	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO.....	1
3.	DEFINIÇÕES.....	2
4.	DOCUMENTOS DE REFERÊNCIA	3
5.	RESPONSABILIDADES	4
6.	REGRAS BÁSICAS	11
7.	CONTROLE DE REGISTROS	39
8.	ANEXOS	39
9.	REGISTRO DE ALTERAÇÕES	49

1. OBJETIVO

O presente procedimento de resposta a incidentes de segurança da informação visa instruir as equipes responsáveis sobre o tratamento de ocorrências detectadas ou informadas, baseando-se na rede operativa, apoiar uma resposta rápida e eficaz a incidentes cibernéticos alinhada com a segurança da organização e objetivos do negócio. Incluindo as melhores práticas de mercado sobre o tema; aumentando, assim, a capacidade responsiva frente a ameaças sistêmicas de maneira rápida, efetiva e ordenada. Com objetivo de prevenir, tratar e responder a incidentes cibernéticos na rede operativa visando a disponibilidade dos serviços.

Tendo por objetivo:

- Fornecer orientação sobre as medidas necessárias para responder a incidentes cibernéticos.
- Definir os papéis, responsabilidades, e autoridades do pessoal e das equipes necessárias para gerenciar respostas a incidentes cibernéticos.
- Definir requisitos de conformidade legal e regulatória para incidentes cibernéticos.
- Traçar processos de comunicação interna e externa na resposta a incidentes cibernéticos.
- Fornecer orientação sobre as atividades pós-incidente para apoiar a melhoria contínua.

2. ÂMBITO DE APLICAÇÃO


2.1. Empresa

Todas as empresas do Grupo CPFL, incluindo as que atuam na geração, transmissão, distribuição e comercialização de energia elétrica.

2.2. Área

Todas as áreas do **Grupo CPFL**.

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 1 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	--------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

3. DEFINIÇÕES

3.1 CSIRT: Computer Security Incident Response Team (CSIRT) é o time que atua na preparação, identificação, contenção, erradicação e documentação do incidente de segurança, sendo a equipe participante de todas as fases de gestão de um incidente de segurança.

3.2 Autenticação: O processo pelo qual se confirma se uma entidade é quem afirma ser. A autenticação identifica um indivíduo com base em credencial (senha, cartão inteligente ou biometria).

3.3 Autorização: Após autenticada, a entidade receberá seus direitos de acesso, ou seja, suas permissões por meio da autorização.

3.3 Confidencialidade: Garantia de que os dados da empresa não estarão disponíveis nem serão divulgados a indivíduos, entidades ou processos sem autorização.

3.4 Conscientização: Processo de aprendizagem que prepara o estágio de treinamento, mudando atitudes individuais e organizacionais para perceber a importância das práticas de privacidade e proteção de dados e as consequências adversas de sua falha.

3.5 Controles: Refere-se a controles tecnológicos ou de processos que podem impedir um criminoso de ler ou usar os dados acessados ou adquiridos. Definem os objetivos principais de uma implementação de segurança apropriada.

3.6 Notificação de violação: Refere-se geralmente às leis que se aplicam a uma entidade que exige que tal entidade notifique órgãos quando ocorrida acesso não autorizado.

3.7 Incidente de Segurança da Informação: Ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, diretrizes, política de segurança, procedimento de segurança ou política de uso.

3.8 Impacto: Consequências que podem ocorrer caso o risco se manifeste.


3.9 Incidente de maior impacto: É estabelecido com base na classificação de severidade que consta do processo de gestão de riscos de segurança da informação do Grupo CPFL.

3.10 Grupo CPFL: A CPFL Energia S.A., e todas as suas controladas diretas e/ou indiretas, exceto as empresas com seus próprios padrões de governança e gestão que compartilham controle com outras empresas.

3.11 Ambiente Operativo do ONS: Toda a infraestrutura computacional e de telecomunicações de Tempo Real e histórico, que atende à sala de controle e outras áreas interessadas do ONS, e que está protegida pelos Firewalls operativos.

3.12 RACI: É uma ferramenta visual de fácil utilização que define com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades de um processo.

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 2 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	--------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

3.13 SUBESTAÇÃO: É uma instalação elétrica de alta potência, contendo equipamentos para transmissão e distribuição de energia elétrica, além de equipamentos de proteção e controle.

3.14 REDE OT: OT ou tecnologia operacional é uma categoria de um sistema de computação que processa dados operacionais como telecomunicações, componentes técnicos, computadores e é usada para monitorar dispositivos, vários processos industriais e alguns dos eventos da indústria e conseqüentemente, faça ajustes se necessário em uma indústria ou empresa.

3.15 REDE USINA: Uma usina elétrica, também conhecida como estação geradora ou usina geradora, é uma instalação industrial para a geração de energia elétrica gerada pela transformação das diversas fontes de energia encontradas na natureza.

3.16 SISTEMA SCADA: SCADA (Supervisory Control and Data Acquisition) é um sistema de controle e aquisição de dados utilizado em processos industriais e de infraestrutura crítica — a exemplo de setores como energia elétrica, água, gás e petróleo.

3.17 ARCIBER: Ambiente Regulado Cibernético é o conjunto de redes e equipamentos que estão considerados no escopo desta Rotina Operacional. O ARCiber é composto por: Centros de operação dos agentes; Equipamentos que participam da infraestrutura de envio ou recebimento de dados e voz para ambientes operativos do ONS ou para centros de operação de outros agentes; Ambiente operativo do ONS.

3.18 SISTEMA ADMS: O sistema ADMS utiliza informações em tempo real sobre a rede elétrica (SCADA), incluindo informações sobre a topologia da rede (GIS), fluxo de energia, tensão e carga, para isolar a seção da rede afetada pela falha. Em seguida, o sistema realiza uma série de manobras automáticas para restaurar a energia elétrica aos consumidores afetados, minimizando o número de clientes sem energia elétrica.


3.19 SISTEMA SAGE: SAGE é um sistema SCADA/EMS modular, robusto e escalável, concebido para ser facilmente expandido através da adição de novas funcionalidades. O sistema é baseado em uma infraestrutura computacional distribuída, redundante e de alto desempenho. Esta arquitetura confere grande flexibilidade e escalabilidade ao sistema.

3.20 DMIC: Duração Máxima de Indisponibilidade Contínua

4. DOCUMENTOS DE REFERÊNCIA

- Política de Segurança Cibernética do Grupo CPFL - 19368;
- ISO/IEC 27001;
- NIST Computer Security Incident Handling Guide;
- International Standard ISO/IEC27035-1;
- ISA-95;
- ISA/IEC 62443;
- NIST SP-82;
- RO-CB.BR.01;
- IEC 61850;
- NIST 800-61r2.

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 3 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	--------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

- Plano de Resposta a Incidentes de Segurança da Informação TI - 18851;
- Gestão de Crise e PCNs
- Procedimento de Análise de Risco do SGSI;
- Resolução Normativa da ANEEL nº 964/2021;
- Ferramentas Blue e Red Team;
- PLAYBOOK OT;

5. RESPONSABILIDADES

5.1 SOC OT

- Monitorar/receber chamados de incidentes;
- Registrar o incidente;
- Analisar o chamado e definir se é um incidente de segurança da informação, conforme item 6.3 deste documento;
- Encaminhar para a Segurança da Informação o incidente, caso necessário;
- Aciona as equipes envolvidas;
- Realiza medidas iniciais para contenção do incidente;
- Realiza a verificação e ações de contenções em equipamentos corporativos que possui interação a rede OT;
- Acompanhar e atuar em conjunto com outras áreas as ações corretivas e preventivas até o encerramento do incidente; e
- Gerar indicadores e reportes referentes aos incidentes.

5.2 Segurança da Informação

- Receber o incidente através do SOC OT;
- Informar o incidente para atuação em conjunto com as equipes responsáveis e envolvidas;
- Atuar nas ações corretivas e preventivas e encerrar o incidente;
- Acionar o Facilitador de Crise caso o incidente seja classificado como 'crise' com base nos gatilhos de crise descritos no item 6.8 deste documento; e
- Identificar, proteger, diagnosticar, responder e recuperar os incidentes cibernéticos na rede operativa.

5.3 Gestor de Segurança da Informação

- Receber informação do incidente através da equipe de Segurança da Informação;
- Atuar nas ações corretivas e preventivas junto à equipe de Segurança da Informação e demais envolvidos;
- Centralizar os acionamentos a outras áreas;
- Estabelecer comunicação interna de incidentes
- Aprovar o acionamento do Facilitador de Crise caso o incidente seja classificado como 'crise' com base nos gatilhos de crise descritos no item 6.8 deste documento e/ou documento 17922; e
- Acionar o Porta-Voz para comunicar *stakeholders* internos e externos (em casos de crise);
- Acionar a sala de crise estratégica com base nos gatilhos de crise descritos no item 6.8 deste documento e/ou documento GED nº 17922;

5.4 Diretor de Tecnologia

- Receber informação do incidente através do gestor de segurança da informação (CSIRT Leader);

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 4 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	--------------------

- Atuar na tomada de decisão relacionada as ações corretivas e preventivas junto às equipes envolvidas;
- Ser consultado sobre o acionamento do Facilitador de Crise (Dir. de Comunicação) caso o incidente seja classificado como 'crise' com base nos gatilhos de crise descritos no item 6.8 deste documento.

