PODER JUDICIÁRIO

Tribunal Regional Eleitoral do Espírito Santo

PLANO DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS (Anexo à NSI 014)

Maio/2025

CONTROLE DE VERSÕES

Data	Versão	Descrição	Elaboração/Aprovação
Maio/2025	1.0	Versão inicial	Elaborado pela Equipe de Gestão da Privacidade de Dados Pessoais. Aprovado pela CSI em 13.05.205

SUMÁRIO

1. INTRODUÇÃO

Escândalos de vazamentos de dados e de ataques cibernéticos tornaram-se comuns atualmente e são provenientes de meios cada vez mais sofisticados para burlarem os controles e as medidas de segurança da informação.

Considerando o volume de dados que o Tribunal Regional Eleitoral do Espírito Santo (TRE/ES) trata, e a relevância de seu papel institucional na entrega de serviços públicos, é importante que o órgão esteja consciente de que incidentes de segurança tornaram-se uma realidade possível, e devem ser evitados com medidas de salvaguarda e prevenção.

Conforme definição constante no art. 4º do GDPR - General Data Protection Regulation - Regulamento Geral de Proteção de Dados, e tendo em vista que o TRE/ES custodia dados pessoais dos seus eleitores, é imprescindível que esteja preparado para agir em caso de "violação da segurança que provoque, de modo acidental ou ilícito a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

A LGPD (Lei Geral de Proteção de Dados Pessoais) trata dos incidentes de segurança que envolvam dados pessoais de forma muito rígida e o TRE deve estar preparado para atender às suas exigências, caso se veja envolvido em uma situação de risco.

> *Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*
> *§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, 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 de a comunicação não ter sido imediata; e*
> *VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.*
> *§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:*
> *I - ampla divulgação do fato em meios de comunicação; e*
> *II - medidas para reverter ou mitigar os efeitos do incidente.*
> *§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.*

A Política Geral de Privacidade e Proteção de Dados Pessoais da Justiça Eleitoral, instituída pela Resolução nº 23.650/2021, preconiza que as unidades administrativas da Justiça Eleitoral devem informar à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) os incidentes de

segurança que representem risco ou dano relevante aos titulares de dados pessoais, na forma e nos termos da Política de Segurança da Informação da Justiça Eleitoral (PSI-JE), da NSI-014 do TRE/ES e da LGPD. A ETIR deverá comunicar o fato ao Encarregado, caso verifique a presença de risco ou de dano aos titulares.

A comunicação da ocorrência de incidente de segurança à autoridade nacional e ao titular de dados deverá ser realizada pelo controlador, por meio do Encarregado de Dados.

As medidas a serem adotadas no caso de uma situação de emergência ou evento de risco que ocasione danos aos titulares de dados e à própria instituição devem ser de conhecimento de todos os magistrados, servidores, terceirizados e demais colaboradores do TRE-ES, de modo a viabilizar que a comunicação apropriada seja feita de forma tempestiva à ANPD e aos afetados, quando for o caso.

2. OBJETIVOS

Objetivo Geral:

Orientar os magistrados, servidores, terceirizados e demais colaboradores do TRE-ES, nas respostas aos incidentes de segurança da informação envolvendo dados pessoais.

Objetivos Específicos:

* Definir os procedimentos a serem adotados na ocorrência de incidente de segurança da informação envolvendo dados pessoais, com os respectivos responsáveis.
* Assegurar respostas rápidas, efetivas e coordenadas, para atender ao prazo legal.
* Garantir a comunicação adequada às partes interessadas.
* Preservar a integridade, a disponibilidade e a confidencialidade das informações.
*Resguardar as evidências que possam ajudar a prevenir novos incidentes e atender às exigências legais de comunicação e transparência.

