TRT4	PODER JUDICIÁRIO JUSTIÇA DO TRABALHO **TRIBUNAL REGIONAL DO TRABALHO DA 4.ª REGIÃO**

REGISTRO DE REUNIÃO

1. INFORMAÇÕES DA REUNIÃO

Data	**28/10/2021**	**Horário início**	**16h**	**Horário término**	**17:30h**
Tipo	Reunião do Comitê Gestor de TIC				
Local	SETIC				
Objetivo	1. Fluxo de Resposta a incidentes de segurança com dados pessoais 2. Teletrabalho na SETIC				

2. PARTICIPANTES

Nome	Área
Natacha Moraes de Oliveira	Diretora da SETIC
Alberto Muller	Coordenadoria de Gestão de TIC
Fabio de Oliveira Garcia	Coordenadoria de Desenvolvimento de Sistemas
Denilson de Quadros	Coordenadoria de Atendimento a Usuários
Pablo Barros	Coordenadoria de Implantação de Sistemas
Eric Guatimozin	Coordenadoria de Infraestrutura Tecnológica
Lucas Pozatti	Escritório de Segurança da Informação
Deise Koerber	Escritório de Projetos

3. PONTOS DISCUTIDOS

3.1	**Aprovação do Fluxo de Resposta a incidentes de segurança com dados pessoais**

Lucas apresentou o documento de proposta de Fluxo de Resposta a incidentes de segurança com dados pessoais. O fluxo define ações a serem realizadas pela SETIC na ocorrência de um incidente de segurança com dados pessoais tratados pelo TRT, cuja origem seja o ambiente tecnológico, de forma a auxiliar o TRT na resposta e resolução do evento.

- **Não contempla** a definição de ações a serem tomadas pelo TRT (comunicação ao público interno e externo, informar o incidente à ANPD e ao CNJ, etc) - tal plano deve ser

elaborado pelo GT-LGPD, uma vez que abarca ações institucionais, de diversas áreas, que extrapolam o campo de atuação da SETIC.

  - O plano da SETIC poderá fazer parte do plano institucional de resposta a incidentes com dados pessoais.

- **Não contempla** a definição de ações para o tratamento de incidentes de dados pessoais cuja origem não seja o ambiente tecnológico.

O fluxo completo está descrito como anexo desta ata.

Deliberação: Aprovado por unanimidade

3.2	**Teletrabalho na SETIC**

Natacha propôs aos coordenadores que, embora tenha sido feita uma proposta de regra interna pelos servidores da SETIC e que esta estava pendente de análise deste comitê, que inicialmente sejam adotadas combinações mais simples comuns a todas coordenadorias e que o regramento proposto seja registrado em um proad para análise futura em caso de necessidade de maior formalização. Após discussão entre os presentes, chegou-se à conclusão de que como regra comum, todos os servidores deverão realizar seu trabalho dentro do horário de funcionamento do TRT (das 8h às 18h) e que as exceções serão tratadas por cada chefia imediata. As demais regras estabelecidas pelo CNJ e TRT deverão ser seguidas por todos.
Natacha lembrou que ainda não há a necessidade de solicitar teletrabalho pois os servidores da SETIC permanecem em trabalho remoto compulsório e que a partir do momento em que é solicitado, é necessário que o gestor faça o preenchimento do formulário de planejamento e avaliação das atividades.

Deliberação: Todos de acordo.

SETIC - Plano de Resposta a incidentes de segurança com dados pessoais

OBJETIVO

- Definir ações a serem realizadas pela SETIC na ocorrência de um incidente de segurança com dados pessoais tratados pelo TRT, cuja origem seja o ambiente tecnológico, de forma a auxiliar o TRT na resposta e resolução do evento.
- **Não contempla** a definição de ações a serem tomadas pelo TRT (comunicação ao público interno e externo, informar o incidente à ANPD e ao CNJ, etc) - tal plano deve ser elaborado pelo GT-LGPD, uma vez que abarca ações institucionais, de diversas áreas, que extrapolam o campo de atuação da SETIC.
    - O plano da SETIC poderá fazer parte do plano institucional de resposta a incidentes com dados pessoais.
- **Não contempla** a definição de ações para o tratamento de incidentes de dados pessoais cuja origem não seja o ambiente tecnológico.

JUSTIFICATIVA

Ainda que a SETIC adote medidas técnicas alinhadas às melhores práticas de segurança da informação e de governança de TIC com vistas à redução do risco de incidentes envolvendo dados pessoais tratados pelo TRT, problemas eventualmente podem ocorrer.

