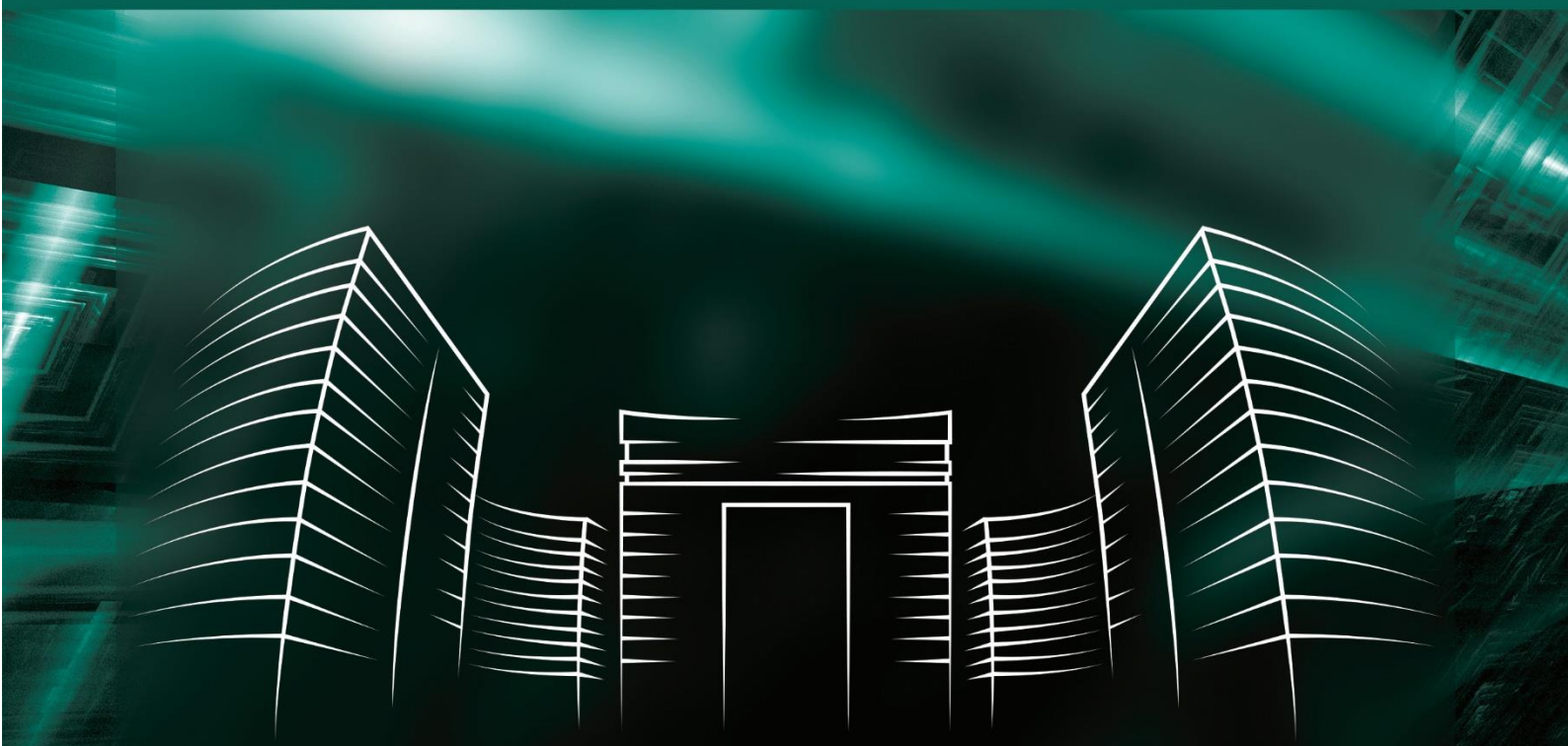
PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO



