MINUTA

MINUTA DE RESOLUÇÃO Nº 0554083/REIT - POSIC/IFRO, DE 07 DE MAIO DE 2019

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

2019-2021

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autores
13/02/2019	1.0	Elementos textuais preliminares	Erlan, Evandro e Joilson
14/02/2019	1.1	Revisão	Comissão
27/02/2019	1.2	Definição dos Papéis	Evandro, e Joilson
28/02/2019	1.3	Revisão	Comissão
08/04/2019	1.4	Penalidades e Definição de Papéis	Presidente
10/04/2019	1.5	Revisão Geral e Definição de Papéis	Comissão
22/04/2019	1.6	Revisão Geral	Presidente
10/05/2019	1.7	Encaminhamento para ser disponibilizado para consulta publica	Presidente

REITOR

Uberlando Tiburtino Leite

COMISSÃO DE ELABORAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Joilson Dantas Siqueira Silva	DGTI / Reitoria
Ana Cristina de Souza Falcão	PROPESP / Reitoria
Cledenice Blackman	PROEN / Reitoria
Dennis Weberton Vendruscolo Gonçalves	ASCOM / Reitoria
Erlan Fonseca de Souza	DGTI / Reitoria
Evandro Souza de Paula Cordeiro	DGTI / Reitoria
Ewerton Rodrigues Andrade	Campus Porto Velho Calama
Flavia Cristina do Nascimento Anziliero	Gabinete / Reitoria
Gislaine Cristina Rodrigues de Souza	Ouvidoria
Jaqueline Almeida de Andrade	DGP / Reitoria
Jardel de Souza Pereira	PRODIN / Reitoria
John Alison Ribeiro da Costa Maia	PROAD / Reitoria
Rogério Shockness da Silva	PROEX / Reitoria

Documento assinado eletronicamente por **Joilson Dantas Siqueira Silva**, **Presidente do Grupo de Trabalho**, em 10/05/2019, às 11:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Evandro Souza de Paula Cordeiro**, **Membro da Comissão**, em 10/05/2019, às 11:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Flavia Cristina do Nascimento Anziliero**, **Membro da Comissão**, em 10/05/2019, às 14:25, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ana Cristina de Souza Falcao**, **Membro da Comissão**, em 13/05/2019, às 09:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Erlan Fonseca de Souza**, **Membro da Comissão**, em 13/05/2019, às 14:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Dennis Weberton Vendruscolo Goncalves**, **Membro da Comissão**, em 13/05/2019, às 15:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **GISLAINE CRISTINA RODRIGUES DE SOUZA**, **Membro da Comissão**, em 13/05/2019, às 17:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jaqueline Almeida de Andrade**, **Membro da Comissão**, em 14/05/2019, às 11:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jardel de Souza Pereira**, **Membro da Comissão**, em 14/05/2019, às 17:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **John Alison Ribeiro da Costa Maia**, **Membro da Comissão**, em 15/05/2019, às 16:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ewerton Rodrigues Andrade**, **Membro da Comissão**, em 16/05/2019, às 14:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0554083** e o código CRC **75A618DE**.

ANEXO I À MINUTA DE POLITICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

1. APRESENTAÇÃO

A informação é um ativo da instituição que, como equipamento, conhecimento e pessoal, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. A informação pode existir em diversas formas, podendo ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida. (ABNT NBR ISO/IEC 27002, 2005)

A Política de Segurança da Informação e Comunicação – POSIC, é essencial para que seja possível identificar riscos e ameaças que possam prejudicar o Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), seja em seu funcionamento cotidiano ou então em sua imagem.

Para esta política, o grupo de trabalho responsável pela elaboração da Política de Segurança da Informação e Comunicação estabeleceu as diretrizes necessárias para que o comitê gestor de segurança da informação possa desenvolver as ações de gestão da segurança da informação em todo o IFRO.