Diante disso, uma das iniciativas necessárias diz respeito à elaboração de um plano de ação para resposta a um incidente de segurança com dados pessoais, de forma a definir as ações e procedimentos a serem executados, seus responsáveis e quando executá-los, provendo à SETIC capacidade fundamental para responder ao evento adverso com efetividade e eficácia, reduzindo ao máximo seus danos e o tempo de resolução.

A elaboração de um plano de resposta a esse tipo de incidente também demonstra diligência por parte da SETIC e, consequentemente, do Tribunal, pois a falta de ou atraso na resposta ao evento não apenas representa desconformidade com com a Lei, ao passo que o tempo de resposta acaba sendo maior na ausência de procedimentos definidos e documentados. Nessa linha, a LGPD, no art. 52, §1º, X, estabelece que: "*§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa,*

isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: […] X – a pronta adoção de medidas corretivas.".

Por fim, a elaboração deste plano de resposta a incidente também visa auxiliar no atendimento à Resolução CNJ nº 363/2021 - Relacionado ao Art. 1º, Inciso XI, Alínea a).

PAPÉIS / RESPONSABILIDADES

- **CGPD**: o Comitê Gestor de Proteção de Dados Pessoais[1] tem em sua composição representantes diretivos de diversas áreas do TRT, incluindo o Encarregado de Tratamento de Dados Pessoais (ETPD). A sua função é deliberar, atuar e assessorar a Presidência em assuntos relacionados à LGPD no âmbito do TRT.
- **SETIC:** realizar a investigação de suspeita e/ou confirmação de incidentes de segurança com dados pessoais analisando o tipo de incidente, a extensão, quais sistemas tecnológicos foram afetados e, se possível, quais dados foram envolvidos; propor e executar ações para estancar o problema/falha tecnológica que originou o incidente; realizar correções no ambiente tecnológico para sanar o problema que causou o incidente; elaborar relatório do incidente e encaminhá-lo às instâncias superiores (representadas pelo CGPD);

O QUE É UM INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS?

Segundo a Agência Nacional de Proteção de Dados (ANPD), um incidente de segurança com dados pessoais é: *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.*

Atualmente, um dos principais incidentes de segurança envolvendo dados pessoais é o **vazamento de dados pessoais**. Segundo um estudo da IBM[2], 80% dos vazamentos de dados em organizações envolvem o extravio ou roubo de dados pessoais dos clientes. Ainda de acordo com a publicação, há também o comprometimento de dados de propriedade intelectual, dados pessoais de funcionários e dados empresariais em geral.

Devido à larga adoção de tecnologia da informação para consecução das atividades de uma organização, as principais causas para vazamento de dados residem no ambiente

[1] Instituído pela Portaria TRT4 nº 389/2021
[2] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

tecnológico. Portanto, os ciberataques são as ações que mais frequentemente causam os incidentes, seguidos de erros de sistema e falhas humanas.

RESPONDENDO A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

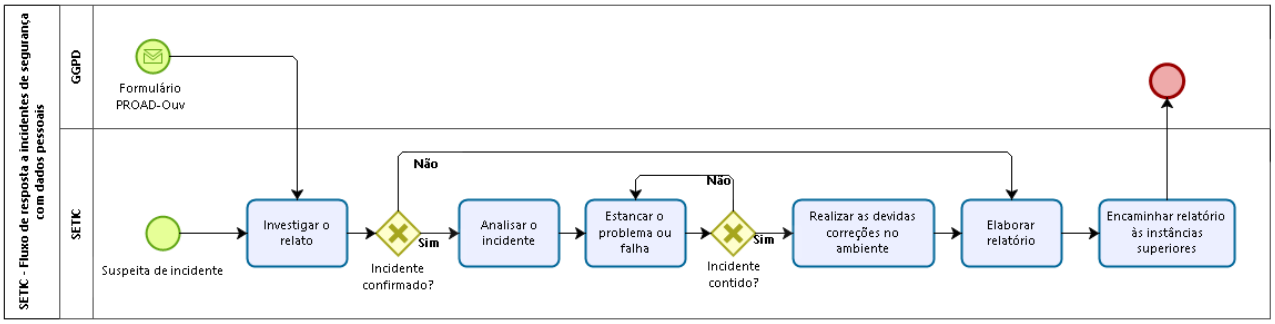
De acordo com a ANPD[3], as informações contidas na comunicação do incidente devem ser claras e concisas. A LGPD define como a comunicação deve ser feita no § 1º do artigo 48 da LGPD. Adicionalmente, é recomendado incluir as seguintes informações:

- Data e hora da detecção.
- Data e hora do incidente e sua duração.
- Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros.
- Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados.
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento.
- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados.
- Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD.
- Resumo das medidas implementadas até o momento para controlar os possíveis danos.
- Possíveis problemas de natureza transfronteiriça.
- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Segundo o Art. 48 da LGPD, o controlador tem a obrigação de comunicar o incidente à ANPD e ao titular dos dados. Portanto, não é escopo desse plano a definição dessa atividade. A SETIC apenas elaborará o relatório técnico do incidente, no âmbito do ambiente tecnológico, que poderá compor a comunicação feita à ANPD.

FLUXOGRAMA

[3] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca



SETIC - Fluxo de resposta a incidentes de segurança com dados pessoais
v1 - set/2021

DETALHAMENTO DAS ATIVIDADES

Formulário PROAD-Ouv		
Descrição	É quando uma pessoa (geralmente externa) entra em contato com o TRT por meio do sistema da Ouvidoria, requisitando algo em relação aos dados pessoais tratados pelo Tribunal. Dependendo do tipo da requisição, poderá ser encaminhado à SETIC para que seja avaliado se trata-se de um incidente de segurança com dados pessoais ou não.	
Papéis	CGPD	
Considerações importantes	Se a requisição não estiver relacionada a um possível incidente (vazamento, exposição, extravio, etc), o fluxo de atendimento é outro (ainda assim poderá envolver a SETIC).	
Entradas	Formulário PROAD-Ouv	
Saídas	Encaminhamento à SETIC	
Atividades	**Encaminhar expediente à SETIC**	Repassar expediente PROAD à SETIC

Suspeita de incidente	
Descrição	É quando a SETIC, por algum meio que não o PROAD-Ouv, recebe a informação sobre a ocorrência de um possível incidente de segurança com dados pessoais - exemplos: sistemas de monitoramento, abertura de chamado, notificação do CTIR.br, noticiário, responsável pelo ciberataque, dentre outros.
Papéis	SETIC
Considerações importantes	Neste caso, a SETIC deverá imediatamente informar ao CGPD a ocorrência suspeita e formalizar um expediente para registrar a investigação e eventual tratamento do caso.
Entradas	Contatos externos ao TRT;
Saídas	Informe ao CGPD e abertura de expediente para registro das ações

Atividades	**Abrir expediente para registro das ações**	Abrir um expediente no PROAD para registrar as ações tomadas;

Investigar o relato		
Descrição	Avaliar o formulário ou a suspeita para verificar se de fato é um incidente de segurança com dados pessoais, oriundo do ambiente tecnológico do TRT.	
Papéis	SETIC	
Considerações importantes	É importante confirmar se não é um falso-positivo, se a fonte dos dados vazados é o TRT.	
Entradas	Formulário PROAD-Ouv; Relato de suspeita de incidente	
Saídas	Decisão se trata-se de um incidente ou não	
Atividades	**Analisar o PROAD-Ouv**	Tomar conhecimento do expediente encaminhado e analisar as informações. Caso se confirme o incidente, atuar de acordo com a necessidade e com o fluxo estabelecido. Se não for confirmado o incidente, atualizar o expediente e devolver às instâncias superiores.
	Analisar a suspeita	Avaliar a suspeita encaminhada à SETIC de forma a confirmar a ou não ocorrência de um incidente. Em caso positivo, atuar de acordo com a necessidade e com o fluxo estabelecido. Se não for confirmado o incidente, atualizar o expediente aberto e encaminhá-lo às instâncias superiores para ciência.

Analisar o incidente	
Descrição	Realizar avaliações, diligências e análises para entender qual é o tipo de incidente envolvendo dados pessoais (vazamento, apagamento, acesso indevido, etc), onde que está o problema, o que causou o incidente, para que possam ser elencadas medidas para contornar ou corrigir a fragilidade que ocasionou o incidente, estancando o problema.
Papéis	SETIC
Considerações importantes	Registrar os passos da investigação e os achados de acordo com as boas práticas forenses, primando pela integridade dos achados, pois o incidente poderá ser tratado como crime. Levantar quais dados pessoais foram afetados (por exemplo, se há dados pessoais sensíveis); Separar eventuais evidências que forem importantes para a documentação das ações de resposta ao incidente;
Entradas	Relato do incidente

