Ministério da Educação
Universidade Federal de Alfenas
Rua Gabriel Monteiro da Silva, 700 - Bairro centro, Alfenas/MG - CEP 37130-001
Telefone: (35) 3701-9000 - http://www.unifal-mg.edu.br

Resolução Nº 02/2024, DE 05 DE novembro DE 2024

Aprova o Plano de Gestão de Incidentes de Segurança da Informação e Comunicação e a Política de Confidencialidade e Manutenção do Sigilo no âmbito da UNIFAL-MG

O Comitê de Governança Digital (CGD) da Universidade Federal de Alfenas – UNIFAL-MG, no uso de suas atribuições regimentais,

CONSIDERANDO o constante dos autos do processo nº 23087.010451/2024-23,

R E S O L V E :

Art. 1º Aprovar, na forma do anexo SEI Nº 1386270, o Plano de Gestão de Incidentes de Segurança da Informação e Comunicação no âmbito da UNIFAL-MG;

Art. 2º Aprovar, na forma do anexo SEI Nº 1386271, a Política de Confidencialidade e Manutenção do Sigilo no âmbito da UNIFAL-MG;

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

Assinado Eletronicamente

SANDRO AMADEU CERVEIRA

Presidente do Comitê de Governança Digital

Documento assinado eletronicamente por **Sandro Amadeu Cerveira**, **Reitor**, em 11/12/2024, às 14:38, 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.unifal-mg.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1386267** e o código CRC **A5C5B699**.

Plano de Gestão de Incidentes de Segurança da Informação e Comunicação

ETIR/UNIFAL-MG

1 - Apresentação

O objetivo do Plano de Gestão de Incidentes de Segurança da Informação e Comunicação – ETIR/UNIFAL-MG é garantir um tratamento e resposta eficazes aos eventos de segurança da informação e comunicação que afetam a disponibilidade, integridade e/ou confidencialidade associados aos ativos e sistemas de informação da Universidade Federal de Alfenas - UNIFAL-MG. Além disso, deve contribuir para que a comunicação de um incidente seja rápida e eficiente de forma a permitir correções em tempo hábil e aceitável, limitar o seu impacto, proteger os ativos e as informações, organizar os recursos necessários para lidar com eventos como: *malwares* (códigos maliciosos), acesso não autorizado a informações, uso não autorizado de serviços, ataques de negação de serviço, fraudes, entre outros.

2 – Termos e Definições

Para fins deste Plano de Gestão, serão considerados os conceitos constantes do Glossário de Segurança da Informação, aprovado e atualizado por portaria do Gabinete de Segurança Institucional da Presidência da República, bem como os termos e definições abaixo:

- **Ativo**: tudo que tenha valor para a UNIFAL-MG e para as atividades institucionais, como informações, softwares, hardwares, pessoas, processos e serviços;
- **Segurança da Informação e Comunicação (SIC)**: preservação da confidencialidade, integridade e disponibilidade da informação, da comunicação e dos ativos institucionais contra quaisquer tipos de ameaças, visando garantir a continuidade das atividades, a minimização dos riscos e a maximização da eficiência e da efetividade das ações; além disso, pode envolver outras propriedades, como autenticidade, não-repúdio e confiabilidade;
- **Evento de SIC**: evento adverso que tenha a probabilidade de comprometer as operações normais de um ativo ou ameaçar a segurança da informação e comunicação;
- **Ameaça**: possibilidade de qualquer evento que explore vulnerabilidades, causando potenciais incidentes indesejados, que possam resultar em danos para os ativos da UNIFAL-MG;
- **Incidente de SIC**: um único evento ou uma série de eventos indesejados ou inesperados de segurança da informação, confirmada ou sob suspeita, que tenham uma grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação e comunicação;
- **Plano de Gestão de Incidentes de SIC**: documento escrito que estabelece a abordagem para tratar e gerenciar incidentes de SIC, definir funções, responsabilidades e requisitos para responder às notificações de incidentes de SIC;

- **Procedimentos de Resposta a Incidentes de SIC**: documentos escritos com as ações a serem tomadas ao tratar e resolver os incidentes de SIC.

3 – Papeis e Responsabilidades

Função	Responsabilidades	Responsável
Gerente de Segurança da Informação	Responsável pelas ações de segurança da informação e comunicação na UNIFAL-MG e Coordenador da ETIR/UNIFAL-MG (ver regimento interno do NTI)	Gerente de Segurança da Informação em exercício
Gerente de Desenvolvimento de Sistemas e Gestão da Informação	Responsável pelo desenvolvimento e manutenção de sistemas e gestão de bancos de dados na UNIFAL-MG (ver regimento interno do NTI)	Gerente de Desenvolvimento de Sistemas e Gestão da Informação em exercício
Gerente de Redes e Infraestrutura	Responsável pela gestão da infraestrutura de redes e serviços na UNIFAL-MG (ver regimento interno do NTI)	Gerente de Redes e Infraestrutura em exercício
Gerente de Suporte Técnico ao Usuário	Responsável pela manutenção do parque computacional e suporte ao usuário na UNIFAL-MG (ver regimento interno do NTI)	Gerente de Suporte Técnico ao Usuário em exercício
Diretor do Núcleo de Tecnologia da Informação	Responsável pela Administração do Núcleo de Tecnologia da Informação da UNIFAL-MG (ver regimento interno do NTI)	Diretor do Núcleo de Tecnologia da Informação em exercício

4 – Notificação

4.1 – Notificações Recebidas

As notificações acerca de eventos de SIC serão recebidas através dos seguintes canais:

- **Sistema de Ordens de Serviço – SOS da UNIFAL-MG (preferencialmente)**: https://sistemas.unifal-mg.edu.br/app/gerenciamentoordemservico
- **Telefone:** a ser divulgado no site da ETIR;
- **e-mail**: etir@unifal-mg.edu.br
- **Página Web**: https://www.unifal-mg.edu.br/etir (com redirecionamentos para os endereços: /csirt, /seguranca e /security)

- **Alertas automáticos**: Análise ativa de servidor centralizado de LOGs, servidores de monitoramento e afins.

Observação: todas as notificações recebidas serão cadastradas no SOS para a manutenção de base de dados de eventos e de conhecimento, relatórios gerenciais e estatísticos.