Dessa forma, este trabalho apresenta de forma estruturada a política que o IFRO deve seguir no que tange a Segurança da Informação e Comunicação, fruto de um trabalho participativo entre o grupo de trabalho e seus representantes de diversas áreas do IFRO.

2. INTRODUÇÃO

O que é a Política de Segurança da Informação e Comunicação?

De acordo com ABNT (2005), "Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio." Sendo assim, o Sistema de Gestão de Segurança da Informação é apoiado pelos pilares demonstrados na figura 1.

Figura 1 - Pilares da Segurança da Informação

Fonte: Adaptado de ABNT NBR ISO/IEC 27002, 2015

A Política de Segurança da Informação e Comunicação (POSIC) é um documento que contém um conjunto de normas, métodos e procedimentos, que deve ser divulgado amplamente na instituição. Deve também ser analisado e revisado criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias (FONTES, 2006). No IFRO, o Comitê Gestor de Segurança da Informação, é o responsável por garantir a viabilidade e o uso dos ativos, somente por pessoas autorizadas e que realmente necessitam delas para realizar suas funções em âmbito institucional.

Por que se aplica a POSIC?

O Decreto 9.637, de 26 de Dezembro de 2018, Institui a Política Nacional de Segurança da Informação, no âmbito da administração pública federal com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional. Diante disso, o Departamento de Segurança da Informação e Comunicações (DSIC) disciplina este tema, por meio da publicação de normas que são consideradas obrigatórias.

3. ALINHAMENTO ESTRATÉGICO

O alinhamento estratégico da POSIC 2019-2021 do IFRO é realizado por meio do atendimento aos objetivos estratégicos "Assegurar estruturas e práticas de segurança da informação" e "Fortalecer o alinhamento entre o planejamento de TI, às estratégias do IFRO e a estratégia geral de TI" demonstrados no Plano de Desenvolvimento Institucional 2018-2022 do IFRO. Esse tema, também é abordado no Plano Estratégico de TI 2014-2019 do IFRO.

Por fim, a política também possui alinhamento com documentos norteadores que extrapolam o IFRO. Dessa forma, este documento possui também a finalidade de "Garantir a Segurança da Informação e Comunicações" da Estratégia Geral de Tecnologia da Informação (EGTI) do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação). Isto contribui para a realização das seguintes iniciativas estratégicas:

- Promover o desenvolvimento de políticas de segurança da informação e comunicações.
- Estimular a adoção de práticas de gestão de incidentes de segurança da informação e comunicações.
- Implementar práticas de gerenciamento de riscos e continuidade de negócios.

4. ABRANGÊNCIA

A abrangência desta política alcança todo o IFRO, que deverão seguir as diretrizes da segurança da informação para o gerenciamento e administração segura dos seus ativos, abrangendo todos os usuários da informação, incluindo qualquer organização/instituição/empresa que possuem, possuíram

ou virão a possuir acesso às informações do IFRO e/ou fizeram ou farão uso dos recursos computacionais compreendidos na infraestrutura do IFRO.

5. ESCOPO

O escopo da Política de Segurança da Informação e Comunicação do IFRO refere-se:

- Aos aspectos estratégicos, estruturais e institucionais, preparando a base para elaboração dos demais documentos publicados pelo comitê gestor de segurança da informação como normas complementares;
- Aos requisitos de segurança humana;
- Aos requisitos de segurança física;
- Aos requisitos de segurança lógica e virtual;
- À sustentação dos procedimentos, dos processos de trabalho e dos ativos que influenciarão diretamente nos serviços oriundos da Informação e Comunicação do IFRO.

6. VIGÊNCIA, VALIDADE E ATUALIZAÇÃO

A presente política passa a vigorar a partir da data de sua publicação e será válida para o biênio 2019-2021.

O Comitê Gestor de Segurança da Informação, a fim de que a POSIC e/ou seus instrumentos normativos, não fiquem ultrapassados ou desatualizados, deve revê-la periodicamente ou quando se fizer necessário, sendo ainda obrigatória a revisão anual.