5.5 Grupo de Crise: Time Estratégico (vide procedimento de Gestão de Crises)

- Receber notificações sobre crises e atuar na camada executiva, acompanhando e deliberando sobre planos de ação para contenção e recuperação do evento.

5.6 Grupo de Crise: Time de Avaliação Inicial (vide procedimento de Gestão de Crises)

- Avaliar e classificar o incidente como crise.

5.7 Grupo de Crise: Time de Apoio Técnico-operacional (vide procedimento de Gestão de Crises)

- Decidir sobre acionamento e encerramento de PCN;
- Implementar ações para tratamento da crise; e
- Auxiliar na comunicação com *stakeholders*.

5.8 Porta-voz

- Comunicar *stakeholders* internos e externos sobre a crise conforme alinhamento com o Time Estratégico.

5.9 RACI

A matriz RACI é formada por um acrônimo, que também define os papéis e as atribuições dos envolvidos, na ocasião, compreendido para o ambiente de rede operativa.

Quem é designado para trabalhar nessa atividade? **R: Responsável**

Quem tem a autoridade para tomar decisão? **A: Autoridade**

Quem deve ser consultado e participar da decisão da atividade no momento que for executada?


C: Consultado

Quem deve receber a informação de que uma atividade foi executada?

I: Informado.

	ONS / ANEEL	Executivos	CISO	CSIRT	COS / COI *	COT / REST** / TI	RESM**	SegInfo OT	SOC OT	REGULATÓRIOS
Registrar incidente									RA	
Revisão e triagem inicial dos alertas de incidentes									RA	
Resolução de incidentes N1									RA	
Resolução de incidentes N2									RA	
Resolução de incidentes N3									RA	
Acionamento da Segurança da Informação									RA	
Acionamento Grupo de Crise				I		I	I	RA		

	ONS / ANEEL	Executivos	CISO	CSIRT	COS / COI *	COT / REST** / TI	RESM**	SegInfo OT	SOC OT	REGULATÓRIOS
Acionamento Porta-voz				CI				RA		
Centralização dos acionamentos a outras áreas				CI				RA		
Sustentação das plataformas de segurança				CI		RA		RA		
Revisão dos casos de uso (regras para gerar alertas)						CI	CI	RA	R	
Criação de novos casos de uso baseados em ameaças						CI	CI	A	RA	
Revisão do monitoramento dos ativos						RA	CI	CI	I	
Contenção das ameaças detectadas						RA	A	RA	CI	
Saneamento das vulnerabilidades do ativos						CI	RA	RA	CI	
Coordenação dos testes dos casos de uso						CI		RA	CI	
Execução de simulações de ataques					CI	CI	CI	RA	I	
Investigação e análises forenses				RA		CI	CI	CI	C	
Geração de reportes diários dos incidentes			I	I		I	CI	I	RA	
Geração de reportes executivos dos incidentes		I	I	RA	I	I	CI	I	RA	
Gerar indicadores referentes aos incidentes		I	CI	RA	CI	CI	CI	CI	RA	
Análises de artefatos e <i>malwares</i>			I	A	I	CI	CI	R	R	
Comunicação interna de incidentes Alto		CI	RA	I						I
Comunicação externa de incidentes Alto	I	CI	RA	I						R
Acionamento de PCN		I	RA	I	I	RCI	I	RCI	I	
Reportar o desempenho da execução do processo		I	RA	I	I	I	I	RA	I	
Manter registro de melhorias do processo			RA	I	I	I	I	R	I	
Definir e promover ações de melhoria no processo		CI	RA	CI	CI	CI	CI	CI	CI	
Encerrar incidente		I	I	I	I	CI	CI	RA	I	

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

* COS/COI se refere a todos os Centro de Operações de Sistema do Grupo CPFL.

** COT/REST/RESM Se refere a todos os Centro de Operações de Telecom e Medição do Grupo CPFL.

5.10 Árvore de Acionamento

Com as responsabilidades definidas, nesta seção, será indicado os contatos a serem acionados mediante a concretização de um incidente de Segurança da Informação para Rede Operativa.

Líder L = é o responsável pela área/função indicada no organograma, em sua ausência, o

Suplente S = fica responsável por essa área/função.

Time	Área	Líder	Suplente(s)
Rede Operativa	COI	Luiz Fernando Velo (Gerente) (14) 99841-5017 E-mail: luizvello@cpfl.com.br	Thiago Eduardo Lisboa (Coordenador) (19) 99937-4011 E-mail: thiagolisboa@cpfl.com.br
	COS	Rodrigo Mazo Rocha (Gerente) (19) 99266-5919 E-mail rodrigomazo@cpfl.com.br	Sara Regina Consoni (Coordenadora) (19) 99822-7614 E-mail: sarap@cpfl.com.br
	COT	Rafael Diniz (Gerente) (19) 99902-7570 E-mail: rafaeldiniz@cpfl.com.br	Luiz Carlos Bigon (Eng. Operações.Telecom Senior) (19) 99728-0646 E-mail: bigon@cpfl.com.br
	Centro de Operação da Transmissão (COT)	José Eduardo Malvestio Cereja (Gerente) (51) 98448-8504 E-mail: jose.cereja@cpfl.com.br	Humberto Margel Wickert (Coordenador) (51) 98600-2427 E-mail: humberto.wickert@cpfl.com.br

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 7 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	--------------------

	Engenharia de Telecomunicação – CPFL-T	<p>Felipe Tatsch (Gerente)</p> <p>(51) 99509-3131</p> <p>E-mail: felipe.tatsch@cpfl.com.br</p>	<p>Igor Freitas Fagundes (Coordenador)</p> <p>(53) 99942-9429</p> <p>E-mail: igor.fagundes@cpfl.com.br</p>
	COI RENOVAVEIS	<p>Filipe Moraes Monteiro (Gerente)</p> <p>(11) 97450-8731</p> <p>E-mail: filipe.monteiro@cpfl.com.br</p>	<p>Vitor Perez (Gerente)</p> <p>(19) 3796-1335</p> <p>E-mail: vitor.perez@cpfl.com.br</p>
	REST	<p>Eduardo Henrique Trepodoro (Gerente)</p> <p>(19) 98194-9414</p> <p>E-mail: atrepodoro@cpfl.com.br</p>	<p>Adriano da Silva Filgueiras (Esp. Planejamento em Telecom)</p> <p>(11) 99636-1491</p> <p>E-mail: afileguas@cpfl.com.br</p>
	RESM	<p>Evaldo Baldin Dias (Gerente)</p> <p>(19) 99187-0037</p> <p>E-mail: baldin@cpfl.com.br</p>	<p>Eduardo Henrique da Silva (Gerente)</p> <p>(19) 99660-2058</p> <p>E-mail: eduardosilva@cpfl.com.br</p>
Tecnologia da Informação	Diretória de TI	<p>Thiago Amante (Diretor)</p> <p>(11) 99602-8319</p> <p>E-mail: thiago.amante@cpfl.com.br</p>	<p>Emerson Cardoso (CISO)</p> <p>(11) 99593-9300</p> <p>E-mail: emerson.cardoso@cpfl.com.br</p>
	Segurança da Informação	<p>Emerson Cardoso (Gerente - CISO)</p>	<p>Renato Amabile (Coordenador)</p>


Tipo de Documento: Procedimento

Área: EIS-GERENCIA DE SEGURANCA DE TI

Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

		(11) 99593-9300 E-mail: emerson.cardoso@cpfl.com.br	(19) 99971-5763 E-mail: ramabile@cpfl.com.br
	Sustentação de TI	Diogo Ribeiro Santana (Gerente) (19) 99644-1025 E-mail: diogo.santana@cpfl.com.br	Alexandre Alves Barrias (Gerente) (19) 99715-7806 E-mail: alexandre.barrias@cpfl.com.br
	Rel. TI – Sistemas Operativos/Transmissão	Carlos Alberto Belarmino Teixeira (Gerente) (19) 99222-9966 E-mail: belarmino@cpfl.com.br	Patricia Lopes Cavalcante (Especialista) (19)98202-6609 E-mail: pcavalcante@cpfl.com.br
	TI – Sistemas Clientes Externos	Augusto Cesar Reolon (Gerente) (19) 99369-1089 E-mail: areolon@cpfl.com.br	Leandro Danilo Piovezan (Coordenador) (17) 99158-1794 E-mail: ldpiovezan@cpfl.com.br
	TI – Sistemas Corporativos/ Suporte Interno	Cristiano Alberto (Gerente) (19) 98287-3201 E-mail: cristianoalberto@cpfl.com.br	Lucianna Alves Freire (Colaborador) (19) 3756-4154 E-mail: lucianna@cpfl.com.br
	Arquitetura e Dados	Diego Perissato (Gerente) (51) 93756-4179 E-mail: diegoh@cpfl.com.br	Rafael Antonio Pivoto Adami (Coordenador) E-mail: rafaeladami@cpfl.com.br