4.2 – Notificações Enviadas

Todas as notificações acerca de eventos de SIC serão enviadas pelo Coordenador da ETIR/UNIFAL-MG através do e-mail: etir@unifal-mg.edu.br.

As notificações enviadas, quando aplicável, devem ser copiadas para os endereços de e-mail do CAIS/RNP, do CERT.br, do GSI/PR e demais CSIRTs de coordenação e outros órgãos de monitoramento que vierem a ser legalmente instituídos.

4.3 – Responsabilidades

As notificações acerca de eventos de SIC serão recebidas e deverão ser enviadas pelo Coordenador da ETIR/UNIFAL-MG. No caso do recebimento de notificações por qualquer outro membro da ETIR/UNIFAL-MG, este deverá efetuar o cadastro da notificação no SOS para que o coordenador da ETIR/UNIFAL-MG possa tomar as devidas providências com relação à resolução do problema.

5 – Registro

5.1 – Sistema de Gerenciamento de Incidentes

Todas as notificações acerca de eventos de SIC serão registradas no SOS a fim de se manter uma base de dados dos eventos e o histórico das ações realizadas no seu tratamento.

5.2 – Identificador da Notificação

O ID da ordem de serviço cadastrada no SOS (ticket) será utilizado para identificar unicamente uma notificação. O título/assunto de todas as comunicações e/ou divulgações será composto pelas seguintes informações: o ID da notificação, precedido pela inscrição “ETIR” (entre [ ]), o tipo de notificação e a informação se a notificação foi enviada, emitida ou fechada no sistema. Todas as ações referentes à notificação deverão ser informadas no SOS e a cada uma delas será emitida uma comunicação sobre o seu andamento.

5.3 - Atribuição

A notificação será atribuída para um dos membros da ETIR/UNIFAL-MG, de acordo com a sua área de atuação, observando a pertinência com o evento de SIC notificado. O coordenador da ETIR/UNIFAL-MG acompanhará o andamento da resolução do evento e poderá solicitar, também, acompanhamento e colaboração por parte da Gerência de Segurança da Informação do NTI – GSI/NTI, de outras Gerências, Unidades e/ou áreas de TI dos outros *campi* da UNIFAL-MG.

5.4 – Resposta Padrão Inicial

O texto de resposta inicial da notificação deve seguir o padrão descrito abaixo:

ID: 123456 Assunto: Phishing enviado por e-mail Descrição: Phishing recebido no meu e-mail institucional.   Para mais informações acesse o Sistema de Ordens de Serviço.   Este é um e-mail automático, favor não responder. Caso seja necessária uma resposta à Ordem de Serviço, favor utilizar o campo de respostas do SOS.

6 – Triagem

6.1 – Validação da Notificação

As notificações deverão estar de acordo com o que consta na Portaria de instituição da ETIR/UNIFAL-MG, ou seja, o escopo de abrangência da ETIR/UNIFAL-MG.

Toda notificação de evento de SIC registrada no SOS deverá ser avaliada pela ETIR/UNIFAL-MG de forma a validá-la ou não como um evento de segurança da informação. Essa validação será feita pelo Coordenador da ETIR/UNIFAL-MG.

Caso a notificação seja avaliada como um evento de SIC, deverão ser verificadas se as seguintes informações estão presentes na notificação:

- **Remetente Válido**: se o e-mail, telefone ou outro meio de contato utilizado pelo remetente da notificação é válido;

- **Descrição do Evento**: se a notificação enviada se refere de fato a um evento de SIC (incidente ou vulnerabilidade);
- **Endereço IP de Origem**: se existe na notificação informações sobre o endereço IP (IPv4 e/ou IPv6) do host que originou o evento de SIC;
- **Endereço IP de Destino**: se existe na notificação informações sobre o endereço IP (IPv4 e/ou IPv6) do host que sofreu o evento de SIC;
- **Registro do Tempo**: se existem informações na notificação acerca da data e hora da ocorrência do evento de SIC, no formato GMT, com indicação explícita do fuso-horário (timezone);
- **Informações sobre Serviços, Protocolos e Portas**: se existem informações na notificação sobre o tipo do protocolo (IP, TCP, UDP, etc) e portas de origem e destino utilizadas na notificação do incidente, bem como sobre os serviços (HTTP, SMTP, P2P, etc) envolvidos na notificação do evento de SIC;
- **LOGs ou Evidências**: a existência de LOGs ou outras evidências na notificação do evento de SIC.

6.2 – Ações Pós-Triagem

Após a realização da avaliação das informações presentes na notificação, as seguintes ações deverão ser realizadas, de acordo com cada cenário:

Cenário	Ação
A notificação não é um evento de SIC	Será descartada. Ticket com status “Cancelada”.
A notificação tem remetente inválido	Será descartada. Ticket com status “Cancelada”.
A notificação não tem informações de endereços IP de origem e/ou destino	Será descartada. Ticket com status “Cancelada”.
A notificação não tem informações de data, hora ou timezone	Será descartada. Ticket com status “Cancelada”.
A notificação não tem informações sobre Serviços, Protocolos e Portas	Será descartada. Ticket com status “Cancelada”.
A notificação necessita de mais informações para identificação do incidente	Será feita uma solicitação ao remetente para que este envie mais informações que ajudem na identificação e resolução do evento; o ticket ficará aguardando estas novas informações e depois seguirá o restante do fluxo de tratamento. Ticket com status “Emitida[1]”.
A notificação foi originada em outra organização com contatos de segurança desconhecidos	Caso necessário o ticket seguirá o restante do fluxo de tratamento, senão, será cancelado. Ticket com status “Emitida” ou “Cancelada”, dependendo da situação.

[1] A ordem de serviço (ticket) com status “Emitida” indica que ela está em atendimento por um técnico que foi alocado para seguir o fluxo de tratamento da notificação.

A notificação foi originada em outra organização com contatos de segurança conhecidos	Será reencaminhada para o respectivo responsável com a maior quantidade possível de informações que ajudem na resolução do evento; caso necessário, o ticket seguirá o restante do fluxo de tratamento, senão, será fechado. Ticket com status “Emitida” ou “Fechada”, dependendo da situação.
A notificação é válida, com todas as informações necessárias e dentro do escopo de abrangência da ETIR/UNIFAL-MG	O ticket seguirá o restante do fluxo de tratamento. Ticket com status “Emitida”.