7. APROVAÇÃO E PUBLICAÇÃO

Esta política deverá ser aprovada pelo Conselho Superior do IFRO, após consulta pública e, oficializado por meio de resolução do mesmo. A POSIC e suas atualizações devem ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e colaboradores que habitualmente integram o quadro funcional do IFRO.

8. FINALIDADE

A Política de Segurança da Informação e Comunicação do Instituto Federal de Rondônia é uma declaração formal acerca do seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os envolvidos internamente e externamente ao IFRO, que podem ser:

1. Servidores;
2. Alunos;
3. Colaboradores;
4. Estagiários;
5. Prestadores de serviço que exerçam atividades no âmbito da Instituição ou;
6. Qualquer cidadão que tenha acesso a dados ou informações no âmbito do Instituto.

O seu propósito é estabelecer diretrizes gerais que servirão como base para as normas, procedimentos e instruções referentes à segurança da informação, atribuindo responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes a Instituição.

Tem como finalidade também:

- Orientar quanto a adoção de controles e processos para atendimento dos requisitos de Segurança da Informação;
- Resguardar as informações do IFRO, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade.

9. CONCEITOS E DEFINIÇÕES

Para os efeitos desta política são estabelecidos os seguintes conceitos e definições:

- **Equipe de Segurança da Informação e Comunicação**: Grupo de Trabalho responsável por assessorar a implementação das ações de segurança da informação e comunicação no âmbito da Instituição.
- **Comitê Gestor de Segurança da Informação e Comunicação**: responsável pelas ações de segurança da informação e comunicação no âmbito da Instituição.
- **Equipe de Tratamento e Resposta de Incidentes**: equipe responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança.
- **Política de Segurança da Informação e Comunicação (POSIC):** documento aprovado pela autoridade responsável da Instituição, com o objetivo de fornecer

diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

- **Ativo:** qualquer bem, tangível ou intangível, que tenha valor para a Instituição. Neles incluem-se:

a) Ativos de informação;

b) Ativos de software;

c) Ativos físicos;

d) Serviços;

e) Pessoas e suas qualificações, habilidades e experiências;

f) Reputação e a imagem da instituição;

- **Informação:** ativo principal a ser resguardado por esta política.
- **Confidencialidade:** somente pessoas devidamente autorizadas pela Instituição devem ter acesso à informação.
- **Integridade**: a informação não deve ser alterada sem autorização da Instituição.
- **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado.
- **Autenticidade:** princípio de segurança que atesta com exatidão a origem da informação e a responsabilidade pela criação ou divulgação da mesma.
- **Não-Repúdio:** garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação.
- **Risco**: a possibilidade de um ativo estar sujeito a vulnerabilidades e incidentes (ameaças explorando essas vulnerabilidades), comprometendo a continuidade das atividades de uma organização (ABNT, 2013).
- **Vulnerabilidade**: Fragilidade de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças
- **Ameaça**: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização
- **Impacto:** mudança adversa no nível obtido dos objetivos de negócios
- **Probabilidade:** estudo das chances de ocorrência de um resultado, que são obtidas pela razão entre casos favoráveis e casos possíveis
- **Falha:** Defeito ou uma condição anormal em um componente, equipamento, subsistema ou sistema, que pode impedir o seu funcionamento como planejado, uma situação chamada de fracasso
- **Criticidade**: Grau de importância que um requisito, módulo ou erro possui no sistema.
- **Incidente de segurança da informação**: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação [ISO/IEC TR 18044:2004];
- **Ataque**: Qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede.
- **Política:** intenções e diretrizes globais formalmente expressas pela direção.