2022

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Delner Freire

Superintendente

Maico Moreira Silva

Diretor Técnico

COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

Leonardo Courinos Lima da Silva

ELABORAÇÃO

Daltro Barbosa

Eduardo Falkemback Zimmer

Rosemeire Vidal

Tiago Lopes de Aguiar

REVISÃO

Anderson Gomes de Souza

Carlos Cunha

Ed Carlos Egert Galvão

Hendrei de Souza Maia

Idan Souza

Jean Franco Ronconi de Lima

Leonardo Courinos Lima da Silva

Luma Damon de Oliveira Melo

Monike Izzo Martins

Rafael Domingues Cordeiro

Rogério Eduardo Vieira Alvez

VERSÃO

VERSÃO	DATA	AUTOR	AÇÃO
1.0	01/08/2022	Daltro Barbosa, Eduardo Zimmer, Rosemeire Vidal e Tiago Lopes.	Criação do documento Plano de Gestão de Incidentes de Segurança da Informação.

LISTA DE ABREVIATURAS

Além das abreviaturas, conceitos e definições descritos neste item, também será considerado o Glossário de Segurança da informação do Departamento de Segurança da Informação - DSI do Gabinete de Segurança Institucional da Presidência da República - GSI/PR, instituído por meio da Portaria nº 93, de 18 de outubro de 2021 (Glossário de Segurança da Informação), ou o que vier a lhe substituir:

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

CAF - Coordenadoria de Administração e Finanças;

CGPD - Comitê Gestor de privacidade de Dados Pessoais da Setic**;**

CI - Controle Interno;

COINFRA - Coordenação de Infraestrutura;

COSEGI - Coordenação de Segurança da Informação e Comunicação;

CPSI - Comissão Permanente de Segurança da Informação;

CSIRT - Grupo de Resposta a Incidente de Segurança (*Computer Security Incident Response Team*);

GEDC - Gerência de Datacenter;

GLPI - Sistema de gestão de chamados de código aberto (*Gestionnaire Libre de Parc Informatique*);

GOPS - Gerência de Operações;

GPREVI - Gerência de Prevenção e Resposta a Incidentes;

PGISI - Plano de Gestão de Incidentes de Segurança da Informação;

SETIC - Superintendência Estadual de Tecnologia da Informação e Comunicação.

SUMÁRIO

1- INTRODUÇÃO.....7
2- OBJETIVO 8
2.1 Abrangência e prazo de vigência 9
3- PAPÉIS E RESPONSABILIDADES 8
4- FLUXOS DE PROCESSOS 11
5- INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NÃO RELACIONADOS A RECURSOS COMPUTACIONAIS 16
6- RESPOSTAS A INCIDENTES DE SEGURANÇA 16
7- COMUNICAÇÃO 17
8- INDICADORES DOS PROCESSOS 18
9- PRESERVAÇÃO DE EVIDÊNCIAS 18
10-CONSIDERAÇÕES FINAIS 19
11-REFERÊNCIAS 20

1 INTRODUÇÃO

Considerando a Política de Segurança da Informação da SETIC, constituída por meio da Portaria nº 97, de 9 de junho de 2021, destacando-se seu art. 126, que prevê a instituição do Plano de Gestão de Incidentes de Segurança da Informação da rede de dados da SETIC que deverá ser fielmente cumprido, devendo ser regulamentado por normativo próprio e executado por um processo contínuo, definido de maneira formal, visando assegurar que fragilidades e eventos de segurança da informação sejam comunicados, registrados, monitorados e avaliados.

Considerando a definição de “incidente” conforme previsto na ISO/IEC 27000:2008, a saber:

> 3.30 Evento de segurança da informação
> “ocorrência identificada de um sistema, serviço ou estado de rede indicando uma possível quebra da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança”.
>
> 3.31 Incidente de segurança da informação
> “um único, ou uma série de eventos indesejados ou inesperados de segurança da informação, que têm uma probabilidade significativa de comprometer as operações do negócio e de ameaçar a segurança da informação”.

Considerando ainda a Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD); o Decreto Estadual nº 26.451, de 4 de outubro de 2021, que dispõe sobre a adoção de medidas para aplicação da LGPD no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo do Estado de Rondônia; e a Portaria SETIC nº 54/2021, que institui o Programa de Governança em Privacidade da SETIC.