6.3 – Responsabilidades

A triagem das notificações será feita pelo Coordenador da ETIR/UNIFAL-MG.

7 – Classificação

7.1 – Categorias de Tipo

Todo evento de SIC deverá ser classificado de forma unívoca, utilizando os parâmetros de tipo, de acordo com a tabela[2] abaixo e, se necessário, com um subtipo para melhor identificar o evento:

Categoria	Tipo	Descrição
Conteúdo Abusivo	SPAM	Mensagem em massa não solicitada, ou seja, enviada sem a permissão do destinatário. Geralmente contendo propaganda.
	Discurso de Ódio, Difamatório, Discriminatório (racismo, homofobia, xenofobia, bullying, etc)	Cyber bullying ou qualquer conteúdo de ódio, difamatório, discriminatório contra indivíduos ou grupos.
	Pedofilia (Pornografia ou Exploração Infantil), Assédio Sexual, Apologia às Drogas ou à Violência	Conteúdo sobre pedofilia, assédio sexual, apologia às drogas ou à violência.

[2] Baseado na metodologia de classificação da ENISA: Reference Incident Classification Taxonomy - Task Force Status and Way Forward – Jan/2018 - Disponível em: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy e atualizações do grupo de trabalho: https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

Código Malicioso	Sistemas Infectados (worm, vírus, trojan, spyware, scripts, rootkits, etc)	Qualquer sistema infectado por um malware (computador, celular, etc). Na maioria das vezes se refere a uma conexão com um servidor de comando e controle.
	Servidores de Comando e Controle (C2 Servers)	Servidor de comando e controle conectado ao sistema infectado.
	Distribuição de Malwares	URL usada para a distribuição de malwares
	Configuração de Malwares	URL usada para a distribuição de arquivos de configuração de malwares.
Prospecção de Informação	Varredura de IPs, Serviços, Protocolos, Portas, etc (scanning)	Ataques que enviam solicitações a um sistema para descobrir pontos fracos. Isso também inclui processos de teste para coletar informações sobre hosts, serviços e contas.
	Escuta de Tráfego de Rede (sniffing)	Monitoramento e registro de tráfego de rede (redes de dados, escutas telefônicas, etc).
	Engenharia Social	Obtenção de informações sigilosas de pessoas se utilizando de manipulação, confiança e boa fé.
Tentativas de Intrusão	Exploração de Vulnerabilidades Conhecidas	Tentativa de comprometimento ou acesso de um sistema ou interrupção de um serviço através de ataques que explorem vulnerabilidades conhecidas. (estouro de buffer, backdoor, XSS, etc)
	Tentativas de Login	Tentativas de acesso não-autorizado a contas de usuários em serviços (SSH, Webmail, FTP, etc), usando força bruta (ataques de dicionários) ou não.
	Ataques Novos	Ataques usando técnicas desconhecidas ou novas.
Intrusão/Invasão	Comprometimento de Conta de Administrador	Ataque onde o invasor consegue privilégios administrativos ao sistema.

	Comprometimento de Conta de Usuário	Ataque onde o invasor consegue acesso a contas de usuários ou serviços.
	Comprometimento de Aplicação ou Serviço	Comprometimento de sistema ou aplicação através da exploração de vulnerabilidades conhecidas ou desconhecidas de software.
	Arrombamento (invasão, vandalismo)	Invasão ou vandalismo físico ao prédio do datacenter.
Indisponibilidade de Serviço ou Informação	Negação de Serviço (DoS, DDoS, etc)	Ataque que indisponibiliza serviços ou informações, através do envio massivo de requisições ao servidor, exaurindo recursos de hardware, software ou conectividade.
	Configuração Incorreta	Configuração incorreta de software, resultando em problemas de disponibilidade de serviço ou informação.
	Sabotagem	Sabotagem física (corte de fios, desligamento intencional de energia, incêndio criminoso, etc).
	Interrupção	Indisponibilidade causada por ações locais (destruição, interrupção do fornecimento de energia, etc), defeitos em equipamentos, erro humano, desastres naturais.
Segurança da Informação	Acesso não Autorizado à Informação	Utilizando credenciais de acesso a sistemas roubadas através de interceptação de tráfego, força bruta, engenharia social, etc. Não envolve comprometimento de sistemas. Não ocorre a modificação da informação.
	Alteração não Autorizada de Informação	Utilizando credenciais de acesso roubadas, encriptação de dados através de ransomware, etc.
	Perda de Dados	Causada por falha no disco rígido ou roubo físico.

Fraude	Uso não Autorizado de Recursos	Utilizar recursos de forma não autorizada (correntes de e-mail, servidores de jogos ou para fins lucrativos particulares, etc).
	Violação de Direitos Autorais	Cópia, venda, instalação, download ou distribuição de material não licenciado ou protegido por direitos autorais.
	Fingir ou Falsificar Identidade ou Instituição	Ataque no qual uma entidade assume ilegitimamente a identidade de outra para obter qualquer tipo de informação, recurso ou vantagem (e-mails falsos, páginas falsas, etc).
	Phishing	Fazer se passar por outra pessoa, grupo, setor, departamento ou instituição para persuadir o usuário a revelar credenciais de acesso privadas. Esse tipo de ataque geralmente se refere a uma URL, muitas vezes enviada por e-mail, contendo um formulário usado para capturar as credenciais de acesso privadas do usuário.
Vulnerabilidades	Criptografia Fraca	Serviços publicamente acessíveis que oferecem criptografia fraca (servidores web suscetíveis a ataques POODLE/FREAK, etc).
	Amplificação de DDoS	Serviços publicamente acessíveis que podem ser utilizados na reflexão/ampliação de ataques DdoS (DNS Resolvers abertos, servidores NTP com o MONLIST ativado, etc).