3. TERMOS E DEFINIÇÕES

Para fins deste documento, aplicam-se as seguintes definições:

Agentes de tratamento: corresponde ao Controlador e ao Operador. Não são considerados controladores ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento;

Anonimização: é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Ataque: evento de exploração de vulnerabilidades. Ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

Autoridade Nacional de Proteção de Dados (ANPD): é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro;

Controlador: é o Tribunal Regional Eleitoral, representado pelo Presidente, a quem competem decisões referentes ao tratamento de dados pessoais;

Dados pessoais: informação relacionada à pessoa natural identificada ou identificável;

Dados pessoais sensíveis: são dados pessoais que dizem respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Encarregado pelo Tratamento de Dados Pessoais (Encarregado de Dados) ou Data Protection Officer (DPO): pessoa indicada pelo controlador ou operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Operador: toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador;

RIPD: Relatório de Impacto à Proteção de Dados Pessoais

Sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pelo TRE-ES para dar suporte na execução de suas atividades.

Tratamento: qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;

Vazamento de dados: qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

4. ATORES E RESPONSABILIDADES

Dentre os principais responsáveis pelas medidas a serem tomadas, em caso de incidente de segurança envolvendo dados pessoais, estão:

Comitê de Crises Cibernéticas do Tribunal Regional Eleitoral do ES: comitê responsável por promover o gerenciamento adequado de crises, por meio de resposta rápida e eficiente a incidentes em que os ativos de informação do TRE/ES tenham a sua integridade, confidencialidade ou disponibilidade comprometidas por longo período, ou quando tenha grande impacto à imagem da instituição, nos termos da Portaria PRE n. 236, de 04 de julho de 2022.

Comitê Gestor de Proteção de Dados Pessoais (CGPD): comitê responsável, em última instância, pela implementação da LGPD no TRE-ES, e por decidir, com base nas informações do Encarregado de Dados, sobre a comunicação do incidente de segurança à ANPD e aos titulares de dados (instituído pelo Ato n. 82, de 11/03/2021, alterado pelo Ato n. 181, de 02 de maio de 2024).

Comissão de Segurança da Informação do TRE-ES (CSI): comitê responsável, dentre outras atribuições, por acompanhar os processos de segurança da informação e de proteção de dados pessoais, nos termos do Ato PRE n. 171, de 26/04/2024).

Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo de servidores com responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação. Quando se tratar de incidente de segurança que envolva dados pessoais, a ETIR comunicará o ocorrido ao Encarregado de Dados, para as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança, nos termos do Ato PRE n. 339, de 23/09/2022.

5. INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Conforme art. 46 da LGPD, os agentes de tratamento devem adotar 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, e tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução.

Em caso de incidente que comprometa a segurança de dados pessoais de potenciais titulares, a ETIR deverá comunicar o evento ao encarregado, conforme previsto no art. 17, inciso X, do Ato PRE n. 339, de 23/09/2022, incluindo, minimamente, as seguintes informações, nos termos do Guia de Resposta a Incidentes de Segurança do Governo Federal:

- impacto do evento;
- natureza;
- categoria e quantidade de titulares de dados pessoais afetados;
- categoria e quantidade de dados afetados;
- consequências do incidente para os titulares de dados e para o TRE-ES;
- criticidade

O Encarregado de Dados do Tribunal, após comunicação da ETIR e com apoio das áreas afetadas e do Grupo de Trabalho Técnico de Adequação do TRE-ES à LGPD, deverá adotar os seguintes procedimentos:

5.1 COMUNICAR A OCORRÊNCIA DO INCIDENTE AO CGPD

O Encarregado de Dados, após ser comunicado pela ETIR do incidente, registrará em controle próprio o evento, e reportará imediatamente as informações recebidas ao CGPD, sugerindo o agendamento de reunião em caráter extraordinário, em até 24 horas da notificação do evento pela ETIR, se entender necessário.

5.2 PREENCHER O FORMULÁRIO DE COMUNICAÇÃO À ANPD

Considera-se como medida de boa prática a interação do Encarregado de Dados com as unidades envolvidas, de modo a dar início ao preenchimento do formulário de comunicação à ANPD (Peticionamento Eletrônico ANPD — Autoridade Nacional de Proteção de Dados), com as informações disponíveis no momento, e guardá-lo para futuro envio à ANPD, se assim for deliberado pelo CGPD.