A SETIC resolve instituir o Plano de Gestão de Incidentes de Segurança da Informação - PGISI, que tem intuito de definir o processo de tratamento de incidentes de segurança, resposta a incidentes de segurança e de privacidade por meio de etapas, com implementação de procedimentos bem definidos que nortearão a equipe para o desenvolvimento de ações em caso de ocorrência de um incidente de segurança, ou para evitá-los através de identificação prévia. O

grupo de etapas estabelecidas permite designar um fluxo lógico municiando ações a serem realizadas nas diferentes etapas do processo.

Isto posto, o plano designa o passo a passo adotado para responder aos cenários de emergência, ou evento de risco, que possam ocasionar algum impacto aos ativos sob a responsabilidade da SETIC, logo, visa uma resposta célere e precisa.

Salientamos que este Plano não aborda um modelo específico de incidente, mas estabelece etapas factíveis e processos pré-definidos, atendendo aos preceitos legais. Reforçamos que na hipótese de ocorrência de incidente grave e que não haja tempo para estudo mais complexo, a premissa é de ação imediata para conter maiores danos. Destarte, não será caracterizado incidente de segurança o ato de analisar vulnerabilidades e realização de *pentest* previamente autorizado.

2 OBJETIVO

O PGISI descreve a maneira como a **SETIC** vai tratar incidentes de segurança da informação, avaliando a gravidade e as respostas aos incidentes de segurança da informação, ao mesmo tempo que resguarda evidências forenses, a fim de ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência.

O PGISI objetiva instrumentalizar a SETIC por meio de direcionamentos, diretrizes e responsabilidades quanto à gestão de incidentes de segurança da informação, estabelecendo o adequado tratamento em resposta aos incidentes de segurança, buscando reduzir ao máximo os impactos suportados e a promoção da continuidade das operações de funcionamento.

Conforme preconiza o Anexo A da ABNT NBR ISO/IEC 27001:2013, no item A.8 Gestão dos ativos, objetiva identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.

2.1 ABRANGÊNCIA E PRAZO DE VIGÊNCIA

Este plano abrange todos os recursos computacionais pertencentes, operados, mantidos e controlados pela SETIC.

O Plano de Gestão de Incidentes de Segurança da Informação entrará em vigor na data de sua publicação, sendo revisado e atualizado a cada 2 (dois) anos, podendo ser revisto ou alterado sempre que houver a necessidade, pela Coordenação de Segurança da Informação por meio da Comissão Permanente de Segurança da Informação.