	Governança de TI	<p>Luana Ap. Ribeiro Javoni (Gerente)</p> <p>(19) 99288-0338</p> <p>E-mail: luanaj@cpfl.com.br</p>	<p>Daniele Nohama Roveri (Coordenador)</p> <p>(19) 98226-3044</p> <p>E-mail danieleroveri@cpfl.com.br</p>
Segurança da Informação	GRC	<p>Everton F. Duarte dos Santos (Coordenador)</p> <p>(19) 97172-2778</p> <p>E-mail everton.duarte@cpfl.com.br</p>	<p>Mateus Augusto Pereira Rocha (Analista S.I – Sênior)</p> <p>(19) 99794-7062</p> <p>E-mail: mateus.rocha@cpfl.com.br</p>
	IDM		<p>Beatriz Snieg (Analista S.I – Pleno)</p> <p>(19) 97172-2778</p> <p>E-mail: bsnieg@cpfl.com.br</p>
	Arquitetura e Projetos	<p>Adriana Soares Pimenta Silva (Coordenadora)</p> <p>(11) 98571-4755</p> <p>E-mail adriana.pimenta@cpfl.com.br</p>	<p>Aluizio Rodrigues de Souza (Especialista)</p> <p>(19) 99911-4083</p> <p>E-mail aluizio.souza@cpfl.com.br</p>
	SegInfo OT	<p>Leandro Barbosa do Carmo (Coordenador)</p> <p>(19) 97151-7509</p> <p>E-mail: leandro.carmo@cpfl.com.br</p>	<p>Victor Bastos Araujo (Analista S.I- Sênior)</p> <p>(19) 99679-9229</p> <p>E-mail vbastosaraujo@cpfl.com.br</p>
			<p>Alexandre Mundim de Oliveira (Analista S.I – Sênior)</p> <p>(19) 99690-5887</p> <p>E-mail: alexandre.oliveira@cpfl.com.br</p>

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

	SOC OT	Wesney Bolzan Silva (Gerente) (11) 99940-4526 wesney.silva@nava.com.br	Marcelo Cardelli de Camargo (Gerente) (11)98765-1613 marcelo.cardelli@nava.com.br
	Threat Intel	Renato Amabile (Coordenador) (19) 99971-5763 E-mail: ramabile@cpfl.com.br	Tiago Barbosa Pessoa (Analista S.I – Sênior) (11) 98334-4740 E-mail: tiago.barbosa@cpfl.com.br
			Felipe Almeida (Analista S.I – Sênior) (19) 99497-5512 E-mail: felipe.almeida@cpfl.com.br
Diretoria de Auditoria Riscos e Compliance	Privacidade de Dados	Denise Ramos de Lima (Gerente - DPO) (19)97151-5064 E-mail deniselima@cpfl.com.br	Nadine Emile Prado Maroeste (Coordenadora) E-mail nadine@cpfl.com.br
	Riscos	Bruna Victorelli (Gerente) E-mail bvictorelli@cpfl.com.br	Amanda Cristina Gava (Coordenadora) E-mail agava@cpfl.com.br

6. REGRAS BÁSICAS

6.1 Ciclo de Vida

O processo de respostas a incidentes de segurança da informação é composto por uma série de etapas. Esse processo fornece uma abordagem padronizada e organizada. Se um possível incidente de segurança da informação for relatado ou detectado, as equipes de tratamento devem seguir o presente processo, a fim de tomar as medidas apropriadas. O processo de resposta consiste em quatro fases ilustradas abaixo:

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 11 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------



Fonte NIST: Ciclo de Vida de resposta a incidentes de segurança

A etapa inicial envolve estabelecer e treinar uma equipe de resposta a incidentes de segurança da informação de rede operativa e a aquisição das ferramentas e recursos necessários. Durante esta etapa, a organização, representada pelos que estão no item 5.9 e 5.10 implementa um conjunto de controles, baseado nos resultados das avaliações de risco, visando a limitação do número de incidentes.

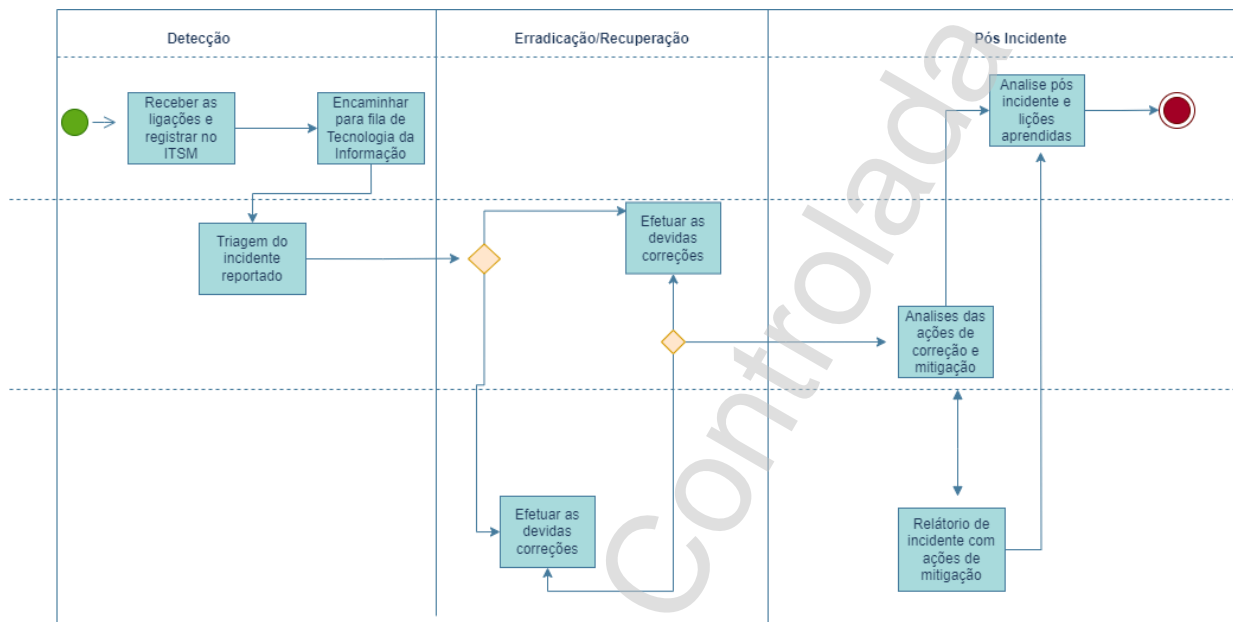
Após a implementação destes controles, ainda persistirá o risco residual de incidentes. Diante disso, a detecção de violações de segurança se faz necessária, a fim de alertar a organização, representada pelos que estão no item 5.9 e 5.10 sempre que ocorrerem incidentes. De acordo com a gravidade do incidente, a organização, representada pelos que estão no item 5.9 e 5.10 poderá mitigar o impacto do incidente, contendo-o e consecutivamente restabelecendo o ambiente.

Durante esta etapa, novas detecções e análises poderão ocorrer, a fim de garantir, por exemplo, que ao eliminar um malware de um sistema utilizado pela rede operativa, este não tenha contaminado outros sistemas.

Após o devido tratamento do incidente, a organização, representada pelos que estão no item 5.9 e 5.10 deve emitir um relatório detalhado do incidente, determinando sua causa-raiz, os possíveis prejuízos causados pelo incidente e finalmente, apresentar as etapas necessárias para prevenir sua reincidência.

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 12 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

O fluxo abaixo apresentado tem por objetivo, determinar as etapas mínimas que devem ser contempladas e/ou executadas:



6.2 Preparação

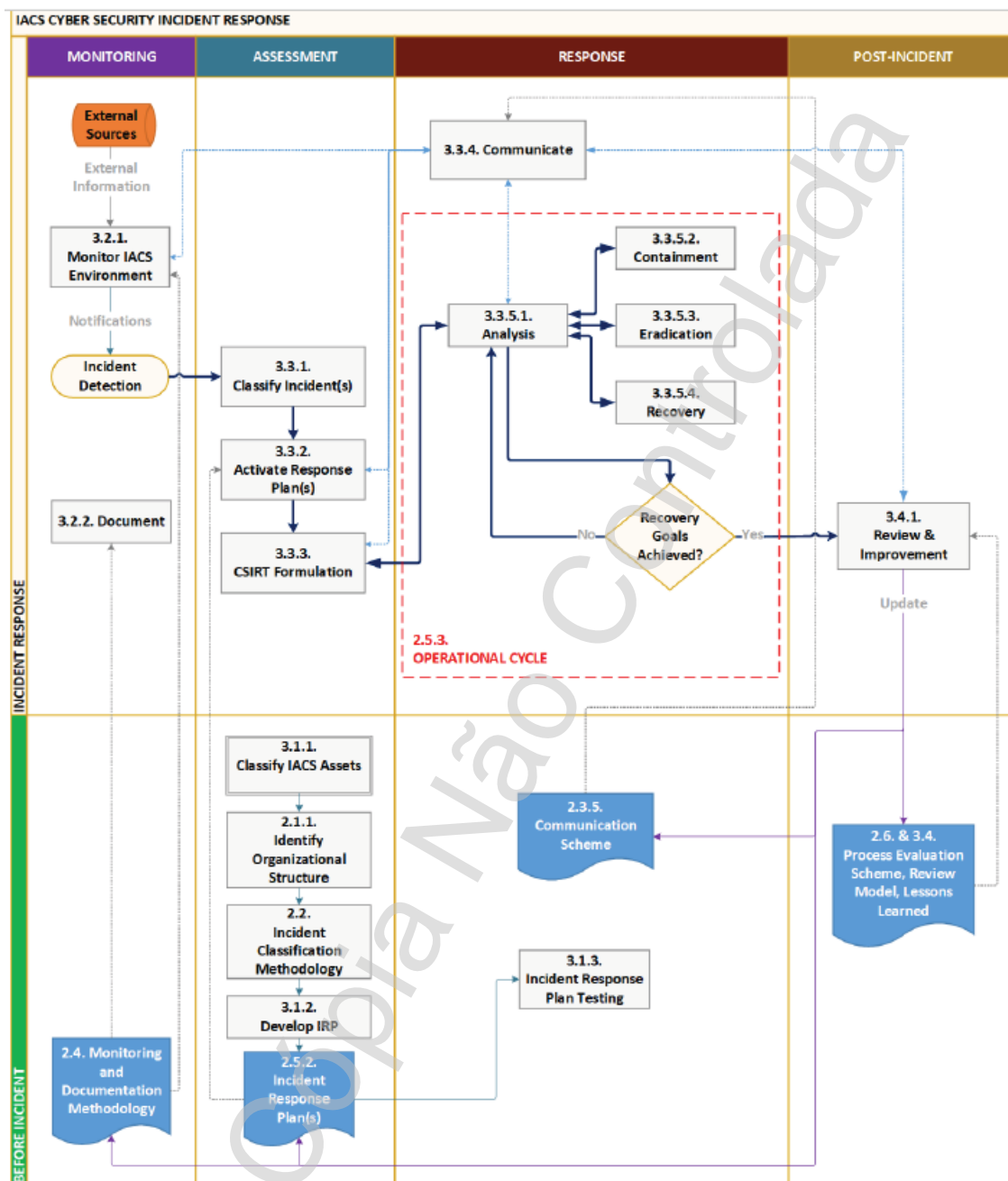
A etapa de Preparação visa capacitar a organização na adequada resposta a um incidente de segurança da informação da rede operativa, garantindo que sistemas, softwares e redes estejam suficientemente seguros, ativos de resposta a incidentes relacionados e equipes envolvidas devidamente treinadas.

Nesta fase, serão produzidos os seguintes documentos, não ficando restrito a esta lista:

- Lista de contatos da organização, atualizada periodicamente;
- Playbooks e ferramentas para resposta a incidentes;
- Procedimento para estabelecimento de war rooms;
- Definição de categorização e criticidade de incidentes;
- Modelos de treinamentos;
- Teste/Exercício;
- Simulações de cenários e ameaças para testes de resiliência, de análise das ferramentas e da capacidade e tempo de resposta;

Segue abaixo etapas do incidente de segurança da informação desde a fase de detecção do incidente, até o pós incidente:

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 13 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------




6.3 Detectar, Investigar, Analisar & Ativar

Nessa etapa envolve a confirmação do incidente, classificação de incidentes, ativação CSIRT e Perguntas de investigação. A detecção de um incidente pode ocorrer a partir de uma ou mais fontes, como alertas provenientes de ferramentas de monitoração, observação de logs e notificação de ocorrências feitas por colaboradores. Todas as fontes devem ser consideradas para a correta análise e determinação da criticidade do incidente.

Todo funcionário, terceiro ou prestador de serviços que atue diretamente no Grupo CPFL, é responsável por notificar uma ocorrência de segurança da informação, sempre que identificar um desvio, podendo identificar-se ou não para realizar o registro.

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 14 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Caso não possua acesso à intranet corporativa, poder-se realizar a comunicação por meio dos contatos abaixo:

- Ramal: 8002 (serviços corporativos); ou
- E-mail: seginfo@cpfl.com.br

No caso de terceiros que não possuem acesso à intranet corporativa, deve-se comunicar ao seu gestor do Grupo CPFL a ocorrência de um evento de segurança.

Notificações de incidentes também podem ser recebidos diretamente de uma entidade externa, como por exemplo: parceiros de negócio, fornecedores etc. O canal oficial para envio de notificações é o endereço eletrônico seginfo@cpfl.com.br.

Deve ser provido, de igual modo, um canal de comunicação que garanta o sigilo e privacidade de quem identifica e reporta um incidente de segurança da informação na rede operativa. Nesses casos, os usuários podem utilizar o seguinte meio:

- E-mail: ouvidoria@cpfl.com.br;
- Telefone: 0800 770 27 35;
- Fax: (19) 3756 8040; ou
- Internet: <https://www.cpfl.com.br/agencia/ouvidoria>

As ocorrências de segurança da informação devem ser registradas com seus artefatos e armazenados em repositório protegido.

Todos os incidentes de segurança devem ser comunicados às partes envolvidas tempestivamente, quando aplicável.

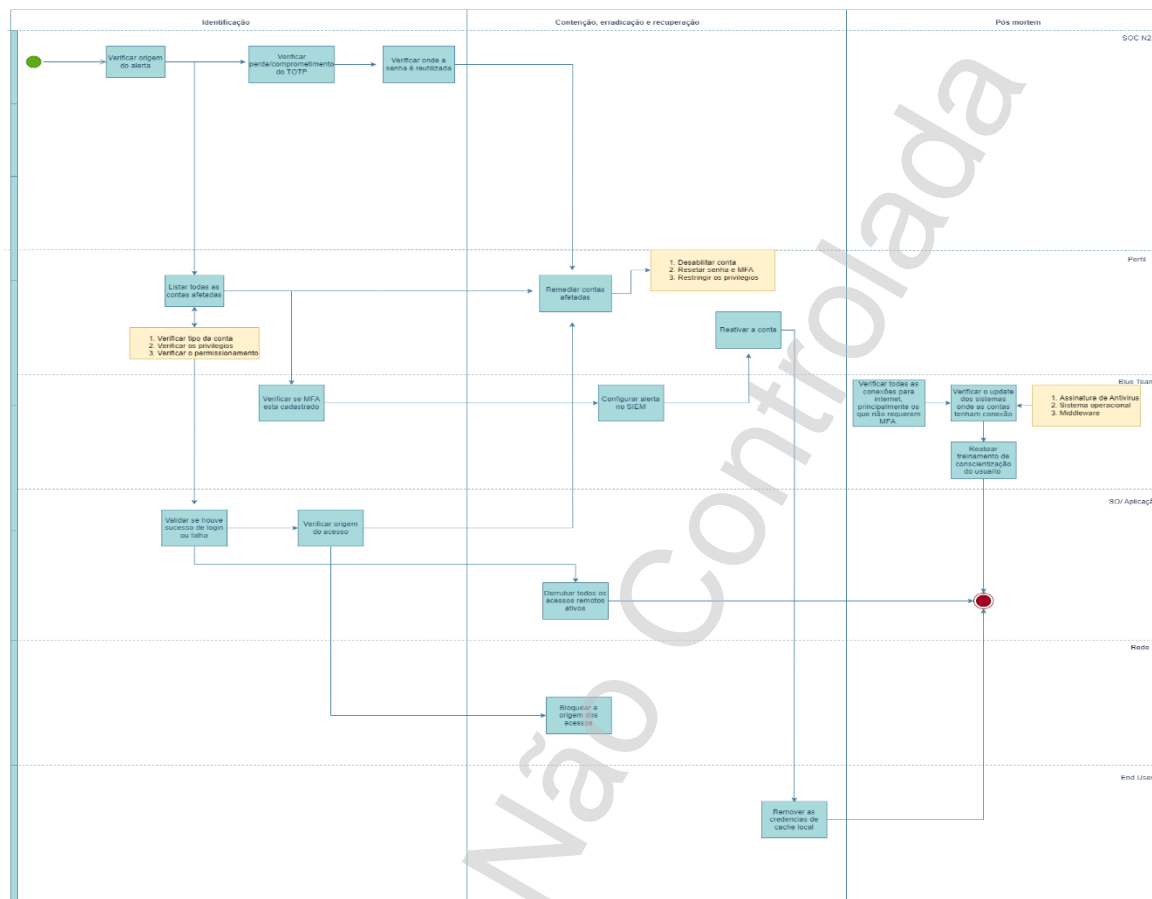
O registro de uma ocorrência de segurança da informação deve estar acessível, quando necessário e previamente autorizado pela Segurança da Informação, para funcionários, terceiros e entidades externas interessadas, e todos devem ser instruídos sobre a responsabilidade em notificar e registrar quaisquer fragilidades e falhas de segurança da informação.