Na medida em que outras informações forem sendo levantadas, essas deverão ser adicionadas ao formulário, para complementar o registro, dentro do prazo legal.

5.3 REUNIR COM O CGPD

Caso o CGPD entenda oportuna a realização de reunião, poderá convocar o Encarregado de Dados e demais equipes envolvidas no levantamento das informações, a fim de deliberar quanto à necessidade de comunicação ao Comitê de Crises Cibernéticas do TRE-ES, à ANPD e ao(s) titular(es) de dados afetados, bem como quanto à estratégia de comunicação externa e interna a ser executada pela assessoria de comunicação do Tribunal, se for o caso.

A comunicação à ANPD de Incidente de Segurança que possa acarretar risco ou dano relevante aos titulares, nos termos da Resolução CD/ANPD 15/2024, deve considerar os interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

a - dados pessoais sensíveis;

b - dados de crianças, de adolescentes ou de idosos;

c - dados financeiros;

d - dados de autenticação em sistemas;

e - dados protegidos por sigilo legal, judicial ou profissional; ou

f - dados em larga escala.

Considera-se incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

Para apoiar a análise do incidente de segurança, os envolvidos poderão utilizar os Manuais de Gestão de Riscos adotados pelo TRE-ES.

5.4 COMUNICAR O INCIDENTE AO COMITÊ DE CRISE CIBERNÉTICA

Caso o CGPD entenda tratar-se de incidente de alto risco, convocará o Comitê de Crises Cibernéticas do TRE-ES, nos termos da Portaria PRE n. 236, de 04 de julho de 2022 para, mediante o apoio da Assessoria de Comunicação Institucional (ASCI) e de outras unidades do Tribunal envolvidas no incidente, detalhar a estratégia de comunicação com a imprensa, público em geral e titulares de dados afetados.

Para fins deste Plano, considera-se de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:

I. critérios gerais:

a. tratamento de dados pessoais em larga escala; ou

b. tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares.

II. critérios específicos:

a. uso de tecnologias emergentes ou inovadoras;

b. vigilância ou controle de zonas acessíveis ao público;

c. decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou

d. utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

Os questionamentos a seguir servirão como parâmetro para a coleta de informações, que deverá ser realizada pela ASCI, podendo ser aprofundados e ajustados em consonância com as particularidades do incidente.

a. Quais informações foram objeto do incidente?
b. O titular pode ser vítima de fraude em razão do incidente?
c. O incidente foi devidamente comunicado às autoridades?
d. O que o titular pode fazer em benefício da sua proteção?
e. Onde o titular pode obter mais informações sobre o incidente?
f. A descrição da natureza dos dados pessoais afetados;
g. As informações sobre os titulares envolvidos;
h. A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
i. Os riscos relacionados ao incidente;
j. Os motivos da morosidade, no caso de a comunicação não ter sido imediata;
k. E as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

5.5 COMUNICAR O INCIDENTE À ANPD E AO(S) TITULAR(ES) DE DADOS PESSOAIS

Caso o CGPD entenda pertinente a notificação do incidente de segurança à ANPD, o Encarregado concluirá o preenchimento do formulário disponível no sítio eletrônico da Agência https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

O Controlador, por meio do Encarregado de Dados Pessoais do TRE/ES, será responsável por comunicar à ANPD o incidente de segurança ocorrido, **no prazo de até 3 (três) dias úteis**, nos termos da Resolução CD/ANPD nº 15, de 24 de abril de 2024 que aprova o Regulamento de Comunicação de Incidente de Segurança. As informações fornecidas poderão ser complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação.

Igualmente, deverá comunicar o incidente, de forma direta e individual sempre que possível, aos titulares cujos dados tiverem sido violados. Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, devem ser comunicados todos os presentes na base de dados comprometida.

A comunicação poderá se dar por quaisquer meios tais como SMS, e-mail, reuniões, mensagem eletrônica, ou por outro meio que seja mais adequado ao contexto.