3 PAPÉIS E RESPONSABILIDADES

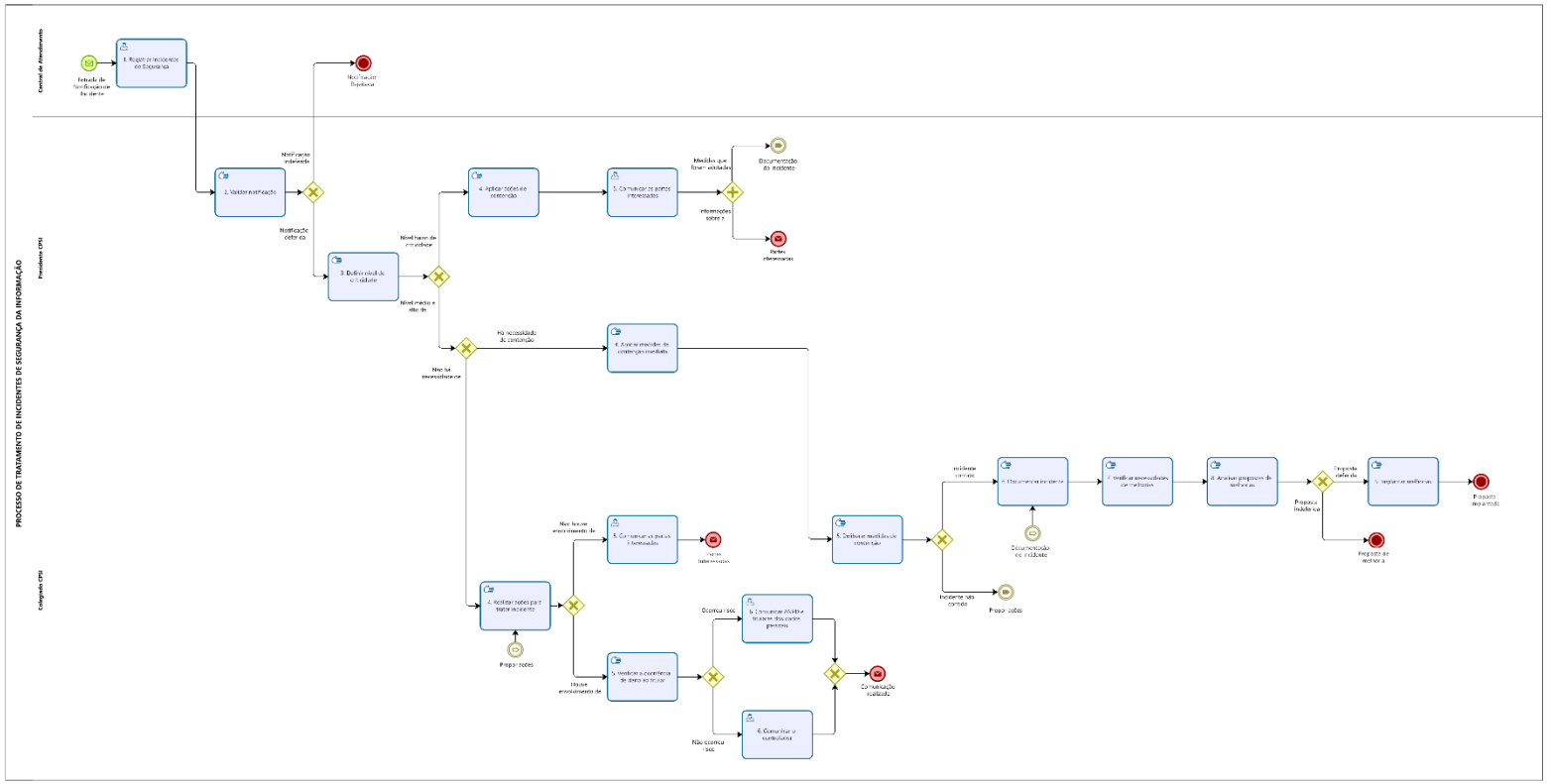
A tabela abaixo tem por objetivo promover a identificação dos principais atores e descrever os papéis e responsabilidades individuais e em grupo, pela proteção dos ativos:

Papéis	Responsabilidades
Central de Atendimento (Suporte e conectividade)	Atendimento de chamados Nível 1 e 2, atendimento via VOIP, via Chat e SEI. Suporte a sistemas do governo, gerenciamento de usuários e monitoramento de ativos. A Central de Atendimento será o meio de entrada de registro dos incidentes de segurança para posterior tratamento e resposta aos mesmos.
Notificador	É uma pessoa ou sistema de monitoração que notifica incidentes.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (conforme Lei Federal nº 13.709, de 14 de agosto de 2018 - LGPD);
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (conforme Lei Federal nº 13.709, de 14 de agosto de 2018 - LGPD);
Comissão Permanente de Segurança da Informação (CPSI)	Responsável por receber, analisar e responder a notificações e atividades classificadas como incidentes de segurança da informação da SETIC; Realizar análise e/ ou investigação de incidentes de segurança da informação e propor medidas de contenção, ou para solucionar problemas que causaram o incidente.

