar os efeitos e danos decorrentes do incidente.

5.2.1. Incidentes devem ser classificados como sendo de Alto Risco, Médio Risco ou Baixo Risco, de acordo com o formulário recebido do(s) funconário(s) que comunicou o incidente conforme estabelecido no **FOR-GCE-160 – Notificação de incidente com dados pessoais.**

- O dano potencial aos Titulares dos Dados Pessoais comprometidos;
- O dano potencial ao Grupo **EMPAC** ou aos seus clientes e fornecedores cujos Dados Pessoais foram comprometidos;
- O potencial de instauração de investigação ou processo administrativo pelas autoridades relevantes contra o Grupo **EMPAC** ou qualquer de seus funcionários, diretores ou executivos;
- O potencial de reclamação ou adoção de medidas extrajudiciais ou judiciais por terceiros contra o Grupo **EMPAC** ou qualquer de seus funcionários, diretores ou executivos; e
- O potencial de dano à reputação do Grupo **EMPAC.**

5.3. Adoção de medidas

Após avaliação interna sobre o incidente, nos termos da seção anterior, caberá ao funcionário apresentar as informações ao Comitê de Privacidade, para que se possa analisar criticamente os fatos de forma a definir os próximos passos que podem incluir, mas não selimitam a, conforme o caso:

1. Comunicação aos funconários, caso o Grupo **EMPAC** seja Operador dos Dados Pessoais. Para tanto, é recomendável a avaliação dos contratos que regulam a relação com os Controladores para adoção dos procedimentos ali previstos, seexistentes;
2. Comunicação à ANPD e aos Titulares dos Dados Pessoais afetados nos casos em que o incidente acarrete risco ou dano relevante aos Titulares, observado o **FOR-GCE-160 – Notificação de incidente com dados pessoais;** e
3. Elaboração de documentação com a avaliação interna do incidente, medidas adotadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas previsto na LGPD.

6. ATENÇÃO – CHECK-LIST – COMUNICAÇÃO AOS TITULARES E ANPD

De forma a definir se o Grupo **EMPAC** deverá comunicar o incidente à ANPD e respectivos Titularesafetados.
O Grupo **EMPAC** deverá avaliar internamente a relevância do risco ou dano do incidente, incluindo, por meio de resposta às seguintes perguntas:

1. Ocorreu um incidente de segurança a Dados Pessoais?
   [ ] Sim – Próxima pergunta;
   [ ] Não – Não é necessário comunicar a ANPD ou Titulares se não houve incidente desegurança relacionado a Dados Pessoais.

2. Existe risco ou dano relevante aos direitos e liberdades individuais dos Titularesafetados em razão do Incidente de segurança?
   [ ] Sim – Comunique à ANPD e ao Titular;
   [ ] Não – A comunicação à ANPD não será necessária se o Grupo **EMPAC** puder demonstrar, de forma irrefutável, que a violação da segurança dos Dados Pessoais não constitui um risco relevante para os direitos e liberdades do Titular dos Dados Pessoais.

Em caso de dúvidas em relação à resposta à pergunta 2 acima, é recomendável a comunicaçãoao Titular e à ANPD.

Para fins de apuração da probabilidade de risco ou dano relevante para os Titulares, o Grupo **EMPAC** deverá considerar, em acréscimo à regulação aplicável, que a probabilidade de risco ou dano relevante para os Titulares será maior sempre que o Incidente envolver, por exemplo, Dados Sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violaçãodo direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma,deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fée as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

6.1. Comunicação à ANPD

Concluída a avaliação em 6. acima e sendo necessária a comunicação à ANPD, oGrupo **EMPAC,** quando na posição de **"CONTROLADOR",** deverá comunicar o incidente através do **Formulário de Comunicação de Incidente de Segurança com Dados Pessoais,** disponível no site: https://www.gov.br/anpd e as informações devem ser claras e concisas.
Embora a responsabilidade e a obrigação pela comunicação à ANPD sejam do **"CONTROLADOR",** caso o Grupo

EMPAC, se encontre em posição de Operador e o Controlador respectivo seja omisso, atrase ou se negue a submeter a comunicação a ANPD, o Grupo **EMPAC,** poderá fazê-la diretamente observadas as disposições contratuais queregulam a relação com o Controlador.
Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente. No entanto, no momento da comunicação preliminar, deverá ser informado à ANPD seserão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las.
A comunicação à ANPD deverá ser feita na maior brevidade possível. Enquanto inexiste regulação sobre o tema, recomenda-se a comunicação em até 05 (cinco) diasúteis contados da data do conhecimento do incidente.

6.2. Comunicação aos titulares dos dados

Concluída a avaliação conforme previto no item 6. acima e sendo necessária a comunicação aos Titulares, o Grupo **EMPAC,** quando na posição de **"CONTROLADOR",** deverá comunicar o incidente aos Titulares em comunicação objetiva e de fácil leitura, devendo conter no mínimo:

a) a descrição da natureza dos Dados Pessoais afetados;
b) as informações sobre os Titulares envolvidos;
c) a indicação das medidas técnicas e de segurança utilizadas para a proteção dosdados;
d) os riscos relacionados ao Incidente; e
e) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitosdo prejuízo.

