Rodovia PR 412, Km 7, nº 6675, Sala 4, Balneário Leblon. CEP: 83255-000, Pontal do Paraná-PR - Fone: 41-3455-3781 / 3458-2673
E-mail: rimoveis.pontal@gmail.com

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

Data	Descrição
05/01/2022	Implementação
17/01/2023	Atualização

O **Serviço do Registro de Imóveis de Pontal do Paraná** visando proteger e garantir a confidencialidade, integridade e disponibilidade das informações constantes nos sistemas utilizados, elaborou a presente política de segurança a ser observada por todos os profissionais que atuam na serventia.

OBJETIVO

O objetivo da presente política de segurança é prevenir dados e padronizar procedimentos, sendo que no longo prazo, servirá como mecanismo de prevenção de incidentes relacionados às informações.

DIMENSÃO

Os termos constantes na PSI aplicam-se a todos os funcionários, estagiários, prestadores de serviços e a todo e qualquer profissional que possua acesso aos sistemas de informação da serventia.

PRINCÍPIOS

a) CONFIDENCIALIDADE – todas as informações constantes nos sistemas de informação da serventia só podem ser acessadas por pessoas devidamente autorizadas;

b) DISPONIBILIDADE – as informações dos arquivos da serventia estão disponíveis para o correto tratamento a ser realizado pelas pessoas autorizadas;
c) INTEGRIDADE – as informações devem permanecer completas e íntegras, de forma a não serem modificadas ou destruídas de forma acidental.

REQUISITOS

Em busca da uniformização das práticas da serventia, a PSI será comunicada a todos os funcionários, bem como fará parte dos documentos a serem entregues aos futuros profissionais que atuarem na serventia, juntamente com o contrato de trabalho.

A PSI poderá ser alterada sempre que se fizer necessário, havendo fato relevante ou algum evento que motive sua retificação, total ou parcial.

Todos os funcionários devem ser orientados acerca de procedimentos de segurança, bem como correto uso dos equipamentos da serventia, de forma a reduzir o acontecimento de incidentes.

Havendo qualquer incidente de segurança da informação, a serventia está devidamente preparada para repará-lo ou reduzir os possíveis danos sempre que possível. O profissional que deve ser instado a manifestar-se é o encarregado de dados, no âmbito da Lei Geral de Proteção de Dados – LGPD.

A não obediência ao presente plano de segurança de informação acarreta a violação das normas internas e sujeitará o funcionário a responder pelas medidas cabíveis.

CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações constantes na serventia possuem os seguintes níveis de confidencialidade:

a) PÚBLICA – toda informação acessada pelos usuários em geral ou funcionários. Exemplo: informações constantes em murais, redes sociais ou sites.
b) INTERNA – informação interna é aquela que deve ser de conhecimento somente dos agentes internos da serventia (titular e funcionários em geral). Exemplo: portarias internas ou circulares internas.
c) CONFIDENCIAL – é toda informação que pode ser acessada somente a pessoas previamente autorizadas, sendo que a publicidade destas informações pode causar impacto aos envolvidos. Exemplo: conteúdo de testamentos lavrados ou aprovados, conteúdo de mandado referente à adoção;
d) RESTRITA – são informações que podem ser acessadas somente a determinadas pessoas, sendo que a divulgação não autorizada pode comprometer a estratégia organizacional da serventia. Exemplo: folha de pagamento.

RESPONSABILIDADES

São responsabilidades de todos os agentes relacionados à serventia:

- dar cumprimento à presente PSI;
- proteger as informações a que tiverem acesso, impedindo ou reduzindo o risco de perda, modificação ou destruição incidental;
- assegurar que os recursos e informações sejam utilizados somente para o fim específico;
- dar cumprimento a todas as leis e normas que tiverem conhecimento acerca de proteção de dados pessoais;
- não efetuar qualquer comentário que diga respeito às informações restritas, confidenciais ou internas, em ambientes públicos ou com pessoas diversas do ambiente organizacional;
- não compartilhar qualquer informação que tenha acesso em decorrência da função desempenhada na serventia;
- comunicar ao responsável qualquer suspeita ou incidente que tiver conhecimento envolvendo informações.