	A CPSI será caracterizada como Grupo de Respostas a Incidentes de Segurança da Informação (CSIRT) ao receber, analisar, registrar e responder criticamente aos incidentes de segurança da informação considerando seu nível de criticidade.
Coordenador de Segurança da Informação e Comunicação.	Responsável por monitorar o ambiente e recursos de TIC da SETIC, a fim de identificar preventivamente possíveis incidentes de segurança da informação.
Encarregado pelo Tratamento de Dados Pessoais.	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD). Deverá atuar em todas as questões relativas à privacidade e proteção de dados pessoais na SETIC, conforme preconiza o Programa de Governança e Privacidade.
Assessor (a) de Comunicação - ASCOM/SETIC-RO	Responsável pelas comunicações e informativos de interesse público, representando a SETIC e zelando pela veracidade das informações divulgadas.
Alta Administração - Superintendência e Diretoria Executiva.	Responsáveis pela aprovação das ações apresentadas pelo presidente da CPSI e pela Coordenação de Segurança da Informação e Comunicação.
Equipe Técnica das diversas áreas da SETIC: COINFRA, CAGD, GPREVI e CODE.	Auxiliar a CPSI e a Coordenação de Segurança da informação na proposição e execução de medidas para contenção, solução e resposta aos incidentes de segurança da informação.

4 FLUXOS DE PROCESSOS

O fluxo do processo e a descrição das atividades de tratamento de Incidentes de Segurança da Informação e Privacidade é descrito abaixo.



Descrição do Processo de Tratamento de Incidentes de Segurança da Informação:

 **Registrar Incidentes de Segurança:** As notificações de incidentes de segurança da informação serão recepcionadas pela Central de Atendimento, com a utilização do sistema GLPI, podendo as mesmas, serem registradas através do notificador por meio de chamado no sistema supracitado, ou por diversos meios de comunicação, como: e-mail, Sistema eletrônico (SEI), aplicativos de mensagem instantânea e canais de comunicação oficiais. Desta forma evidencia-se que todas as notificações fora do sistema GLPI, serão armazenadas e registradas nesse sistema, a fim de manter a biblioteca de entrada de registros.

 **Validar notificação:** O Presidente da CPSI, em representação da comissão, deve realizar a avaliação preliminar ou contatar outro acionador membro da CPSI em condições de realizar o diagnóstico de identificação de incidente de segurança da informação, descartando as notificações nulas ou claramente improcedentes, tomando as devidas medidas. No processo de avaliação preliminar deve-se coletar informações sobre os possíveis riscos de impactos, sua criticidade, os danos aparentes e o risco de se agravar, caso não tenha resposta imediata. De acordo com a confirmação e diagnóstico positivo de incidente de segurança será encaminhada para trâmites regulares da CPSI. Em caso de incidentes de nível médio / alto e que exigem resposta imediata, o presidente da CPSI aplicará medidas de contenção de forma urgente. Posteriormente essas medidas de contenção emergenciais serão deliberadas pela CPSI.

 **Definir nível de criticidade:** O Presidente da CPSI, no uso das suas atribuições, deverá levar em consideração durante a avaliação o nível de criticidade do incidente, a fim de definir uma ordem de atendimento, considerando a urgência de tratamento e seu impacto. Segue a classificação:

- Alto (Impacto Grave): Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar algum impacto negativo;
- Médio (Impacto Significativo) - Incidente que afeta sistemas ou informações não críticas, sem impacto negativo à instituição;
- Baixo (Impacto Mínimo) - Possível incidente, sistemas não críticos;

Obs.: Todos os incidentes que envolvam dados pessoais serão classificados como de nível médio / alto.

 **Aplicar medidas de contenção imediata:** Os incidentes que forem classificados como de nível médio ou alto, caso haja necessidade de contenção imediata, serão aplicadas medidas emergenciais para a contenção do incidente.

 **Deliberar medidas de contenção:** As medidas de contenção aplicadas de forma imediata serão deliberadas pela CPSI para que seja verificado se estas medidas contiveram o incidente classificado como de nível médio / alto.

 Propor Ações

 **Aplicar ações de contenção:** O presidente da CPSI aplicará medidas de contenção aos incidentes classificados como de nível baixo. Caso a medida não resolva o incidente, deverá ser proposta novas ações para conter o incidente. Caso o incidente seja contido, será necessário comunicar às partes interessadas.

 **Comunicar às partes interessadas:** Diante da ocorrência de incidentes de segurança que não envolvam dados pessoais, o colegiado da CPSI, de posse da extensão e do impacto do incidente, deverá comunicar outras áreas da SETIC sobre o ocorrido.