6.3. Penalidades

O descumprimento das regras e diretrizes impostas nesta Política poderá ser considerado como falta grave, passível de aplicação de medidas disciplinares incluindo advertência e demissão por justa causa.
Para maiores informações, direcionamento de dúvidas e envio de sugestões ao Encarregado de Dados – "DPO", por favor entre em contato por meio do e-mail: dpo@empac.com.br
Denúncias relacionadas à violação efetiva ou suspeita desta Política ou outras políticas internase leis relacionadas à proteção de dados pessoais poderão ser encaminhadas para o Canal de Transparência pelo endereço: https://www.empac.com.br/Canaldetransparencia, sendo preservado o anonimato se assim preferiro denunciante.

7. DIRETRIZES DE GOVERNANÇA

O Encarregado de Dados – "DPO", deve dispor de uma estrutura formalmente constituída de governança.
O Encarregado de Dados – "DPO", tem o papel fundamental de estipular e garantir a aderência às diretrizes da segurança da informação e privacidade de dados, além de auxiliar no estabelecimento de controles de segurança adequados para cada área.

8. PAPÉIS E RESPONSABILIDADES DO ENCARREGADO A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Cada área no Grupo **EMPAC,** tem responsabilidades quando da ocorrência ou mera suspeita de um incidente, conforme descritas a seguir:

8.1. Obrigações de todas as áreas

1. comunicar imediatamente ao Encarregado de Dados – "DPO" sobre a ocorrência ou a mera suspeita de um incidente;
2. cumprir rigorosamente a Política Institucional de Incidentes de Segurança com Dados Pessoais, Manual de conduta e outros regramentos da instituição, contribuindo para a mitigação de riscos; e
3. participar de treinamentos e programas de conscientização para mitigação de incidentes.

8.2. Obrigações do Encarregado de Dados – "DPO"

Entre suas principais responsabilidades, com o apoio dos demais funcionários, destacamos:

1. orientar o Operador (LGPD) e demais funcionários para detectar e corrigir os incidentes;
2. alertar, comunicar e aconselhar os funcionários sobre incidentes emergentes;
3. educar e conscientizar os funcionários sobre a detecção e resposta aos incidentes; e
4. conscientizar o Operador (LGPD) quanto as demais medidas necessárias para prevenir Incidentes e minimizar o impacto de seus efeitos;
5. contatar a Agência Nacional de Proteção de Dados – (ANPD), em caso de incidentes.

8.3. Obrigações de outras áreas

O Operador (LGPD), poderá acionar outros funcionários de outras áreas, dependendo do tipo e da gravidade do incidente.
A Política Institucional de Incidentes de Segurança com Dados Pessoais deverá prever a comunicação ao Comitê de Privacidade, no prazo máximo de 05 (cinco) dias úteis contados da data do conhecimento do incidente, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados.
Os incidentes de segurança com dados pessoais serão imediatamente comunicados pelo Operador e/ou Suboperadores ao "**CONTROLADOR".**

9. DISPOSIÇÕES FINAIS

A presente Política Institucional de Incidentes de Segurança com Dados Pessoais deve ser lida e interpretada sob a égide

das leis brasileiras, no idioma português, em conjunto com outras Normas e Procedimentos aplicáveis e relevantes adotados pelo Grupo **EMPAC.**

Em caso de dúvidas, comentários e/ou sugestões relacionadas a esta Política Institucional de Incidentes de Segurança com Dados Pessoais entre em contato com o Encarregado de Dados do Grupo **EMPAC,** que está à disposição conforme informações a seguir:

DPO – "Encarregado de Dados": Adilson Ferraz Cordeiro
E-mail para contato: dpo@empac.com.br

10. ALTERAÇÕES À ESTA POLÍTICA

O Grupo **EMPAC** reserva-se o direito de alterar a presente Política a qualquer tempo.

As alterações serão idenficiadas por meio de textos sublinhados e esta politica está disponibilizada na rede a todos os funcionários do Grupo **EMPAC.**

Documento	Política Institucional de Incidentes de Segurança com Dados Pessoais
Tipo de Instrumento Normativo	Política Institucional
Categoria do Assunto	Controle e Conformidade
Versão	00/2021
Identificação	POL.GCE_13.00
Elaborado por	Adilson Ferraz Cordeiro
Posição Elaborador	DPO – "Data Protection Offcier"
Categoria do Assunto	Controle e Conformidade
Revisando por	Gustavo de Felippo Gori
Posição do Revisor	Diretor

Esta Política Institucional de Incidentes de Segurança com Dados Pessoais é válida a partir de 31/08/2021.

Fim: Restante do documento propositalmente em branco!