CORREIO ELETRÔNICO

O correio eletrônico corporativo deve ser usado com base nas diretrizes a seguir.

É vedado aos funcionários da serventia:

- remeter mensagens não requeridas, exceto para uso de atividade da serventia;
- utilizar endereço eletrônico alheio para envio de mensagens, ou assinar em nome de terceiro;
- enviar qualquer informação por e-mail que possa ocasionar qualquer dado à serventia nas esferas cíveis ou criminais;
- enviar qualquer informação não autorizada, imagens, documentos, ou qualquer outro, sem a devida autorização;
- adulterar ou falsificar informações com objetivo de evitar punições;
- deletar informações ou mensagens de cunho corporativo sem a devida autorização;
- enviar mensagens que:
  a) possuam conteúdos de ameaças como por exemplo spam ou vírus;
  b) contenham qualquer arquivo que represente risco à segurança do destinatário;
  c) possua como objetivo obter acesso não autorizado a outro computador;
  d) possua como objetivo interromper serviço por meio de qualquer método ilícito;
  e) possua como objetivo burlar qualquer sistema de segurança;
  f) possua como objetivo assediar, ameaçar, vigiar ou intimar outro usuário;
  g) possua como objeto acessar informações restritas;
  h) possua qualquer conteúdo impróprio ou não relacionado à atividade;

i) possua conteúdos obscenos ou ilegais;
j) possua caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, entre outros da mesma natureza, ainda que não especificados;
k) contenha aspecto de perseguição moral ou preconceituosa relacionada à sexualidade, raça, incapacidade física ou mental, dentre outras na mesma natureza, ainda que não especificadas;
l) possuam fins políticos partidários;
m) possuam materiais protegidos por direitos autorais, sem a devida permissão para compartilhamento.

Todas as mensagens enviadas por correio eletrônico devem conter o nome completo e o departamento do subscritor.

DO USO DA INTERNET

O uso da internet nos equipamentos da serventia deve obedecer aos presentes critérios de segurança. Toda informação acessada, transmitida, recebida ou produzida poderá ser objeto de monitoramento pelo titular da serventia.

Os equipamentos fornecidos são de propriedade da serventia, que poderá, através de titular ou pessoa por ele indicada, se necessário, bloquear acesso a sites que não dizem respeito à atividade desempenhada e estejam colocando em risco o correto funcionamento dos serviços inerentes.

O acesso a redes sociais é restrito às contas da serventia. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Os downloads ou uploads de arquivos devem ser autorizados pelo responsável e possuir relação direta com a atividade desempenhada na serventia, sendo que, em nenhuma hipótese, os computadores da serventia poderão ser utilizados para disseminação de material ou programas pirateados.

O acesso a softwares de compartilhamento não é permitido. Já os programas de mensagens instantâneas poderão ser autorizados pelo titular da serventia, desde que possuam finalidade com a atividade prestada.

IDENTIFICAÇÃO DOS EQUIPAMENTOS

Todos os equipamentos da serventia são devidamente identificados, devendo possuir senha de acesso individual e de conhecimento restrito aos que o utilizam, estando cientes os funcionários que o uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

O usuário responsável pelo equipamento é única e exclusivamente responsável pelo seu uso correto. Assim, todo e qualquer dispositivo só poderá ser compartilhado com autorização do responsável.

Em caso de login compartilhado a responsabilidade é solidária dos que utilizarem da referida identificação, salvo se for possível identificar o autor do dano.

SEGURANÇA DOS EQUIPAMENTOS

As senhas de acesso ao computador e aos sistemas devem possuir caracteres de segurança, variando entre letras, números e caracteres especiais, sempre que possível, devendo ser evitadas senhas evidentes.

É de responsabilidade de cada usuário a memorização de sua própria senha.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio do responsável, ou de quem este determinar.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável.

É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

BACKUP

A serventia deverá possuir método eficaz de forma a garantir o correto backup dos dados, através de agendamento automatizado ou qualquer outra forma que garanta o funcionamento ininterrupto.