	Disponibilidade de Serviços Indesejados e Potencialmente Perigosos	Serviços publicamente acessíveis e potencialmente perigosos (Telnet, RDP, VNC, etc).
	Divulgação de Informação	Serviços publicamente acessíveis que divulgam informações confidenciais (SNMP, Redis, etc).
	Sistema Vulnerável	Um sistema vulnerável a certos ataques (configuração errada de cliente de proxy – WPAD, sistemas operacionais desatualizados, etc).
Outros	Sem Categoria	Todos os incidentes que não se encaixam em uma das categorias especificadas devem ser colocados nessa classe ou o incidente não é categorizado. Categorização desconhecida ou indeterminada.
Teste	Teste	Destinado a testes.

7.2 – Categorias de Criticidade

Toda notificação de evento de SIC registrada deverá ter atribuída a ela, de forma unívoca, uma das categorias de criticidade e respectivo tempo para o atendimento definidos na tabela abaixo:

Criticidade	Descrição	Tempo para Atendimento
Baixa	Eventos de SIC que não impactam os serviços e atividades principais da UNIFAL-MG.	1 semana
Média	Eventos de SIC que podem trazer impactos iminentes, diretos ou indiretos, à operação dos serviços e atividades principais da UNIFAL-MG.	48 horas

Alta	Eventos de SIC que afetam a disponibilidade, integridade e confidencialidade dos serviços e atividades principais da UNIFAL-MG.	8 horas úteis

7.3 – Definição de Criticidade por Evento de SIC

Os eventos de SIC devem ter sua criticidade definidos de acordo com os critérios da tabela abaixo:

Categoria	Tipo	Criticidade
Conteúdo Abusivo	SPAM (enviado através de contas de usuários da UNIFAL-MG)	Alta
	Discurso de Ódio, Difamatório, Discriminatório (racismo, homofobia, xenofobia, bullying, etc)	Alta
	Pedofilia (Pornografia ou Exploração Infantil), Assédio Sexual, Apologia às Drogas ou à Violência	Alta
Código Malicioso	Sistemas Infectados (worm, vírus, trojan, spyware, scripts, rootkits, etc)	Média
	Servidores de Comando e Controle (C2 Servers)	Alta
	Distribuição de Malwares	Alta
	Configuração de Malwares	Média
Prospecção de Informação	Varredura de IPs, Serviços, Protocolos, Portas, etc (scanning)	Baixa
	Escuta de Tráfego de Rede (sniffing)	Alta
	Engenharia Social	Alta
Tentativas de Intrusão	Exploração de Vulnerabilidades Conhecidas	Baixa
	Tentativas de Login	Baixa
	Ataques Novos	Baixa
Intrusão/Invasão	Comprometimento de Conta de Administrador	Alta
	Comprometimento de Conta de Usuário	Alta
	Comprometimento de Aplicação ou Serviço	Alta
	Arrombamento (invasão, vandalismo)	Alta
Indisponibilidade de Serviço ou Informação	Negação de Serviço (DoS, DDoS, etc)	Alta
	Configuração Incorreta	Alta

	Sabotagem	Alta
	Interrupção	Alta
Segurança da Informação	Acesso não Autorizado à Informação	Alta
	Alteração não Autorizada de Informação	Alta
	Perda de Dados	Ala
Fraude	Uso não Autorizado de Recursos	Baixa
	Violação de Direitos Autorais	Baixa
	Fingir ou Falsificar Identidade ou Instituição	Média
	Phishing	Alta
Vulnerabilidades	Criptografia Fraca	Média
	Amplificação de DDoS	Média
	Disponibilidade de Serviços Indesejados e Potencialmente Perigosos	Média
	Divulgação de Informação	Alta
	Sistema Vulnerável	Média
Outros	Sem Categoria	Baixa
Teste	Teste	Baixa

7.4 – Categorias de Status

Toda notificação de evento de SIC registrada deverá ter seu status atribuído e atualizado no decorrer do seu processo de tratamento de acordo com as categorias definidas na tabela abaixo:

Status	Descrição
Aberta	Notificação aberta cujo tratamento ainda não foi iniciado.
Emitida	Notificação aberta cujo tratamento já foi iniciado.
Fechada	Notificação tratada e resolvida.
Cancelada	Notificação cujo tratamento não é possível de ser realizado ou que não se configura evento de SIC.

7.5 – Responsabilidades

A classificação dos eventos de SIC será feita pelo Coordenador da ETIR/UNIFAL-MG.

8 – Tratamento

8.1 – Verificação da Origem do Evento de SIC

Antes de se iniciar as ações de tratamento do evento de segurança, deve-se validar a origem deste, e executar as respectivas ações:

Origem	Ação
Evento de SIC interno (reclamante interno e incidente interno)	Manter contato com o reclamante; Notificar os CSIRTs de coordenação, quando aplicável; Tratar incidente;
Origem na UNIFAL-MG (com contatos de destino conhecidos)	Manter contato com o reclamante, quando aplicável; Notificar o(s) CSIRT(s) de destino, quando aplicável; Notificar os CSIRTs de coordenação, quando aplicável; Tratar incidente;
Origem na UNIFAL-MG (com contatos de destino desconhecidos)	Manter contato com o reclamante, quando aplicável; Notificar os CSIRTs de coordenação, quando aplicável; Tratar incidente;
Origem em Outra(s) Instituição(ões) (com contatos conhecidos)	Manter contato com o reclamante, quando aplicável; Notificar o(s) CSIRT(s) de origem, quando aplicável; Notificar os CSIRTs de coordenação, quando aplicável; Tratar incidente;
Origem em Outra(s) Instituição(ões) (com contatos desconhecidos)	Manter contato com o reclamante, quando aplicável; Notificar os CSIRTs de coordenação, quando aplicável; Tratar incidente;

8.1.1 – Informações da Notificação do Evento de SIC

Ao se enviar uma notificação ao domínio responsável pelo IP de origem do evento de SIC, devem ser inseridas as seguintes informações na mensagem:

- **Identificação do Endereço IP de Origem**: endereço IP (IPv4 e/ou IPv6) que originou o evento de SIC. Origem do ataque;
- **Identificação do Endereço IP de Destino**: endereço IP (IPv4 e/ou IPv6) que sofreu o evento de SIC. Destino do ataque;
- **Identificação de Serviços, Protocolos e Portas**: informações sobre o tipo do protocolo (IP, TCP, UDP, etc) e portas de origem e destino utilizadas no ataque, bem como sobre os serviços (HTTP, SMTP, P2P, etc) envolvidos no evento de SIC;
- **Registro do Tempo**: informações acerca da data e hora da ocorrência do evento de SIC, no formato GMT, com indicação explícita do fuso horário local (*timezone*).
- **Descrição do Evento**: breve descrição do evento de SIC, contendo o tipo do ataque, motivação aparente e outras características relevantes;
- **LOGs ou Evidências**: porções de LOGs, prints de telas, códigos de erro e/ou outros registros que evidenciem a ocorrência do evento de SIC.