Os incidentes de maior impacto devem ter o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, para as atividades do Grupo CPFL, abrangendo inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

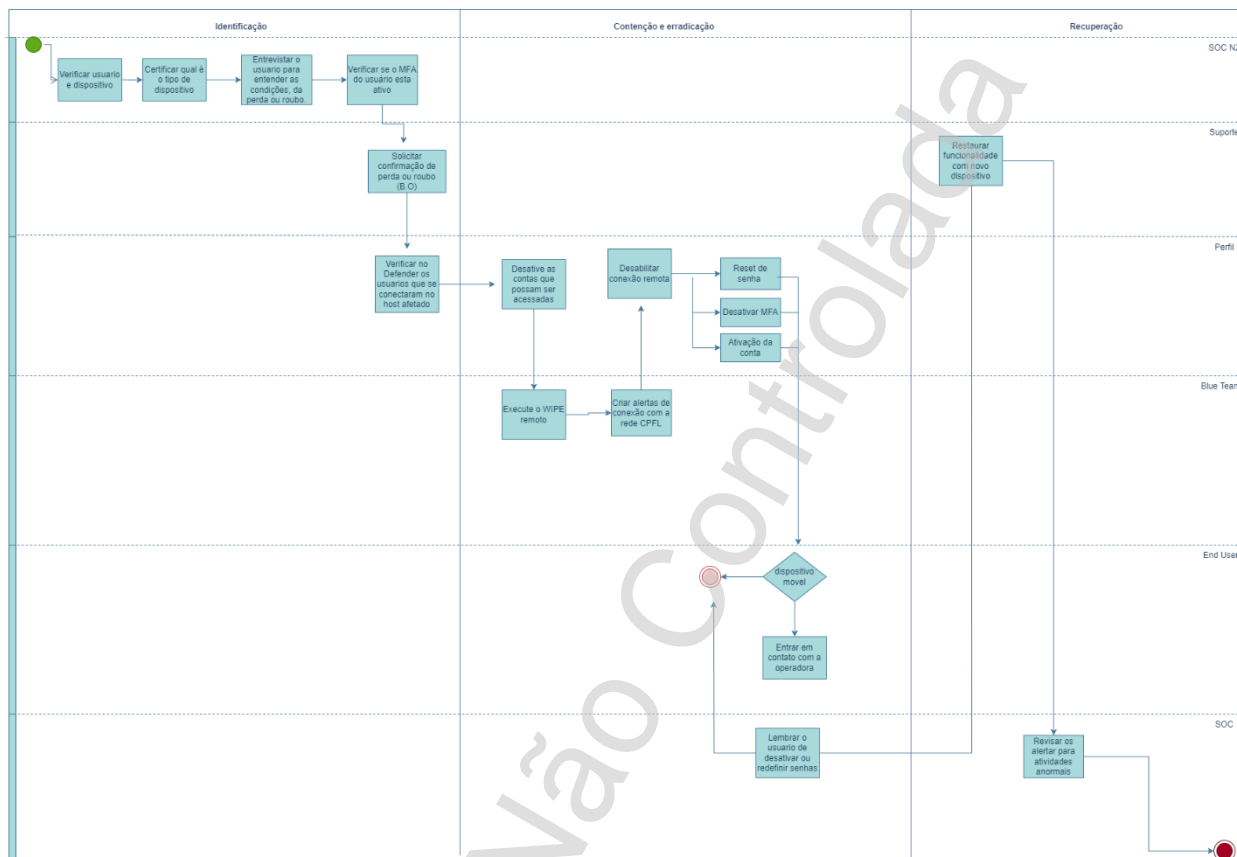
Em casos de incidentes de segurança da informação contendo credencial comprometida; perda, furto e roubo de dispositivo; malware; phishing; ransomwares, e outros descritos no PlayBook OT as equipes devem seguir as atividades e etapas descritas no mesmo. (<https://cpflenergia.sharepoint.com/:f:/s/eis/arearestrita/EvIhIbae3kBNrfHXCwzS2pABs3fwoBk9tWkz2MY2a8Zvrw?e=dgsvPI>).

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 15 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

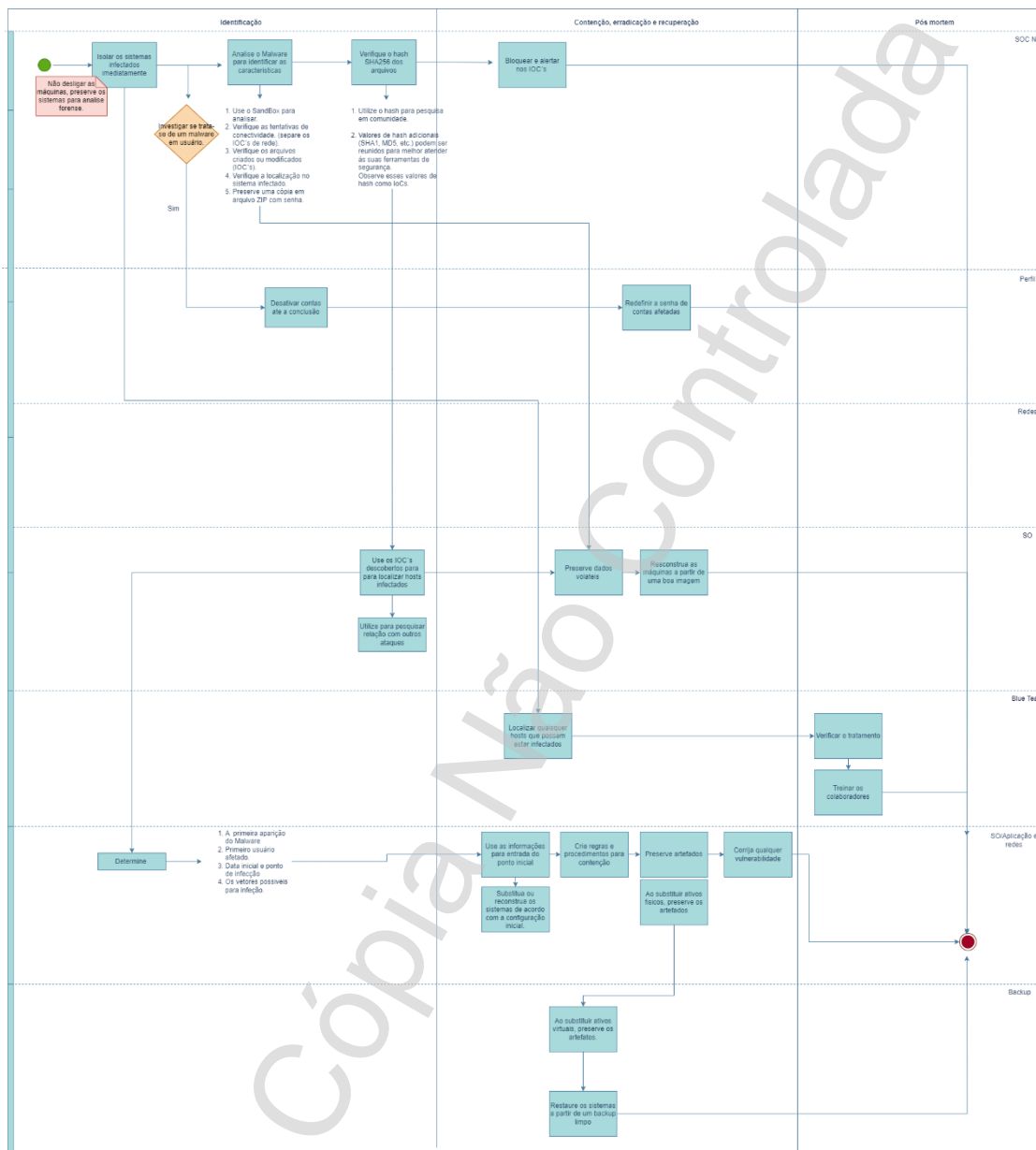
6.3.1 Fluxo Credencial Comprometida



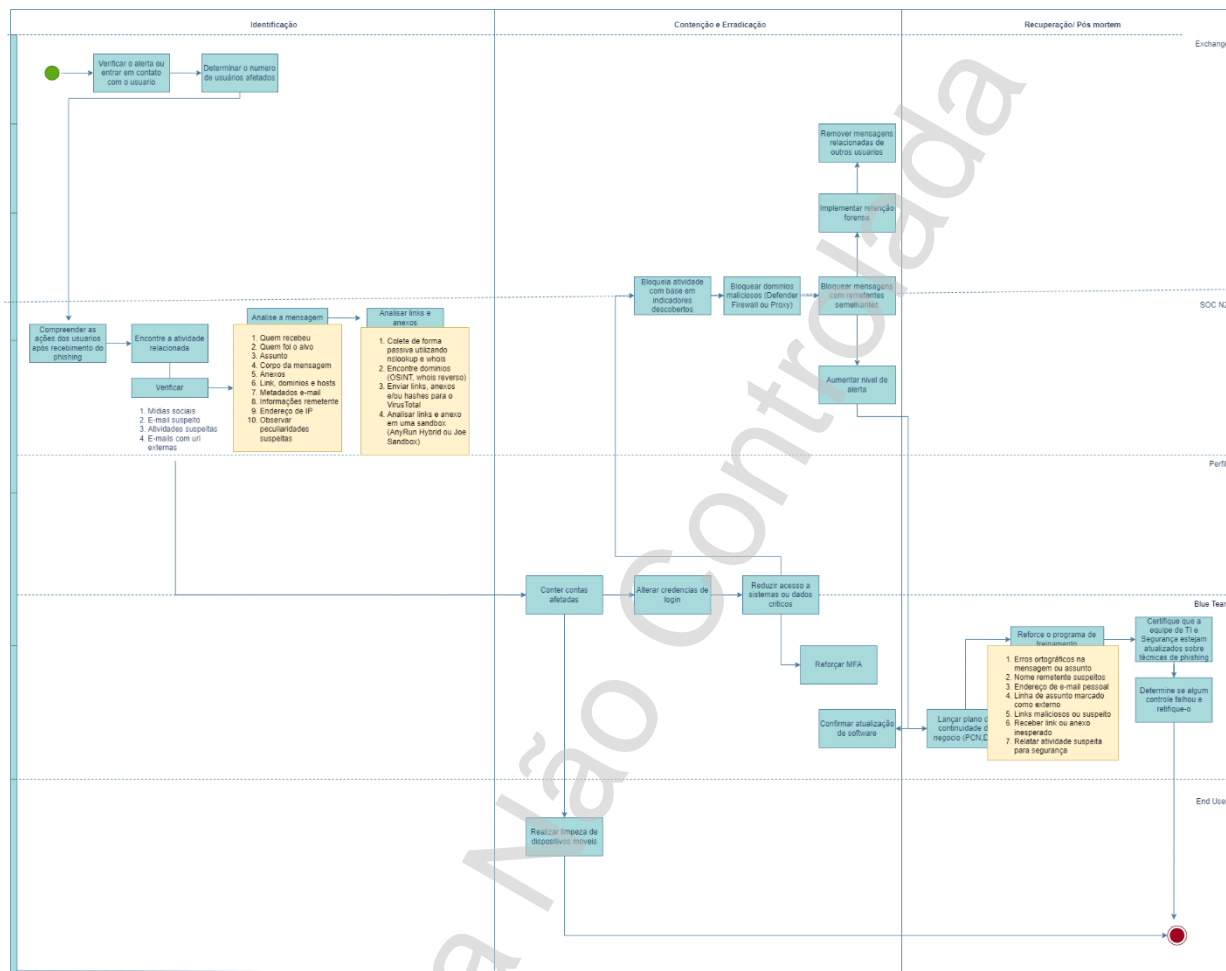
6.3.2 Fluxo Perda, furto e roubo de dispositivo