10. DIRETRIZES GERAIS

Todos os envolvidos interna ou externamente ao IFRO devem observar as seguintes diretrizes gerais desta política:

- **Acesso, Proteção e Guarda da Informação:** O acesso à informação deve ser regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Instituição é considerada seu patrimônio e deve ser protegida seja ela em meio físico ou meio digital.
- **Utilização dos Recursos de Informação:** Os recursos disponibilizados são fornecidos com o propósito único de garantir o desempenho das atividades da Instituição.
- **Classificação das informações**: Para que o nível adequado de proteção para a informação seja estabelecido, é necessário que todas as informações, existentes e

futuras, sejam devidamente classificadas.

- **Gestão de Informação**: Deverão ser estabelecidas normas para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da informação que serão definidos de acordo com a classificação desta, sem prejuízo de outros cuidados que serão especificados pelo IFRO.
- **Gestão de Incidentes**: É estabelecida uma área que consiste em receber, filtrar, classificar e responder as solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências.
- **Gestão de Riscos**: É estabelecido um processo de Gestão de Risco, contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação, produzindo subsídios para a Gestão de Continuidade dos Negócios. Os riscos devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco, como ameaça, vulnerabilidade, probabilidade e impacto.
- **Plano de Continuidade:** É estabelecido um processo de medidas, regras e procedimentos definidos, que serão adotados para assegurar que as funções ou atividades críticas da Instituição possam ser mantidas ou recuperadas após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações.
- **Auditoria e Conformidade:** Deverão ser levantados regularmente os aspectos legais de segurança aos quais as atividades da Instituição estão submetidas, de forma a evitar responsabilizações decorrentes da não observância de tais aspectos por desconhecimento ou omissão.
- **Segurança Física:** Controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos da Instituição e que garantam a proteção dos recursos de forma que apenas as pessoas autorizadas tenham acesso, restringindo a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança.
- **Capacitação e Aperfeiçoamento:** Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicação.
- **Patrimônio Intelectual:** As informações, os sistemas e os métodos criados pelos servidores da Instituição, no exercício de suas funções, são patrimônios intelectuais da Instituição não cabendo a seus criadores qualquer forma de direito autoral.
- **Termo de Responsabilidade e Sigilo:** É o documento oficial que compromete colaboradores, terceirizados e prestadores de serviço com a politica de segurança da Instituição.

11. REFERÊNCIAS LEGAIS E NORMATIVAS

Para elaboração desta política de segurança da informação e comunicação, deve-se considerar as seguintes referências legais e normativas:

- Decreto nº 9.637, de 26 de Dezembro de 2018
- Instruções Normativas do Gabinete de Segurança Institucional da Presidência da República:
    - Instrução Normativa no 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
- NBR ISO/IEC 27001:2006.
- NBR ISO/IEC 27002:2006.
- NBR ISO/IEC 27003:2011
- NBR ISO/IEC 27004:2010
- NBR ISO/IEC 27005:2011.
- Lei nº 8.027 de 12 de abril de 1990
- Lei nº 8.112 de 11 de dezembro de 1990
- Decreto 1.171 de 24 de junho de 1994
- Decreto nº 7.845 de 14 de novembro de 2012
- Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da

Informação/MPOG, de 11 de setembro de 2014

- Acórdão 1603/2008 TCU-Plenário

12. DAS PENALIDADES

Em caso de descumprimento desta política de segurança e comunicação serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial o que consta:

- Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;
- Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171/1994;
- Código Penal, através do Decreto-Lei nº 2848/1940;
- Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;
- Decreto nº 7.845 que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer

13. ESTRUTURA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

A estrutura da Segurança da Informação e Comunicação do IFRO é composta por um conjunto de documentos com dois níveis hierárquicos distintos, relacionados a seguir:

- Política de Segurança da Informação e Comunicação: constituída neste documento, define a estrutura, as diretrizes, os papéis e responsabilidades referentes à segurança da informação e Comunicação;
- Normas complementares de Segurança da Informação e Comunicação: estabelecem procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos.