8.1.2 – Envio da Notificação do Evento de SIC

As notificações dos eventos de SIC deverão ser enviadas conforme item 4.2.

8.2 – Preservação de Evidências

No início do processo de tratamento do evento de SIC, a ETIR/UNIFAL-MG deve executar ações de preservação de evidências, provas e registros de auditoria.

Para isso, a ETIR/UNIFAL-MG deve executar procedimentos conforme descrito no documento Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de SIC, o qual é baseado na Norma Complementar 21/IN01/DSIC/GSIPR.

8.3 – Procedimentos de Resolução

Todos os procedimentos operacionais para a resolução de cada evento de SIC deverão ser documentados e atualizados pela equipe da ETIR/UNIFAL-MG, no seu Wiki, com acesso restrito apenas aos seus membros, com o devido cuidado para não expor informações que possam prejudicar ativos da UNIFAL-MG e farão parte integral deste Plano de Gestão.

Cada procedimento deverá conter a descrição do incidente, o procedimento a ser seguido para a resolução do problema e o seu responsável (conforme Anexo I - Exemplo de Definição de Procedimento). Estes procedimentos devem ser criados baseando-se no fluxo definido a seguir:

8.3.1 – Fluxo de Resolução

8.3.1.1 – Análise dos Dados da Notificação

Em cada procedimento, a ETIR/UNIFAL-MG deve documentar quais as fontes internas de registro de informações existentes devem ser usadas para relacionar com os dados presentes na notificação. Essas fontes podem ser LOGs de roteadores, de firewall, de proxies, de servidores web, de servidores de autenticação, de DNS, de DHCP, de e-mail, entre outros, informações de provedores de acesso ou conteúdo, referências anteriores em casos de reincidência, de forma a obter o máximo de informações necessárias para a resolução do incidente.

8.3.1.2 – Pesquisa da Solução do Evento SIC

Em cada procedimento, a ETIR/UNIFAL-MG deve documentar todas as referências (seja de repositório interno do banco de conhecimento ou sites externos) utilizadas nas quais são baseadas as ações de resolução do evento de SIC.

8.3.1.3 – Aplicação da Solução/Mitigação do Evento de SIC

Em cada procedimento, a ETIR/UNIFAL-MG deve documentar todas as tarefas a serem executadas para realizar a mitigação do evento de SIC (ou seja, cessar ou diminuir os impactos ocasionados pelo evento), bem como as tarefas relativas ao restabelecimento do ambiente ao estado anterior à ocorrência do evento de SIC, incluindo o tratamento das vulnerabilidades que ocasionaram o evento.

8.3.1.4 – Validação da Resolução

Em cada procedimento, a ETIR/UNIFAL-MG deve documentar quais são os critérios definidos para realizar a validação do restabelecimento do ambiente ao estado anterior à ocorrência do evento de SIC.

8.3.2 – Tratamento das Vulnerabilidades

A ETIR/UNIFAL-MG deve documentar, notificar e dar suporte aos responsáveis com relação às vulnerabilidades identificadas durante o processo de tratamento do evento de SIC, de modo a evitar a repetição do evento, garantindo a confiança da operação normal dos serviços computacionais da UNIFAL-MG.

8.3.3 – Lista de Procedimentos

Os procedimentos para a resolução de cada evento de SIC deverão ser documentados conforme item 8.3.

8.4 – Responsabilidades

A responsabilidade pelo tratamento do incidente é do membro da ETIR/UNIFAL-MG que foi atribuído para a resolução da notificação, conforme item 5.3.

9 – Fechamento e Resposta

Após o tratamento do evento de SIC, a ETIR/UNIFAL-MG deve fechar o ticket correspondente à notificação e enviar uma resposta ao remetente da notificação (reclamante) dando uma breve explicação sobre a resolução do problema.

Além disso, havendo recomendações a serem feitas aos usuários, administradores de sistemas ou a outras equipes de segurança, estas devem ser feitas no processo de fechamento do incidente.

9.1 – Encerramento do Ticket

Após o tratamento do evento de SIC, deve-se alterar o status ticket da notificação do incidente para “Fechado”.

9.1.1 – Responsabilidades

A responsabilidade pelo fechamento do ticket é do membro da ETIR/UNIFAL-MG que foi atribuído para a resolução da notificação, conforme item 5.3.

9.2 – Resposta Final à Notificação

Ao encerrar o ticket correspondente à notificação no sistema, deve-se enviar uma resposta ao remetente da notificação (reclamante), informando o encerramento do tratamento do incidente. A resposta deve ser enviada através do e-mail da ETIR/UNIFAL-MG (conforme item 4.2). O texto da resposta final deve seguir o padrão descrito abaixo:

ID: 123456

Assunto: Phishing enviado por e-mail

Descrição: Phishing recebido no meu e-mail institucional.

A ETIR/UNIFAL-MG realizou o tratamento da notificação recebida, registrada pelo identificador [ID da OS], relacionado a [ASSUNTO DO EMAIL DE NOTIFICAÇÃO]. Foram realizadas ações para identificar e tratar a atividade maliciosa, bem como para corrigir possíveis falhas e vulnerabilidades existentes.

Recomendamos que [RECOMENDAÇÕES, CASO SE APLIQUEM].

Nos colocamos à disposição para qualquer dúvida ou novas solicitações.

Atenciosamente,

ETIR/UNIFAL-MG

Para mais informações acesse o Sistema de Ordens de Serviço.

Este é um e-mail automático, favor não responder. Caso seja necessária uma resposta à Ordem de Serviço, favor utilizar o campo de respostas do SOS.

9.3 – Lições Aprendidas

Ao encerrar o ticket, o processo de tratamento do evento de SIC deverá ser avaliado para se verificar a eficácia das soluções adotadas e do processo de tratamento. As falhas e os recursos inexistentes ou insuficientes devem ser relacionados e documentados, para que sejam providenciados em futuras ocasiões.