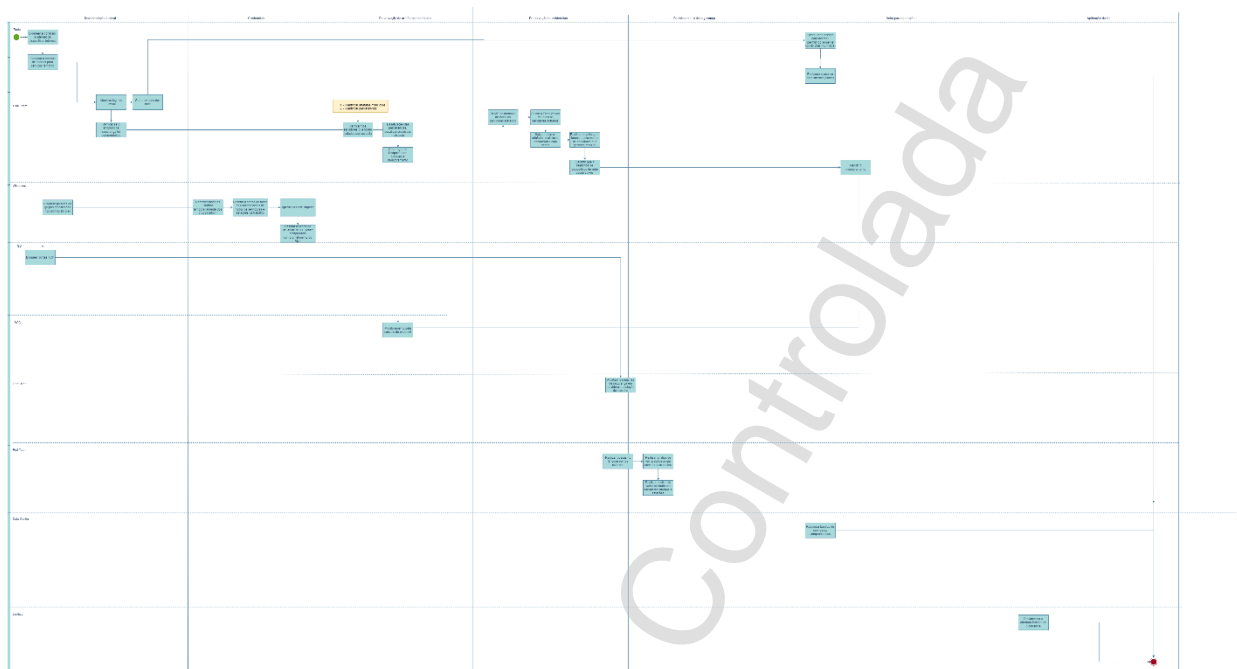
6.3.3 Fluxo Malware



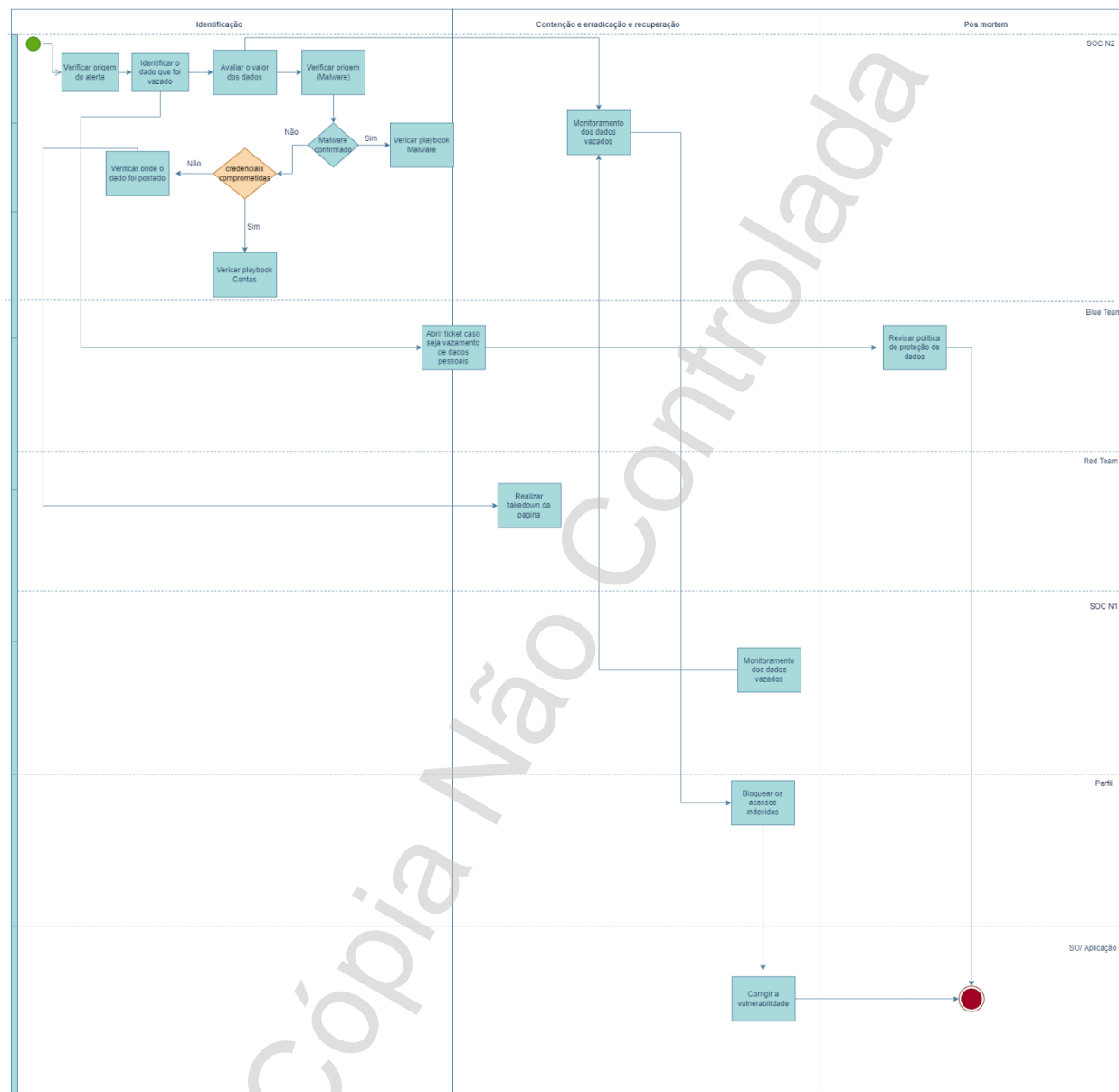
6.3.4 Fluxo Phishing



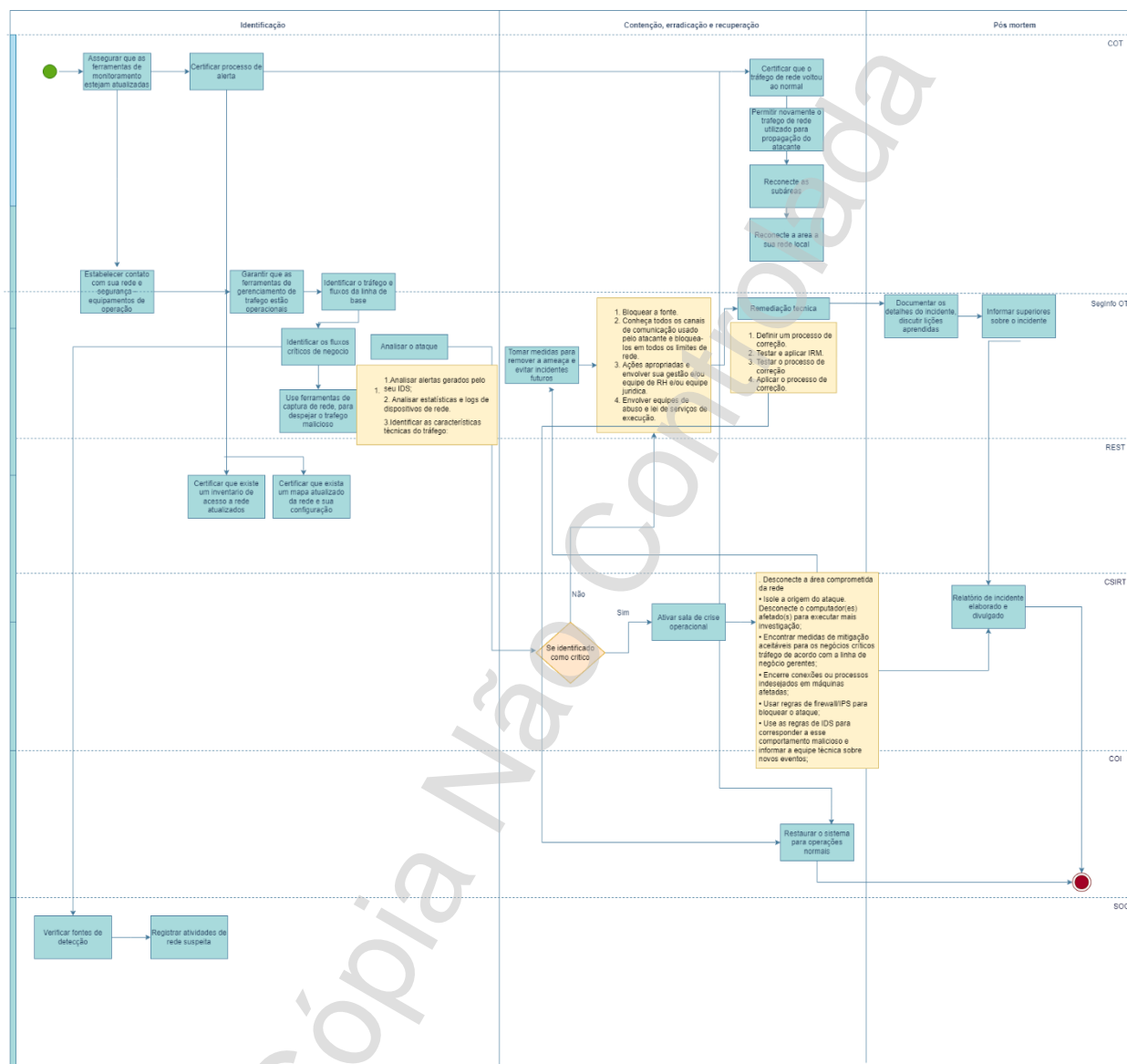
6.3.5 Fluxo Ransomwares



6.3.6 Fluxo Vazamento de Dados



6.3.7 Fluxo Network Attack



6.4 Definição de Incidente de Segurança da Informação

Um incidente de segurança da informação é indicado por um evento isolado ou por uma série de eventos inesperados, que tem a capacidade de comprometer as operações de negócio ou expor indevidamente informações do Grupo CPFL.

São exemplos de incidente de segurança da informação na rede OT quando:

- Atos que violam a Política de Segurança Cibernética;
- Comportamento anômalo de computadores e/ou redes sistêmicas que podem ameaçar a segurança de outros computadores, redes e/ou sistemas operativos;
- Obtenção ou tentativa de acesso não autorizado à sistemas e ativos do Grupo CPFL;

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 22 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

Tipo de Documento: Procedimento

Área: EIS-GERENCIA DE SEGURANCA DE TI

Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT


- Interrupção inesperada ou negação de serviço causada por *software* malicioso ou por ação indevida, intencional ou não, de pessoas não autorizadas ou mal-intencionadas;
- Uso não autorizado de sistemas para processamento ou armazenamento de dados;
- Alterações em características de *hardware* e/ou *software* sem autorização, instrução e/ou conhecimento do proprietário;
- Contaminação isolada ou disseminada por vírus, malwares, *worms* ou provenientes de *software* malicioso;
- Roubo/exfiltração de informações;
- E-mails maliciosos;
- Virus em sites maliciosos;
- Negação de Serviço (DoS ou DDoS);
- Falha nos controles de segurança da informação;
- *Ransomware*;
- *Phishing*;
- *Industrial Control System*;
- *Data Breach*; e
- Utilização de código que vise comprometer a integridade de dados/sistemas/ativos do Grupo CPFL.

As organizações devem se preparar para lidar com qualquer tipo de incidente de segurança da informação, mas é praticamente impossível cobrir todos os tipos de incidentes de segurança existentes.

Neste sentido, a orientação é concentrar-se em estar preparado para lidar com os principais tipos, que usam vetores de ataques comuns. No item a seguir, são apresentados alguns dos tipos de incidentes de segurança da informação, de acordo com sua natureza.


Categoria	Descrição
Negação de Serviço (Dos)	Ataque de negação de serviço.
Negação de Serviço Distribuída (DDoS)	Ataque distribuído de negação de serviço.
Comprometimento de informação	Sucesso ou tentativa de destruição, corrupção ou vazamento de credenciais, informação corporativa sensível ou de propriedade intelectual.
Comprometimento de ativo	Comprometimento de <i>host</i> (conta administrativa, <i>trojan</i> , <i>rootkit</i>), dispositivo de rede, aplicação ou conta de usuário. Isto inclui <i>hosts</i> infectados por <i>malware</i> onde um atacante esteja controlando ativamente o dispositivo.
Atividade ilegal	Furto, roubo, fraude, danos a pessoa. Incidentes de computador de natureza criminal, que provavelmente envolverá autoridade policial, investigações globais ou prevenção de perdas.
<i>Malware</i>	Um vírus ou <i>worm</i> tipicamente afetando múltiplos computadores corporativos. Isto não inclui <i>hosts</i> comprometidos que estejam sendo ativamente controlados por um atacante via um <i>backdoor</i> ou <i>trojan</i> . (veja Comprometimento de Ativo).

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 23 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