DA SEGURANÇA DOS DADOS PESSOAIS

Os agentes de tratamento comprometem-se a adotarem 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.

Ainda, sendo que a autoridade nacional ou qualquer outro órgão fiscalizador da atividade dispor sobre padrões técnicos mínimos para garantir a segurança dos dados pessoais, os agentes de tratamento responsabilizam-se em cumpri-los, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia.

No anexo 01 da presente política consta o plano de respostas a incidentes de segurança a ser aplicado em caso de qualquer incidente com dado pessoal verificado.

DISPOSIÇÕES FINAIS

A presente política de segurança da informação inicia sua vigência na presente data, podendo sofrer alterações sempre que se fizer necessário.

Esta Política de Privacidade e Proteção de Dados será revisada continuamente e pode ser alterada a qualquer tempo, conforme haja necessidade.

Se você ainda possui qualquer questionamento sobre a forma como seus dados pessoais são tratados, pedimos que nos contate em: thaisremorsebolt@gmail.com.br

A/C - THAIS REMOR SEBOLT, Encarregada pelo tratamento de dados pessoais, nomeada em 4/01/2022, nos termos da Portaria RI nº 01/2022.

ANEXO 01

PLANO DE RESPOSTAS A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

INTRODUÇÃO

No âmbito da proteção de dados pessoais, ainda que a organização possua procedimento para o tratamento dos dados, bem como políticas de manipulação, incidentes de dados podem ocorrer a qualquer tempo.

Importante se faz a implantação de um plano de respostas de forma que descreva as ações a serem executadas a partir do momento que se tem conhecimento do incidente de dados pessoais, para o cumprimento dos dispositivos constantes da Lei Geral de Proteção de Dados - Lei n. 13.709/18.

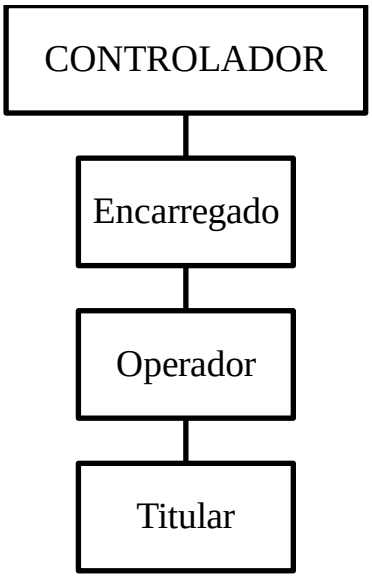
Para o presente plano, elaborou-se as seguintes etapas:

1. Atores
2. Organograma
3. Procedimento
4. Notificação
5. Formulário de triagem
6. Relatório
7. Comunicações
8. Circular

1. ATORES

- Titular - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
- Notificador – agente que identifica o incidente e comunica ao encarregado.
- Encarregado dos dados pessoais – também conhecido como Data Protection Officer (DPO), é o agente responsável em aceitar as reclamações e comunicações, estabelecer o vínculo com a ANPD (Autoridade Nacional de Proteção de Dados), adotar as providências contidas no plano de respostas a incidentes, orientar os demais funcionários com relação aos procedimentos a serem adotados e executar demais tarefas estabelecidas pelo controlador.
- Operador – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- Controlador – agente responsável pelas decisões a serem tomadas referente ao tratamento de dados pessoais.
- ANPD – Autoridade Nacional de Proteção de Dados que deverá ser comunicada caso o incidente possa acarretar riscos ou dano relevante ao titular.