Documentação do Incidente

Propor Ações

Realizar ações para tratar incidentes: considerado um incidente de segurança que não necessite de uma resposta imediata, o colegiado da CPSI irá propor ações de contenção do incidente de segurança, a fim de conter e erradicar, limitando os danos e isolando os sistemas afetados para evitar mais danos. Nesta fase deve-se identificar o máximo de dados envolvidos, métodos e vulnerabilidades exploradas. Em caso de necessidade, deve-se envolver especialistas dos sistemas afetados. Com base nas informações levantadas na investigação do incidente, caso envolvam suspeita / vazamento de dados pessoais, na atividade “verificar a ocorrência de dano ao titular” será feita uma investigação para verificar se houve dano ao titular dos dados. Ainda nessa fase, de acordo com a necessidade e a autorização obtida, poderá ocorrer o desligamento dos sistemas inteiros ou de funcionalidades específicas, comunicados de indisponibilidade e manutenção sempre que necessário e mantendo cuidados para manter evidências que comprovem autoria, origem e métodos utilizados para gerar o incidente. Serão executadas as ações propostas, visando conter o incidente. Nesta etapa podem ser iniciados os Planos de Contingência, levando em consideração as informações disponibilizadas advindas da fase de validação do incidente. É verificado se o resultado esperado foi alcançado. Em caso negativo, deverá propor / realizar novas ações para contenção do incidente.

Verificar a ocorrência de dano ao titular: Se no incidente de segurança for constatado que houve envolvimento de dados pessoais, deverá ser feita uma investigação para identificar se houve dano ao titular dos dados.

Comunicar ANPD e titulares dos dados pessoais: A CPSI notificará o Encarregado pelo Tratamento de Dados Pessoais e o CGPD da SETIC quando forem identificados incidentes de segurança da informação envolvendo dados pessoais. Em caso de identificação que o incidente acarretou risco ou dano relevante aos titulares de dados, deverá o Encarregado de Tratamento de Dados (DPO) da SETIC e a Assessoria de Comunicação fazer as comunicações obrigatórias por Lei, bem como informar e subsidiar. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados e imprensa, bem como relatórios formais para a ANPD.

Comunicar o controlador: Em caso de incidente de segurança em que ocorra vazamento de dados pessoais, mas que não acarrete dano ao titular dos dados, o controlador deverá ser comunicado sobre o vazamento de dados.

Documentação de Incidentes

Documentar do incidente: Após o incidente ser contido e solucionado, as medidas adotadas para contenção / erradicação do incidente deverão ser documentadas para futuras proposituras de melhorias de implementações, atendendo a conformidade da PSI em seu Art.: 116° - Serão documentados todos os incidentes de segurança e vulnerabilidades identificadas durante o processo de desenvolvimento e manutenção do sistema.

Verificar necessidades de melhorias: Com base na fase anterior (Documentar Incidente), será elaborada uma proposta de melhoria para aprovação do colegiado.

Analisar proposta de melhorias: A CPSI irá analisar a proposta de melhoria elaborada no processo anterior, caso a proposta seja aceita, as melhorias deverão ser implementadas.

 **Implantar melhorias:** Após a proposta ser deferida na atividade anterior, a CPSI irá implementá-las.

5 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NÃO RELACIONADOS A RECURSOS COMPUTACIONAIS.

Salientamos que os Incidentes de Segurança da Informação não relacionados a recursos computacionais seguirão o trâmite de entrada de demanda através do Sistema GLPI, para registro. Em seguida será realizado o trâmite de tratamento e resposta ao incidente, passando pela CPSI, que durante a resolução envolverá os responsáveis afetados.

A CPSI irá conduzir o registro do incidente e das lições aprendidas, bem como realizar as comunicações para o Encarregado de Dados (DPO) em casos de envolvimento de dados pessoais.

6 RESPOSTAS A INCIDENTES DE SEGURANÇA

A recepção, tratamento e resposta aos incidentes formam a gestão dos incidentes. Dessa forma, a COSEGI conta com a estrutura da CPSI e da Gerência de Prevenção e Resposta a Incidentes com intuito de atender as demandas de incidentes de segurança da informação.