A ANPD orienta que as informações prestadas aos titulares de dados devem ser claras e concisas. Recomenda ainda que a comunicação mencione, no que couber, os elementos previstos nos incisos do §1º do art. 48 da LGPD, tais como:

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 dos dados, observados os segredos comercial e industrial;
d. os riscos relacionados ao incidente;
e. os motivos da demora, no caso de a comunicação não ter sido imediata; e
f. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

À ANPD, deverão ser fornecidas as seguintes informações:

- A descrição da natureza e da categoria de dados pessoais afetados;
- O número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
- As medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- Os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
- A data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;
- Os dados do encarregado ou de quem represente o controlador;
- A identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;
- A identificação do operador, quando aplicável;
- A descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
- O total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

Quando houver indícios de crime, de acordo com a Lei nº 12.737, de 30 de novembro de 2012, ou outras normas presentes na legislação penal extravagante, o Controlador deverá comunicar à Polícia Federal, por meio de instrumento que entender mais adequado.

5.6 ELABORAR RELATÓRIO FINAL

A elaboração do Relatório Final é de responsabilidade do Encarregado de Dados. Se necessário, poderá solicitar o apoio da ETIR, da Comissão de Segurança da Informação do Tribunal, do Comitê Gestor de Proteção de Dados Pessoais (CGPD) e das áreas envolvidas no incidente.

O relatório deve conter o máximo de informações e evidências que tiverem sido coletadas durante a investigação do incidente, bem como o registro das deliberações das equipes envolvidas. Além disso, deve:

a) discriminar as ações realizadas pelas equipes envolvidas, para o tratamento efetivo do incidente e mitigação dos seus efeitos;
b) conter considerações sobre a promoção da melhoria contínua dos processos de tratamento de incidentes;
c) estar disponível para consulta em caso de atualização do Relatório de Impacto à Proteção de Dados (RIPD);
d) ser devidamente armazenado, para atender eventual demanda de órgãos fiscalizadores, em consonância com o princípio da responsabilização e prestação de contas (art. 6º, X da LGPD).
.