9.3.1 – Responsabilidades

Cabe ao Coordenador da ETIR/UNIFAL-MG organizar reuniões com o intuito de disseminação e alinhamento das lições aprendidas. Tais reuniões, caso sejam necessárias, ocorrerão logo após o fechamento de uma notificação ou quando solicitadas por algum membro.

Anexo I - Exemplo de Definição de Procedimento

Este anexo faz parte integral do documento Plano de Gestão de Incidentes de Segurança da Informação e Comunicação da ETIR/UNIFAL-MG.

Exemplo de definição de procedimento operacional para a resolução de evento de SIC:

Descrição do Incidente:

Phishing

Procedimentos Operacional para a Resolução do Incidente:

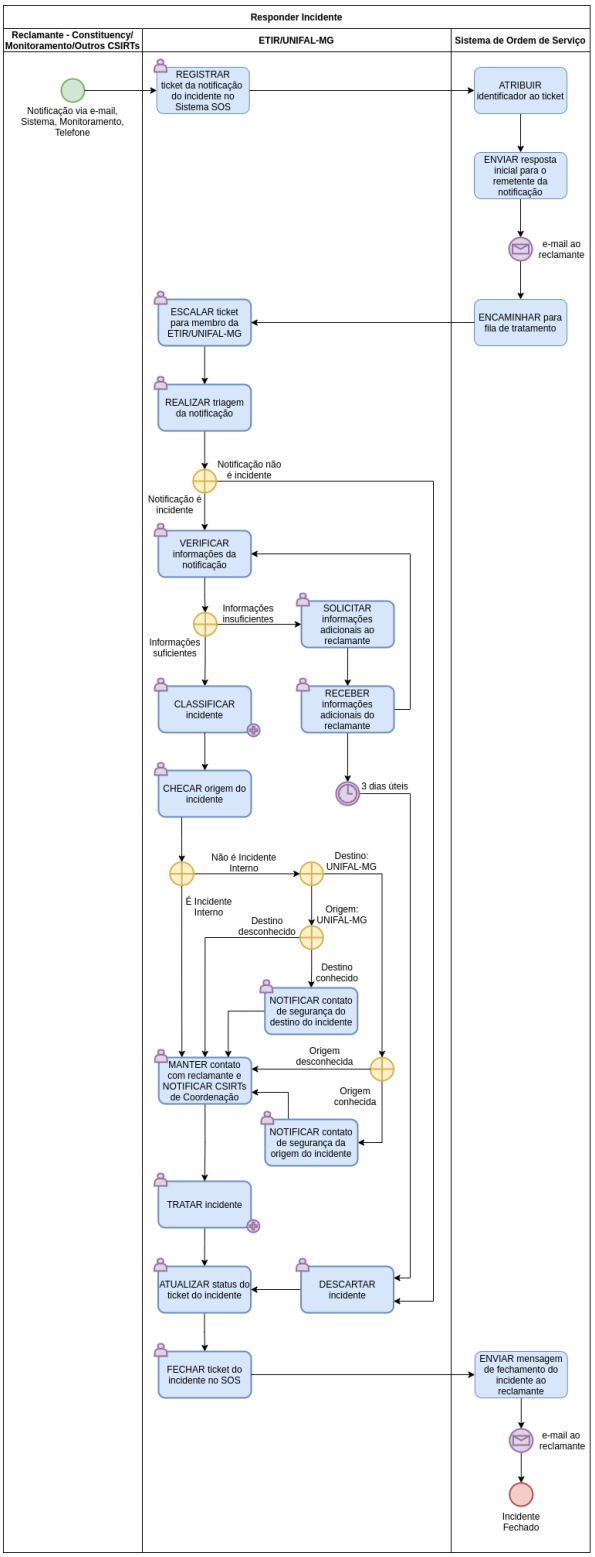
- Phishing recebido pela UNIFAL-MG:
    - Identificar a origem do phishing;
    - Identificar link(s) para captura de dados na mensagem;
    - Bloquear link(s) no firewall;
    - Solicitar a remoção do(s) link(s) ao site de origem;
    - Reportar o evento aos CSIRTs de coordenação;
- Phishing enviado pela UNIFAL-MG:
    - Identificar a conta de usuário utilizada para envio do Phishing;
    - Bloquear a conta de usuário;
    - Identificar link(s) para captura de dados na mensagem;
    - Bloquear link(s) no firewall;
    - Solicitar a remoção do(s) link(s) ao site de origem;
    - Contatar o usuário da conta para maiores esclarecimentos sobre o caso;
    - Caso a conta tenha sido invadida, solicitar a troca imediata da senha e desbloquear a conta;
    - Caso a conta não tenha sido invadida e o phishing tenha sido enviado deliberadamente pelo usuário da conta, manter a conta bloqueada e enviar o caso para o CGD;
    - Verificar/retirar o IP/domínio do servidor de e-mails da UNIFAL-MG de blacklists de bloqueio;
    - Reportar o evento aos CSIRTs de coordenação;