 <p>CPFL ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Violação de Política	Compartilhamento de material ofensivo, protegido por direitos autorais, violação deliberada da política de segurança. Uso indevido de ativo corporativo, como computador, rede ou aplicação. Escalação não autorizada de privilégios ou tentativa deliberada de burlar controles de acesso. Descumprimento das políticas e procedimentos e normas relacionados a privacidade e proteção de dados.
<i>Ransomware</i>	Ransomware é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo.
<i>Phishing</i>	Phishing é uma técnica de fraude online, utilizada por criminosos no mundo da informática para roubar senhas de banco e demais informações pessoais, usando-as de maneira fraudulenta.
<i>Industrial Control System</i>	Industrial Control System. trata-se de "Um sistema de informação usados para controlar processos industriais, como fabricação, manuseio de produtos, produção e distribuição
<i>Data Breach</i>	Uma violação de dados pessoais ou data breach é uma violação de segurança que provoque, de modo accidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento
<i>External/Removable Media</i>	Um ataque executado a partir de uma mídia removível ou de um dispositivo periférico (código malicioso se espalhando em um sistema a partir de uma unidade flash USB infectada)
<i>Attrition</i>	Um ataque que emprega métodos de força bruta para comprometer, degradar ou destruir sistemas, redes ou serviços (DDoS destinado a prejudicar ou negar acesso a um serviço ou aplicativo ou um ataque de força bruta contra um mecanismo de autenticação, como senhas)
<i>Web</i>	Um ataque executado a partir de um site ou aplicativo baseado na Web (ataques de script entre sites usado para roubar credenciais ou um redirecionamento para um site que explora uma vulnerabilidade do navegador e instala malware)
<i>E-mail</i>	Um ataque executado através de uma mensagem de e-mail ou anexo (código de exploração disfarçado como um documento anexado ou um link para um site malicioso no corpo de um e-mail)
<i>Supply Chain Interdiction</i>	Um ataque antagônico a ativos de hardware ou software utilizando implantes físicos, trojans ou backdoors, interceptando e modificando um ativo em trânsito do fornecedor ou varejista
<i>Impersonation</i>	Um ataque envolvendo a substituição de algo benigno por algo malicioso (spoofing, ataques de homem no meio, pontos de acesso sem fio desonestos e ataques de injeção de SQL envolvem representação)
<i>Improper Usage</i>	Qualquer incidente resultante da violação das políticas de utilização aceitáveis de uma organização por um utilizador autorizado, excluindo as categorias acima (Um usuário instala software de compartilhamento de arquivos, levando à perda de dados confidenciais)
<i>Loss or Theft of Equipment</i>	A perda ou roubo de um dispositivo de computação ou mídia usado por uma organização (Um laptop, smartphone ou token de autenticação)

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 24 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

6.4.1 Incidente de Segurança da Informação envolvendo Prestador de Serviço

Caso seja causado um incidente de Segurança da Informação envolvendo prestador de serviço do Grupo CPFL tais como:

- Vazamento de dados;
- Compartilhamento de logins e credenciais;
- Phishing;
- Desenvolvimento com falhas de segurança;
- Homologação incorreta dos desenvolvimentos realizados;
- Concessões de acessos sem as devidas aprovações;
- Compartilhamento de informações Internas e/ou Confidenciais do Grupo CPFL, sem as devidas aprovações

A verificação, pelo Grupo CPFL, da realização de atos ou omissões da Contratada dos itens citados acima acarretará a aplicação das penalidades previstas em Contrato. E casos de reincidência o cancelamento do contrato.