2. ORGANOGRAMA



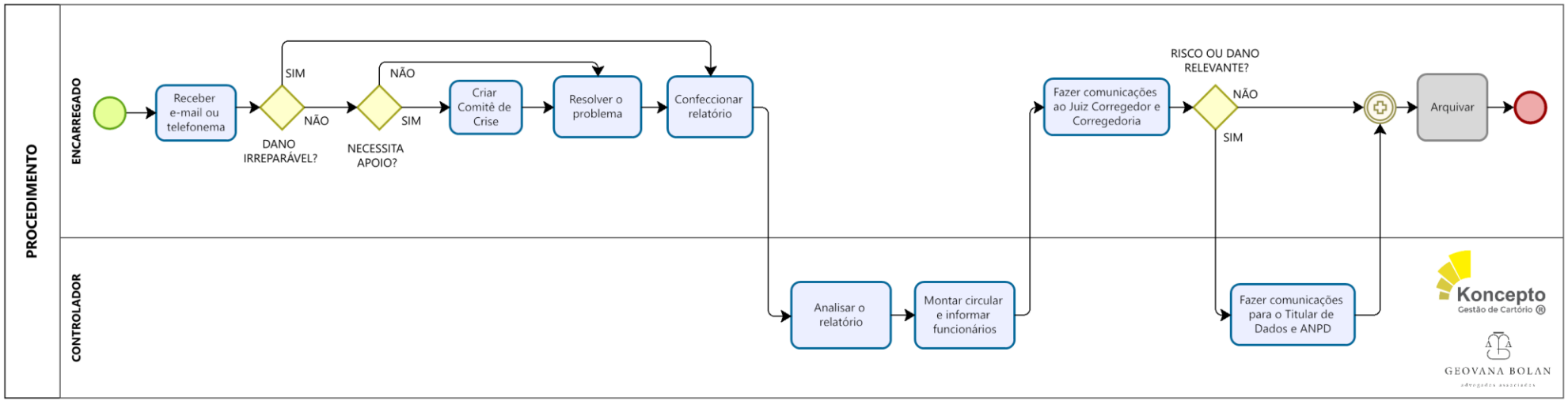
Os agentes que compõem a estrutura organizacional são o controlador, o encarregado, os operadores e os titulares dos dados pessoais.

A necessidade de formação de comitê de crise será analisada a cada caso concreto.

Diante de qualquer incidente de dado pessoal, o agente que tiver conhecimento deverá ser comunicado imediatamente ao encarregado dos dados, o qual será encarregado em aplicar o procedimento referente ao plano de resposta.

3. PROCEDIMENTO

Descrição do procedimento



1. Ao tomar conhecimento de possível incidente de dado pessoal, o notificante deverá notificar o encarregado através do canal de comunicação amplamente divulgado pela serventia (Anexo I).

2. O encarregado efetuará a triagem e classificar o dano como irreparável ou reparável (Anexo II).

3. Na insurgência de dano irreparável, deverá ser confeccionado relatório discriminado acerca do incidente verificado, apontando suas causas e os motivos da falha (Anexo III).

4. Na hipótese de dado reparável, o encarregado deverá apontar a necessidade de criação de comitê para auxílio na resolução do incidente. Após resolução do incidente, deverá ser confeccionado relatório discriminando as causas do incidente e sua resolução (Anexo III).

5. O encarregado enviará relatório ao controlador, o qual elaborará uma circular para os funcionários descrevendo o incidente e os mecanismos para evitar outros da mesma natureza (Anexo V).

6. O encarregado deverá proceder de imediato comunicação ao Juiz Corregedor e à Corregedoria com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos (Anexo IV).

7. Após comunicação ao Juiz Corregedor e à Corregedoria, o encarregado deverá classificar o incidente de acordo com o risco ou dano relevante ao titular do dado.

8. Havendo risco ou dano relevante ao titular do dado, o controlador deverá emitir comunicação à Autoridade Nacional de Proteção de Dados, ao Juiz Corregedor Permanente e à Corregedoria Geral da Justiça, **no prazo máximo de 48 horas úteis**, contados a partir do seu conhecimento, (Anexo IV).

9. Após a emissão dos comunicados, o processo será devidamente arquivado.

ANEXO I - NOTIFICAÇÃO DE INCIDENTE DE DADOS AO ENCARREGADO

Notificante: _____

RG: _____ CPF: _____

Telefone: _____ E-mail: _____

Data da notificação: _____

Data do incidente: _____ Desconhecida ☐

Resumo do incidente: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Pontal do Paraná, _____/_____/_____

_____

NOTIFICANTE

ANEXO II - FORMULÁRIO - TRIAGEM DE INCIDENTE

Data: Clique ou toque aqui para inserir uma data.