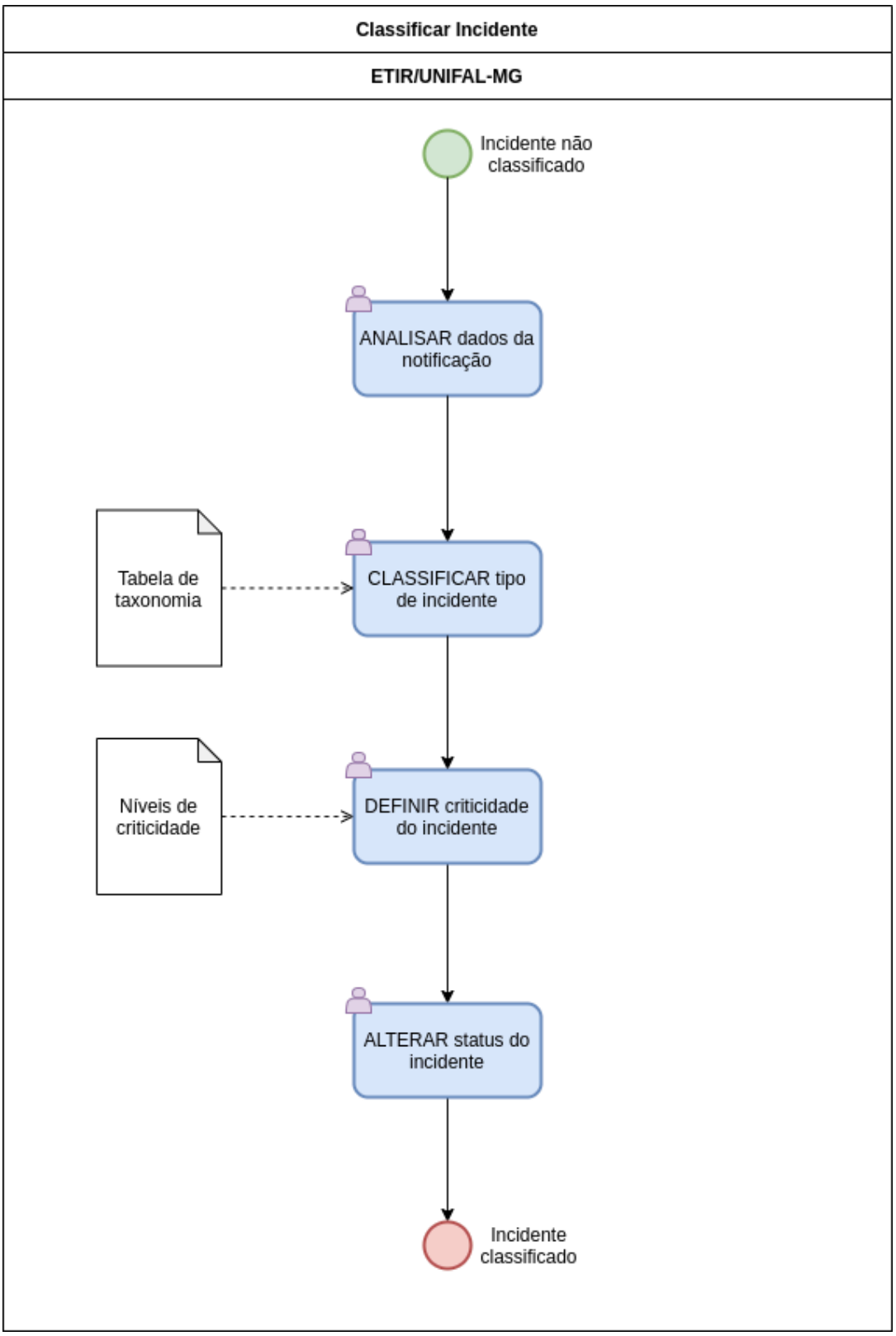
Responsável:

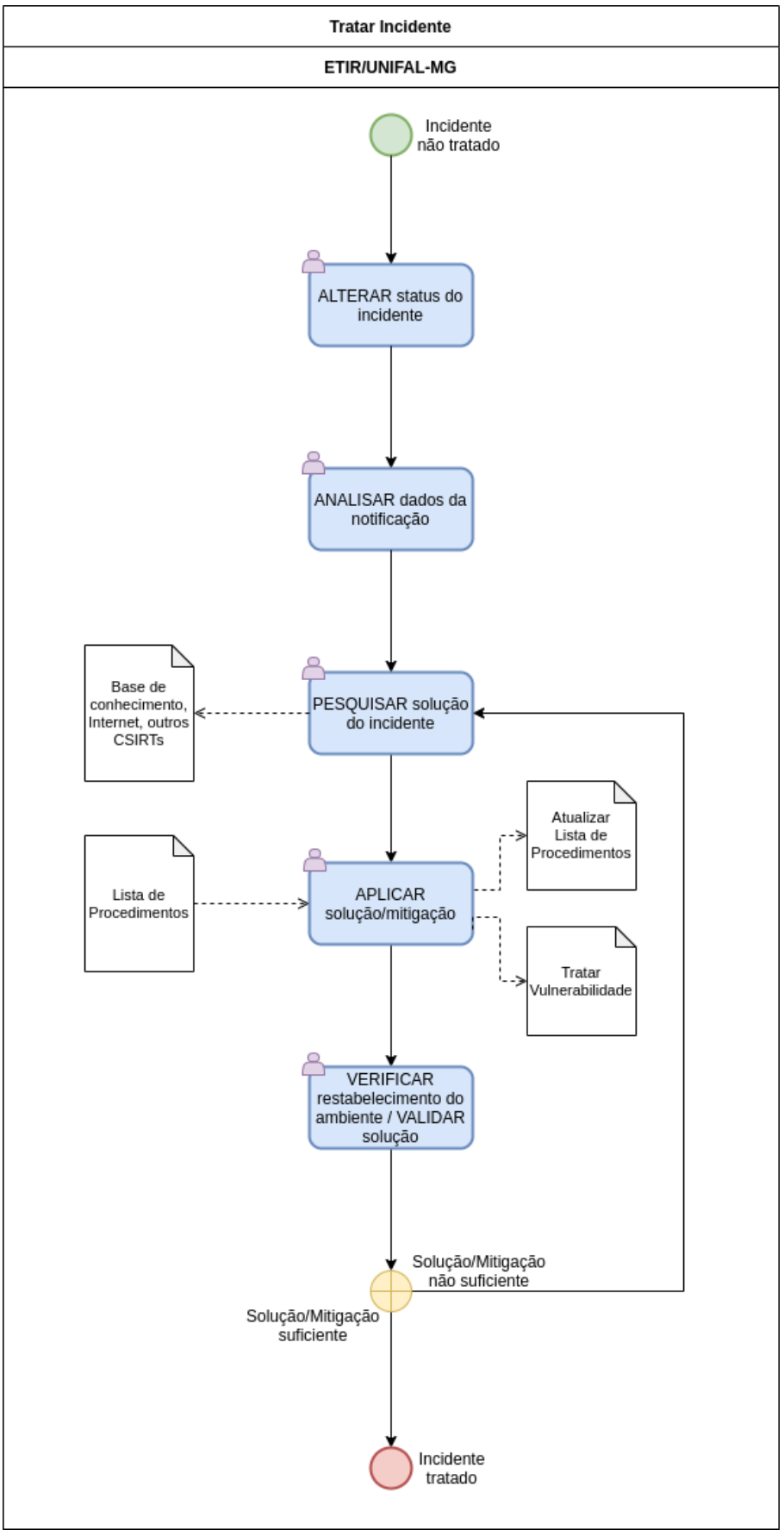
Gerente de Segurança da Informação/Coordenador da ETIR/UNIFAL-MG

Anexo II - Processos

Este anexo faz parte integral do documento Plano de Gestão de Incidentes de Segurança da Informação e Comunicação da ETIR/UNIFAL-MG.