Conforme consta neste Plano de incidentes, é demonstrado o trâmite de entrada, identificação, tratamento e resposta, além dos registros e lições aprendidas, visando a melhoria constante dos serviços realizados no ambiente da SETIC.

Dessa forma, visamos atender todas as demandas identificadas e comunicadas, bem como estar em harmonia com o trabalho do Encarregado de Dados e proteção de todas as informações trafegadas e sob a guarda da SETIC.

Quando houver violação de dados pessoais, deverá ser mantido registro com informações suficientes para fornecer relatório para propósitos forenses e/ou regulatórios, contendo no mínimo: descrição do incidente, período de tempo, consequências, nome do relator, para quem o incidente foi reportado, os passos tomados para resolver o incidente, em que resultou o incidente, tais como

perda, divulgação ou alterações, notificação e sua origem caso houver, e demais informações que a equipe de tratamento julgar necessário.

7 COMUNICAÇÃO

As comunicações internas e que necessitem de publicidade através dos meios de comunicação oficiais serão realizadas pela ASCOM, com orientação da CPSI e aprovação da alta gestão, dessa forma dando publicidade e informando medidas de contenção e mitigação de seus efeitos.

A equipe de tratamento e resposta a incidentes reportará as ocorrências de incidentes de segurança à comunidade interna e externa de acordo com a necessidade.

Quando for necessário proceder com a comunicação à ANPD e ao titular de dados pessoais sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, a SETIC, com apoio da CPSI e do Encarregado de Dados, providenciará a comunicação dentro do prazo, mencionando no mínimo: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; os riscos relacionados ao incidente; os motivos da demora, no caso de a comunicação não ter sido imediata; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A SETIC deverá adotar as providências determinadas pela ANPD tais como: ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

Deve ser criada uma biblioteca com modelos de documentos (templates) para comunicação formal do Encarregado pelo Tratamento de Dados Pessoais com a ANPD, titulares de dados, notificadores e imprensa.

A comunicação dos incidentes advindas dos servidores da SETIC para a CPSI, deve preconizar o previsto na PSI, conforme o Art. 12º É obrigação de todo servidor que tomar conhecimento de incidente que afete a segurança da informação registrar o ocorrido através de chamado no sistema GLPI, mantido pela SETIC, para análise da CPSI.

8 INDICADORES DOS PROCESSOS

Todos os incidentes registrados através do sistema GLPI e avaliados pelo CPSI irão gerar registros e serão acompanhados como indicadores de resultado.

Indicador	Descrição	Métrica
Número de Incidentes de Segurança da Informação identificados.	Número total de incidentes registrados e classificados pela Central de Atendimento como incidentes.	**Resultado:** Número absoluto. **Periodicidade:** Mensal **Fonte:** GLPI e CPSI.
Número de Incidentes de Segurança da Informação solucionados.	Número total de incidentes registrados e classificados pela Central de Atendimento como incidentes solucionados.	**Resultado:** Número absoluto. **Periodicidade:** Mensal **Fonte:** GLPI e CPSI.
Número de Incidentes de Segurança da Informação não solucionados.	Número total de incidentes registrados e classificados pela Central de Atendimento como incidentes não solucionados.	**Resultado:** Número absoluto. **Periodicidade:** Mensal **Fonte:** GLPI e CPSI.
Tempo médio de respostas aos incidentes identificados.	Tempo médio de atendimento dos incidentes identificados.	**Resultado:** Número absoluto em horas. **Periodicidade:** Mensal **Fonte:** GLPI e CPSI.

9 PRESERVAÇÃO DE EVIDÊNCIAS

Após ocorrido um incidente, caso seja necessário a preservação de evidências, será mantido todo material coletado durante o tratamento do incidente pelo período mínimo de 1 (um) ano, com base no art. 13 da Lei Federal nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Tal procedimento é prática, antes de se iniciar as ações de restauração de operação do ambiente, a preservação de provas para identificação correta da causa raiz do incidente e, posteriormente, a realização da recuperação dos sistemas afetados.