Notificador: Clique ou toque aqui para inserir o texto.

Data do incidente: Clique ou toque aqui para inserir uma data. Desconhecida ☐

Objeto do incidente:

☐ Dados pessoais ☐ Dados pessoais sensíveis

Forma de armazenagem dos dados violados:

☐ Meio físico ☐ Meio digital

Risco:

☐Baixo ☐Médio ☐Alto ☐Altíssimo

Tipo do incidente:

☐ Destruição ☐Perda ☐ Alteração ☐Comunicação

☐Outro: _____

Incidente repetitivo:

☐ Sim ☐ Não

Possibilidade de recuperação:

☐ Total ☐ Parcial ☐Sem possibilidade de recuperação

Membros do comitê, se necessário:

Nome: Clique ou toque aqui para inserir o texto.

Contato: Clique ou toque aqui para inserir o texto.

Nome: Clique ou toque aqui para inserir o texto.

Contato: Clique ou toque aqui para inserir o texto.

ANEXO III - RELATÓRIO DE INCIDENTE DE DADOS

Data do incidente: Clique ou toque aqui para inserir uma data. ☐ Desconhecida

Data da descoberta do incidente: Clique ou toque aqui para inserir uma data.

Detalhes do incidente: Clique ou toque aqui para inserir o texto.

Providências tomadas: Clique ou toque aqui para inserir o texto.

Resultados alcançados: Clique ou toque aqui para inserir o texto.

_____

Jorge Susumu Seino
CONTROLADOR

COMUNICAÇÕES – ANEXO IV

1. COMUNICAÇÃO DE INCIDENTE DE DADOS AO JUIZ CORREGEDOR

AO JUIZ CORREGEDOR DA CORREGEDORIA GERAL DE JUSTIÇA DO ESTADO PR – FORO EXTRAJUDICIAL

Vimos através da presente, conforme disposto no Provimento n. 134 do Conselho Nacional de Justiça, comunicar incidente de dados pessoais acontecido no(a) Serviço do Registro de Imóveis de Pontal do Paraná, o qual teve-se conhecimento em data de _____/_____/_____, através de notificação recebida, sendo que prontamente esta serventia adotou todos os procedimentos para resolução do fato e mitigação dos riscos, conforme relatório anexo.

Na oportunidade, renovo protestos de estima e consideração.

Pontal do Paraná, ____/_____/_____.

_____

Jorge Susumu Seino
TITULAR DA SERVENTIA

2. COMUNICAÇÃO DE INCIDENTE DE DADOS À CORREGEDORIA

À CORREGEDORIA GERAL DE JUSTIÇA DO ESTADO PR – FORO EXTRAJUDICIAL

Vimos através da presente, conforme disposto no Provimento n. 134 do Conselho Nacional de Justiça, comunicar incidente de dados pessoais acontecido no Ofício Serviço do Registro de Imóveis de Pontal do Paraná, o qual teve-se conhecimento em data de _____/_____/_____, através de notificação recebida, sendo que prontamente esta serventia adotou todos os procedimentos para resolução do fato e mitigação dos riscos, conforme relatório anexo.

Na oportunidade, renovo protestos de estima e consideração.

Pontal do Paraná, _____/_____/_____.

_____

Jorge Susumu Seino
TITULAR DA SERVENTIA

3. COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E AO TITULAR DO DADO PESSOAL

COMUNICAÇÃO

Tipo de comunicação:

☐Completa. ☐Parcial preliminar. ☐Parcial complementar

Critério para a comunicação:

☐O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
☐Não tenho certeza sobre o nível de risco do incidente de segurança.

AGENTE DE TRATAMENTO

O notificante é:

☐Controlador. ☐Operador.
Se operador, informar se já houve comunicação ao controlador: ☐Sim ☐Não

Dados do agente de tratamento:

Número do CPF ou CNPJ: Clique ou toque aqui para inserir o texto.

Nome ou Razão Social: Clique ou toque aqui para inserir o texto.

Natureza da Organização: ☐ Pública ☐Privada

Endereço: Clique ou toque aqui para inserir o texto.