14. COMPETÊNCIAS E RESPONSABILIDADES

Como forma de garantir o sucesso da gestão da segurança da informação no IFRO, é necessário a definição dos papéis de todos os envolvidos, bem como suas respectivas responsabilidades conforme descrito:

- CONSUP: responsável pela aprovação da Política de Segurança da Informação e Comunicação.
- Reitor do IFRO: responsável pelo Instituto Federal, que compete:
  - Instituir Comitê Gestor de Segurança da Informação e Comunicação, denominando um Gestor de Segurança da Informação e Comunicação do IFRO e seu substituto;
  - Viabilizar o desenvolvimento dos trabalhos do Comitê Gestor de Segurança da Informação e Comunicação.
- Comitê Gestor de Segurança da Informação e Comunicação: formado pelos membros do Colégio de Dirigentes (CODIR), que compete:
  - Instituir Equipe de Segurança da Informação e Comunicação,
  - Apreciar e recomendar a política, normas e procedimentos à apreciação do Conselho Superior;
  - Coordenar a elaboração e/ou revisão da Política de Segurança da Informação e Comunicação (POSIC), normas e procedimentos relacionados;
  - Acompanhar as investigações e avaliações dos dados decorrentes de incidentes de segurança;
  - Sugerir ao reitor apuração de responsabilidades dos envolvidos nos casos de incidentes de segurança, nos termos desta política;
  - Propor programa orçamentário específico para as ações de segurança da informação e comunicação;
  - Avaliar e aprovar normas complementares de Segurança da Informação e Comunicação e de Utilização do Recursos de Informação em parceria com as respectivas áreas da instituição;

- Promover cultura de Segurança da Informação e Comunicação;
- Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República;
- Propor normas relativas à segurança da informação e comunicação.

- Gestor de Segurança da Informação e Comunicações:
  - Coordenar o Comitê Gestor de Segurança da Informação e Comunicação;
  - Acompanhar atividades da Equipe de Segurança da Informação e Comunicações.
  - Propor programa orçamentário específica junto com o Comitê Gestor para capacitação da equipe de segurança e para as ações de segurança da informação e comunicação;
  - Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional;
  - Propor normas relativas à segurança da informação e comunicação
  - Definir o plano de continuidade da Segurança da Informação e Comunicação
  - Coordenar junto ao responsável dos setores que seja realizada a Classificação das Informações para garantir que nenhum dado seja divulgado indevidamente

- Equipe de Segurança da Informação e Comunicação:
  - Os membros da equipe de segurança da informação e Comunicação terão mandato de 01 ano a partir da publicação da portaria de designação, sendo permitida uma recondução por igual período.
  - Elaborar, atualizar e divulgar a normas complementares relativas a esta Política de Segurança da Informação.
  - Apoiar ativamente o cumprimento da Política de segurança da Informação
  - Auxiliar o Comitê Gestor de Segurança da Informação e Comunicação em suas deliberações
  - Conduzir a gestão tática e operação da Segurança da Informação
  - Criar, revisar e atualizar normas e procedimento de Segurança da Informação
  - Apoiar na seleção de controles e soluções técnicas
  - Efetuar a Gestão dos incidentes de Segurança da Informação, garantindo tratamento e resolução adequados;
  - Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação e Comunicação;
  - Auditar e monitorar atividades dos usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário;
  - Promover cultura de Segurança da Informação e Comunicação;
  - Implantar o plano de continuidade de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre
  - Propor o Termo de Responsabilidade e Sigilo a ser adotado pela instituição

- Equipe de Tratamento e Resposta a Incidentes:
  - Auditar e monitorar atividades dos usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário
  - Promover cultura de Segurança da Informação e Comunicação;
  - Executar o Plano de Continuidade da instituição no caso de situação de falhas e desastres.

15. DAS DISPOSIÇÕES FINAIS

Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicação do IFRO devem ser direcionados ao Comitê Gestor de Segurança da Informação.