Classificar Incidente
ETIR/UNIFAL-MG
Incidente não classificado
ANALISAR dados da notificação
Tabela de taxonomia
CLASSIFICAR tipo de incidente
Níveis de criticidade
DEFINIR criticidade do incidente
ALTERAR status do incidente
Incidente classificado


Tratar Incidente
ETIR/UNIFAL-MG
Incidente não tratado
ALTERAR status do incidente
ANALISAR dados da notificação
PESQUISAR solução do incidente
Base de conhecimento, Internet, outros CSIRTs
APLICAR solução/mitigação
Lista de Procedimentos
Atualizar Lista de Procedimentos
Tratar Vulnerabilidade
VERIFICAR restabelecimento do ambiente / VALIDAR solução
Solução/Mitigação não suficiente
Solução/Mitigação suficiente
Incidente tratado

Política de Confidencialidade e Manutenção do Sigilo ETIR/UNIFAL-MG

1 - Apresentação

O objetivo desta política é estabelecer condições para regulamentar as obrigações do membro da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação e Comunicação - ETIR/UNIFAL-MG no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela e pela Universidade Federal de Alfenas - UNIFAL-MG, para execução das atividades profissionais a serem realizadas pela equipe.

Esta política tem como base legal o Código Civil - Lei 10.406/2002, artigo 229, o Código de Ética Profissional do Servidor Público - Decreto no 1.171/1994, o Tratamento da Informação Classificada e Credenciamento - Decreto 7.845/2012, a Resolução Nº 8, de 26 de março de 2018, do Conselho Universitário da UNIFAL-MG, que aprova a Política de Segurança da Informação e Comunicação da UNIFAL-MG, bem como outras legislações e normativas internas e/ou externas pertinentes.

2 – Definições

São consideradas confidenciais e/ou privadas todas as informações, *know-how*, documentos, programas de computador e respectiva documentação, códigos fonte, relatórios, dados estratégicos, financeiros, pessoais ou outros dados, registros, formulários, ferramentas, produtos, serviços, metodologias, pesquisa presente e futura, conhecimento técnico, planos e segredos comerciais e outros materiais tangíveis ou intangíveis, armazenados ou não, compilados ou reduzidos a termo, seja física, eletrônica ou graficamente, por escrito, ou por qualquer meio, assim definida pela UNIFAL-MG.

As informações confidenciais incluem, sem limitação, arquivos e informações:

- que contenham a especificação de propriedade exclusiva ou confidencial;
- cuja natureza confidencial tenha sido informada pela UNIFAL-MG;
- que, em virtude de suas características e natureza, sejam consideradas confidenciais em circunstâncias semelhantes;
- quaisquer outras informações, mesmo que sem a natureza confidencial informada pela UNIFAL-MG, que sejam consideradas confidenciais e/ou privadas de acordo com normativas internas e/ou externas e outras legislações.

3 – Acordo de Confidencialidade

3.1 - O membro da equipe reconhece a natureza confidencial das informações recebidas pela ETIR/UNIFAL-MG e que tenha tomado ou lhe tenha sido dado conhecimento durante o seu período de trabalho na ETIR/UNIFAL-MG, obrigando-se a guardar a confidencialidade, não podendo utilizar em seu benefício próprio, revelar, ceder, partilhar ou permitir sua duplicação, uso ou divulgação a terceiros, no todo ou em parte.

3.2 - O membro da equipe se compromete a:

- tomar todas as providências para impedir a reprodução ou revelação de informações confidenciais e/ou privadas, pelo menos de forma equivalente às providências que toma para proteger suas próprias informações;
- não revelar informações confidenciais e/ou privadas a terceiros ou alguma pessoa que não aquelas que, em razão da natureza do seu trabalho e exercício de suas funções, seja necessário conhecê-las, exceto se devidamente autorizada pela UNIFAL-MG;
- não utilizar informações confidenciais e/ou privadas em proveito próprio ou de terceiros;
- não realizar cópias de informações confidenciais e/ou privadas sem o consentimento expresso e prévio da UNIFAL-MG;
- deixar de utilizar informações confidenciais e/ou privadas imediatamente em caso de desligamento da ETIR/UNIFAL-MG, devolvendo qualquer mídia que as contenham, tais como, por exemplo, papeis, mídias removíveis, CDs, DVDs, aplicativos, códigos fontes e demais materiais que contenham tais informações;
- deixar de acessar espaços de armazenamento compartilhados e excluir quaisquer arquivos que tenham sido compartilhados por terceiros para a execução dos trabalhos da ETIR/UNIFAL-MG;
- não obter, para si ou terceiros, os direitos de propriedade intelectual relativos às informações e soluções desenvolvidas pela ETIR/UNIFAL-MG.

3.3 - Esta política não aplica-se às informações que:

- sejam comprovadamente de domínio público;
- já eram do conhecimento do membro da equipe antes do seu ingresso e que não foram adquiridas direta ou indiretamente da UNIFAL-MG;
- não são mais consideradas como confidenciais pela UNIFAL-MG;
- sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo Federal, requisitadas, através de solicitações expressas, por comissões de sindicância e/ou de processo administrativo disciplinar, desde que sejam cumpridas todas as medidas de proteção pertinentes e tenham sido notificadas sobre a existência da ordem.

3.4 - A UNIFAL-MG, identificando violação desta política, poderá tomar todas as medidas extrajudiciais e judiciais, nas esferas cíveis e criminais, que julgar cabíveis à defesa de seus direitos, inclusive autorais, a fim de obter reparação pelos danos e prejuízos causados.

3.5 - Esta política tem duração por período indeterminado, e é aplicável a todas as informações confidenciais, inclusive àquelas existentes antes do ingresso do membro à equipe.