Cidade: Clique ou toque aqui para inserir o texto. Estado: Clique ou toque aqui para inserir o texto.

CEP: Clique ou toque aqui para inserir o texto. Telefone: Clique ou toque aqui para inserir o texto.

E-mail: Clique ou toque aqui para inserir o texto.

DADOS DO NOTIFICANTE:

Nome: Clique ou toque aqui para inserir o texto.

E-mail: Clique ou toque aqui para inserir o texto.

Telefone: Clique ou toque aqui para inserir o texto.

DADOS DO ENCARREGADO:

☐Mesmos dados do notificante.

Nome: Clique ou toque aqui para inserir o texto.

E-mail: Clique ou toque aqui para inserir o texto.

Telefone: Clique ou toque aqui para inserir o texto.

INCIDENTE DE SEGURANÇA

Descreva de forma resumida como o incidente de segurança com dados pessoais ocorreu.

Clique ou toque aqui para inserir o texto.

Quando o incidente ocorreu?

[Data e hora]

☐Não tenho conhecimento. Justifique: Clique ou toque aqui para inserir o texto.
☐Não tenho certeza. Justifique: Clique ou toque aqui para inserir o texto.

Quando a organização teve ciência do incidente de segurança?

[Data e hora]

Descreva como a organização teve ciência do incidente de segurança.

Clique ou toque aqui para inserir o texto.

Caso a comunicação inicial do incidente não foi comunicada no prazo sugerido de 2 dias úteis após ter tomado ciência do incidente, justifique os motivos.

Clique ou toque aqui para inserir o texto.

Se o incidente não foi comunicado de forma imediata após a sua ciência, justifique os motivos da demora.

Clique ou toque aqui para inserir o texto.

Qual a natureza dos dados afetados?

☐Origem racial ou étnica.
☐Convicção religiosa.
☐Opinião política.
☐Filiação a sindicato.
☐Filiação a organização de caráter religioso, filosófico ou político.
☐Dado referente à saúde.
☐Dado referente à vida sexual.
☐Dado genético ou biométrico.
☐Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).
☐Dado financeiro.

☐Nomes de usuário ou senhas de sistemas de informação.

☐Dado de geolocalização.

Outros: [Resposta]

Qual a quantidade de titulares afetados?

[Resposta]

Qual a categoria dos titulares afetados?

☐Funcionários

☐Prestadores de serviço

☐Clientes

☐Consumidores

☐Usuários

☐Pacientes de serviço de saúde

☐Crianças ou adolescentes

Outros: [Resposta]

MEDIDAS DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a ocorrência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?

[Resposta]

O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?

[Resposta]

RISCOS RELACIONADOS AO INCIDENTE DE SEGURANÇA

Quais as prováveis consequências do incidente de segurança para os titulares afetados?

[Resposta]

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

[Resposta]

COMUNICAÇÃO AOS TITULARES DE DADOS

Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?

☐Sim

☐Não

☐Não sei

Forneça detalhes.

[Resposta]

Caso os titulares afetados não tenham sido informados, quais são os motivos que justificam a não comunicação ou o seu retardo?

Clique ou toque aqui para inserir o texto.

ANEXO V - CIRCULAR

Circular n. ____/____

O delegatário do(a) Serviço do Registro de Imóveis de Pontal do Paraná, no uso de suas atribuições e visando garantir cada vez mais segurança jurídica aos procedimentos realizados na serventia, adequando-os aos requisitos constantes na Lei Geral de Proteção de Dados, expede a presente circular, informando o que segue.

1. **DESCREVER A AÇÃO**

Clique ou toque aqui para inserir o texto.

2. **DESCREVER O PROCEDIMENTO**

Clique ou toque aqui para inserir o texto.

Certos de sua compreensão.

Pontal do Paraná, _____/_____/_____.

_____

Jorge Susumu Seino
TITULAR DA SERVENTIA

Ciência do colaborador:

Estou ciente do teor da presente circular o qual me comprometo a seguir rigorosamente.

Nome Assinatura

1. _____

2. _____

3. _____

4. _____

5. _____