Saídas	Causa, extensão e possíveis remediações do incidente; Relatório de investigação	
Atividades	**Investigar o incidente**	Entender qual foi o impacto às informações (vazamento, exposição indevida, apagamento, alteração indevida, etc), quais dados foram afetados, qual o sistema e/ou serviço originou o incidente, por que o problema ocorreu, etc;
	Propor medidas de contenção do incidente	Definir medidas e ações para estancar o incidente o mais breve possível. Dependendo da ação, talvez seja necessária aprovação do Comitê Gestor de TIC ou até mesmo de instâncias superiores - importante ter um canal de comunicação que forneça agilidade.
	Documentar investigação	À medida em que a investigação for avançando, documentar as ações realizadas, que serão parte do relatório a ser elaborado. Atentar para registrar a linha do tempo, as ações realizadas, quem as realizou, dentre outras informações;

Estancar o problema ou falha		
Descrição	Aplicar as medidas de contenção/contorno do problema que causou o incidente e avaliar sua efetividade.	
Papéis	SETIC	
Considerações importantes	Dependendo da medida a ser aplicada, é necessário obter aprovação formal (Comitê Gestor de TIC, Comitê de Governança de TIC, Presidência, etc)	
Entradas	Análise do incidente, com a proposta de contorno da falha ou problema.	
Saídas	Contenção do problema;	
Atividades	**Aplicar medidas de contenção do problema**	Realizar ações para estancar o problema (restaurar backup, configurar o controle de acesso, ajustar rotinas, etc) de acordo com o tipo de incidente. Pode ser que tal medida já seja uma correção para evitar que o problema volte a ocorrer.
	Avaliar se medidas foram eficientes para estancar o problema	Verificar se as medidas foram suficientes para contornar/resolver o incidente. Caso necessário, propor novas medidas e aplicá-las.

Realizar as devidas correções no ambiente		
Descrição	De acordo com a análise do incidente, propor medidas para corrigir as falhas que ocasionaram o incidente.	
Papéis	SETIC	
Considerações importantes	Avaliar se as medidas para contenção do incidente já não foram suficientes para correção do problema. Dependendo da medida para correção, é necessário obter aprovação formal (Comitê Gestor de TIC, Comitê de Governança de TIC, Presidência, etc).	
Entradas	Análise do incidente; Medidas de contenção do incidente;	
Saídas	Solução definitiva para correção do problema	
Atividades	**Propor e aplicar solução corretiva**	Considerar a análise do incidente para propor medidas para corrigir o problema que ocasionou o incidente e posteriormente aplicá-las. Levar em consideração as medidas para contenção do incidente (verificar se a aplicação delas já não corrigiu o problema em definitivo).

Elaborar relatório		
Descrição	Consolidar informações produzidas durante a atuação no incidente em um relatório, que será anexado ao expediente formal.	
Papéis	SETIC	
Considerações importantes	O relatório deve ser o mais completo possível, observando os requisitos estabelecidos pela LGPD e pela ANPD, além das boas práticas forenses. Anexar eventuais evidências coletadas durante a resposta ao incidente;	
Entradas	Investigação, análise e contenção do incidente, além das medidas de correção.	
Saídas	Relatório do incidente (atuação da SETIC);	
Atividades	**Redigir relatório**	Elaborar relatório com as informações coletadas durante o fluxo das atividades. Caso a suspeita de incidente não tenha se confirmado, documentar o porquê de não ter sido confirmado.

Encaminhar relatório às instâncias superiores	
Descrição	Juntar o relatório produzido ao expediente aberto no PROAD e encaminhá-lo às instâncias superiores.
Papéis	SETIC
Considerações importantes	N/A
Entradas	Relatório do incidente

Saídas	Expediente devolvido às instâncias superiores	
Atividades	**Juntar relatório ao expediente**	Juntar documentação produzida ao expediente aberto anteriormente.
	Devolver expediente	Encaminhar expediente às instâncias superiores (Ouvidoria, CGPD, Presidência, etc).

REFERÊNCIAS

- https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca
- https://www.microserviceit.com.br/lgpd-e-vazamento-de-dados/
- https://www.unoesc.edu.br/unoesc/lgpd/politica-incidentes
- https://opiceblum.com.br/plano-de-resposta-a-incidentes-de-seguranca-de-dados-pessoais-uma-prevencao-importante/
- https://securityintelligence.com/incident-response-under-gdpr-what-to-do-before-during-and-after-a-data-breach/
- https://www.breachrx.com/2021/05/25/understanding-gdpr-incident-response-guidelines/
- https://iapp.org/resources/article/data-breach-response-guide-2/