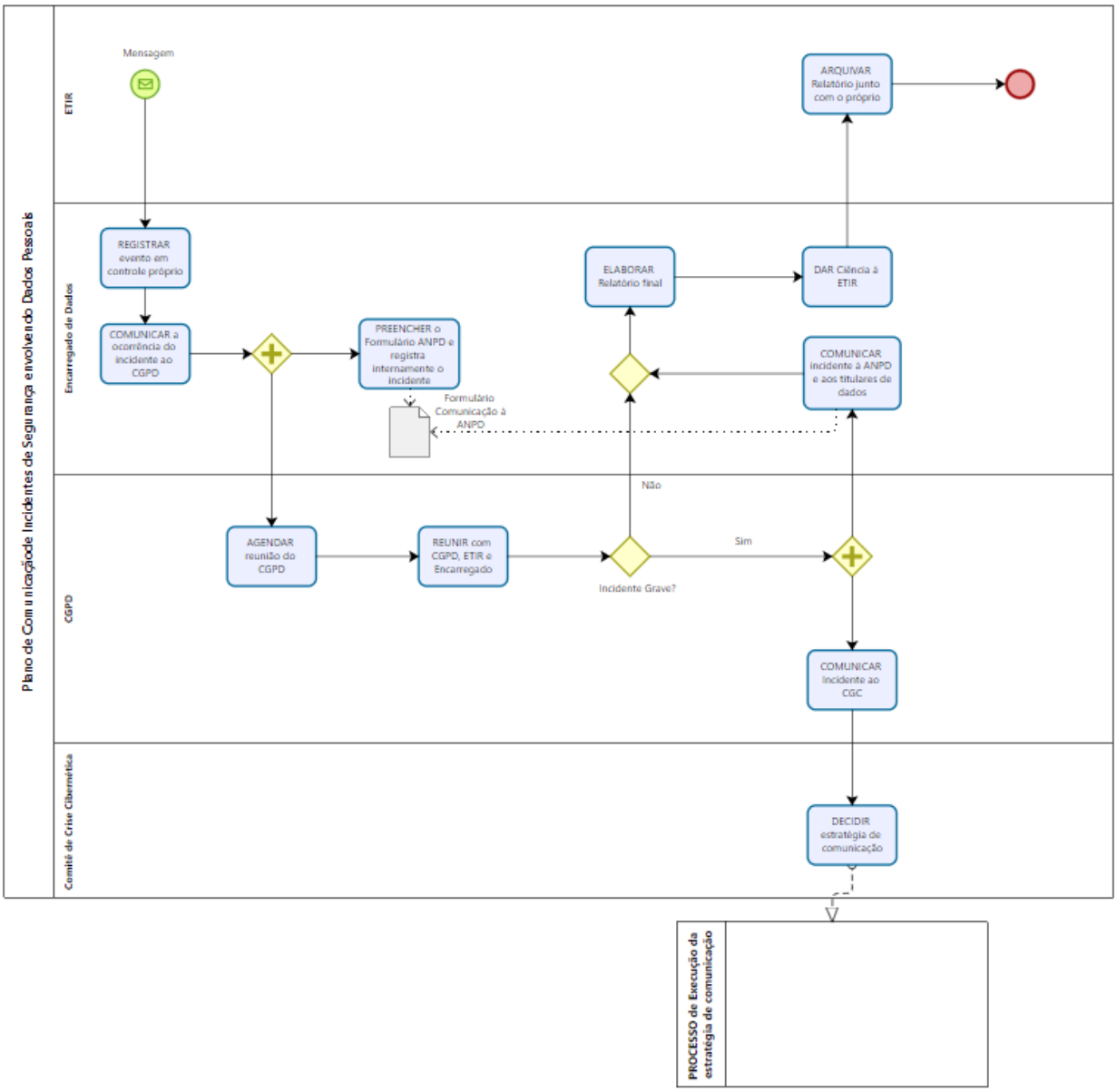
5.7 DAR CIÊNCIA À ETIR DO TRE-ES

Após as medidas de tratamento empreendidas e o registro das ações em processo administrativo eletrônico restrito, o Encarregado de Dados encaminhará o relatório final à ETIR, comunicando o desfecho do incidente de segurança envolvendo dados pessoais.

6. DISPOSIÇÕES FINAIS

Caso a ANPD, no exercício de suas competências legais, preveja procedimentos e prazos diversos dos estabelecidos neste Plano, prevalecerão aqueles definidos pela Autoridade.

7. PROCESSO DE COMUNICAÇÃO



9. REFERÊNCIAS

Lei nº 13.709/2021 - Lei Geral de Proteção de Dados Pessoais (LGPD)

Resolução TSE nº 23.650/2021 - Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral.

Resolução nº 2/2022, da ANPD – Indica critérios para definição de Alto Risco.

Resolução nº 15/2024, da ANPD - Regulamento de Comunicação de Incidente de Segurança.

Resolução nº 18/2024, da ANPD - Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.

Portaria PRE/TRE-ES nº 236/2022 - Institui o Comitê de Crises Cibernéticas no Tribunal Regional Eleitoral do Espírito Santo e define a Sala de Situação.

Ato nº 181/2024 - Atual composição do Comitê Gestor de Proteção de Dados Pessoais (CGPD) do TRE-ES

Ato PRE n. 171/2024 - Designa o Gestor de Segurança da Informação do TRE/ES

Ato PRE nº 339/2022 - Dispõe sobre a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito do TRE-ES

Guia de Resposta a Incidentes de Segurança do Governo Federal

NSI-014 - Gestão de Incidentes de Segurança da Informação - Estabelece as principais estratégias no tratamento de incidentes computacionais, que envolvam ou não dados pessoais, permitindo a adequada preparação, detecção, contenção, erradicação, recuperação, avaliação e comunicação destes incidentes.

Manual de Gestão de Riscos do TRE-ES