10 CONSIDERAÇÕES FINAIS

Portanto, este plano descreve um processo para tratar os incidentes de segurança da informação da SETIC, que venham ocasionar algum impacto aos ativos mantidos pela SETIC. Desta forma, o documento enaltece os passos necessários para uma resposta ágil e precisa, atendendo as exigências legais de comunicação e transparência para segurança da informação e privacidade.

Com enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

Outrossim, pretende-se alcançar os objetivos de detecção de eventos de incidentes de segurança da informação e seu tratamento, prover a identificação, avaliação e resposta adequada. Minimizar os efeitos de incidentes de segurança da informação, tratando-os o mais rápido possível.

11 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: 2013;

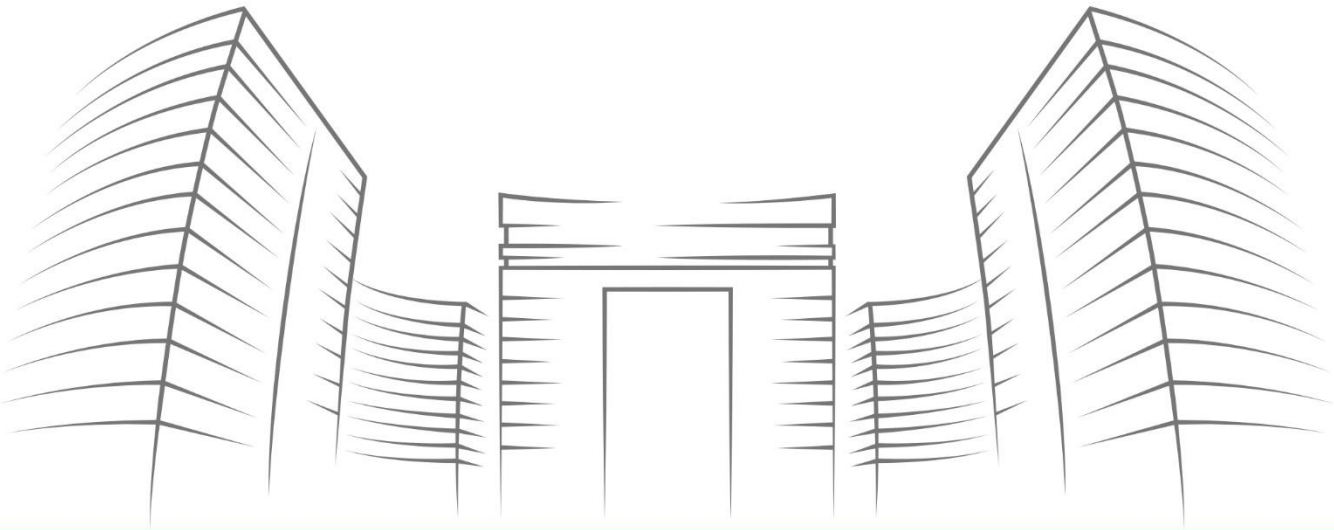
ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistema de gestão da segurança da informação - Requisitos. Rio de Janeiro: 2013;

SETIC/Governo de Rondônia. RELATÓRIO DE ANÁLISE DE RISCOS - Identificar, classificar e comparar o impacto dos riscos com o cenário de atuação, identificando lacunas de segurança e antecipar contingências a riscos iminentes e prever ações para sanar pontos fracos, através da implementação de controles de segurança. COSEGI;

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 17 mar. 2022;

RONDÔNIA. Portaria nº 54/2021/SETIC. Programa de Governança em Privacidade da SETIC. Disponível em: https://wiki.setic.ro.gov.br/doku.php?id=start:docs:programa_privacidade.

RONDÔNIA. Portaria nº 97/2021/SETIC. Política de Segurança da Informação - PSI da SETIC. Disponível em: http://wiki.setic.ro.gov.br/lib/exe/fetch.php?media=start:docs:psi_setic_-_versao_1.0.pdf



setic.ro.gov.br

@setic.rondonia

Telefone: 69 3212 9541
Endereço: Av. Farquar, 2986 - Bairro Pedrinhas
Palácio Rio Madeira, Edifício Rio Cautário - 6º Andar
Porto Velho, RO - CEP 76801470