Para obter a lista completa de fornecedores, deve ser solicitado a equipe de ESQ (Qualificação de Fornecedores) solicitando uma lista completa, com contatos.

6.5 Natureza do Incidente

Todo incidente de segurança da informação na rede operativa será categorizado conforme o guia 'Case Classification' do *Forum of Incident Response and Security Teams* (FIRST). Isso visa facilitar a comunicação interna e externa e a rápida compreensão de um incidente. A tabela abaixo apresenta as seguintes categorizações:


6.6 Criticidade do Incidente

A classificação de criticidade de cada incidente de segurança é baseada na avaliação de impacto, regras de negócio, e dos ativos envolvidos, conforme importância para o negócio. Adicionalmente, as categorizações dos casos de uso são definidas de acordo com a organização MITRE ATT&CK, base de conhecimento de táticas e técnicas (TTP's) adversárias baseadas em observações de ataque ao redor do mundo.

6.6.1 Distribuição:

Criticidade	Descrição
Alta (3)	Indisponibilidade dos sistemas SCADAS críticos. Indisponibilidade no envio de informações críticas para o operador nacional do sistema com esforço máximo para a recuperação ou impossibilidade de recuperação. Indisponibilidade de supervisão e/ou telecomandos em mais ou igual a 20 (vinte) subestações da mesma região. Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 100 mil clientes. Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 25 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------


	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

	- Ataque cibernético comprometendo a disponibilidade, integridade e confidencialidade de dados do Centro de Operação e ativos que compõem o ARCiber.
Média (2)	<p>Indisponibilidade de equipamentos que atende as redes operativas, Impossibilidade de envio temporário ou não envio de informações não críticas para o operador nacional do sistema. Indisponibilidade de supervisão e/ou telecomandos em menos de 20 (vinte) subestações da mesma região. Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 50 mil clientes. Equipamentos de telecomandos infectados com possíveis ações de mitigação de risco sem interrupção do serviço.</p> <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Incidente cibernético que compromete ativos específicos da rede operativa, mas sem impactos a operação. <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Incidente cibernético que compromete ativos específicos da rede operativa, mas sem impactos a operação.
Baixa (1)	<p>Indisponibilidade de equipamentos que atende as redes operativas, Impossibilidade de envio temporário ou não envio de informações não críticas para o operador nacional do sistema. Indisponibilidade de supervisão e/ou telecomandos em menos de 10 (dez) subestações da mesma região. Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 20 mil clientes e equipamentos de telecomandos infectados com possíveis ações de mitigação de risco sem interrupção do serviço.</p> <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Incidente cibernético que compromete ativos específicos da rede operativa, mas sem impactos a operação.

6.6.2 Transmissão:

Criticidade	Descrição
Alta (3)	<p>Indisponibilidade dos sistemas SCADAS críticos. Indisponibilidade no envio de informações críticas para o Operador Nacional do Sistema Elétrico (ONS) com esforço máximo para a recuperação ou impossibilidade de recuperação. Indisponibilidade de teleassistência em mais de 5 subestações.</p> <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Ataque cibernético comprometendo a disponibilidade, integridade e confidencialidade de dados do Centro de Operação e ativos que compõem o ARCiber.
Média (2)	Indisponibilidade de equipamentos que atende as redes operativas, Impossibilidade de envio temporário ou não envio de informações não críticas

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 26 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------


	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

	<p>para o Operador Nacional do Sistema Elétrico (ONS). Indisponibilidade de teleassistência em 5 ou menos de subestações e equipamentos de teleassistência infectados com possíveis ações de mitigação de risco sem interrupção do serviço.</p> <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Ataque cibernético comprometendo pontualmente a disponibilidade, integridade e confidencialidade de dados do Centro de Operação e ativos que compõem o ARCiber.
Baixa (1)	<p>Indisponibilidade de equipamentos que atende as redes operativas, Impossibilidade de envio temporário ou não envio de informações não críticas para o Operador Nacional do Sistema Elétrico (ONS). Indisponibilidade de telecomandos infectados com possíveis ações de mitigação de risco sem interrupção do serviço.</p> <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Incidente cibernético que compromete ativos específicos da rede operativa, mas sem impactos à operação.

6.6.3 Geração:

Criticidade	Descrição
Alta (3)	<p>Indisponibilidade dos sistemas SCADAS críticos. Indisponibilidade no envio de informações críticas para o operador nacional do sistema com esforço máximo para a recuperação ou impossibilidade de recuperação. Indisponibilidade de telecomandos em mais ou igual a 20 aerogeradores da mesma região.</p> <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Ataque cibernético comprometendo a disponibilidade, integridade e confidencialidade de dados do Centro de Operação e ativos que compõem o ARCiber.
Média (2)	<p>Indisponibilidade de equipamentos que atende as redes operativas, Impossibilidade de envio temporário ou não envio de informações não críticas para o operador nacional do sistema. Indisponibilidade de telecomandos em menos de 20 aerogeradores da mesma região e equipamentos de telecomandos infectados com possíveis ações de mitigação de risco sem interrupção do serviço.</p> <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Incidente cibernético que compromete ativos específicos da rede operativa, mas sem impactos a operação.
Baixa (1)	<p>Indisponibilidade de equipamentos que atende as redes operativas, Impossibilidade de envio temporário ou não envio de informações não críticas para o operador nacional do sistema. Indisponibilidade de telecomandos em</p>

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 27 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

	<p>menos de 10 aerogeradores da mesma região e equipamentos de telecomandos infectados com possíveis ações de mitigação de risco sem interrupção do serviço.</p> <p>Os exemplos para essas ocorrências estão descritos, mas não limitados, conforme abaixo:</p> <ul style="list-style-type: none"> - Incidente cibernético que compromete ativos específicos da rede operativa, mas sem impactos a operação.
--	---

6.7 Impacto nos Negócios

O impacto nos negócios deve ser classificado de acordo com os seguintes parâmetros:

6.7.1 Distribuição:


Impacto	Descrição
Alto	<ul style="list-style-type: none"> - Paralisação de distribuição ou geração acima de 4,5 horas de acordo com a DMIC (Duração Máxima de Indisponibilidade Contínua); - Parada de mais de um processo de negócio; - Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 100 mil clientes.
Médio	<ul style="list-style-type: none"> - Paralisação de distribuição ou geração em tempo de 2,5 a 4,5 horas de acordo com a DMIC (Duração Máxima de Indisponibilidade Contínua); - Parada de um processo de negócio; - Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 50 mil clientes.
Baixo	<ul style="list-style-type: none"> - Paralisação de distribuição ou geração em tempo abaixo de 2,5 horas de acordo com a DMIC (Duração Máxima de Indisponibilidade Contínua); - Atraso operacional em um ou mais processos de negócio; - Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 20 mil clientes.

6.7.2 Transmissão:

Impacto	Descrição
Alto	<ul style="list-style-type: none"> - Impacto Financeiro de valor acima de R\$ 100.000,00; - Indisponibilidade de Função de Transmissão acima de 60 minutos; - Parada de mais de um processo de negócio;
Médio	<ul style="list-style-type: none"> - Impacto Financeiro entre R\$ 50.000,00 e R\$ 1.00.000,00; - Indisponibilidade de Função de Transmissão acima de 40 minutos; - Parada de um processo de negócio;
Baixo	<ul style="list-style-type: none"> - Impacto Financeiro abaixo de R\$ 50.000,00; - Indisponibilidade de Função de Transmissão acima de 20 minutos;- - Atraso operacional em um ou mais processos de negócio;

6.7.3 Geração:

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 28 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Impacto	Descrição
Alto	<ul style="list-style-type: none"> - Paralisação de distribuição ou geração acima de 4,5 horas de acordo com a DMIC (Duração Máxima de Indisponibilidade Contínua); - Parada de mais de um processo de negócio; - Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 100 mil clientes.
Médio	<ul style="list-style-type: none"> - Paralisação de distribuição ou geração em tempo de 2,5 a 4,5 horas de acordo com a DMIC (Duração Máxima de Indisponibilidade Contínua); - Parada de um processo de negócio; - Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 50 mil clientes.
Baixo	<ul style="list-style-type: none"> - Paralisação de distribuição ou geração em tempo abaixo de 2,5 horas de acordo com a DMIC (Duração Máxima de Indisponibilidade Contínua); - Atraso operacional em um ou mais processos de negócio; - Indisponibilidade de supervisão e/ou telecomandos em mais de 1 (uma) subestação que, na totalidade, impactem mais de 20 mil clientes.

Tendo sido classificado o incidente, os acionamentos necessários são realizados e as equipes que tratarão o incidente são convocadas.

6.8 Crise Operacional Tático


Caso um incidente de segurança da informação na rede operativa atinja algum dos gatilhos de crise identificados abaixo, o procedimento de Gestão de Crises (GED 17922) do Grupo CPFL deve ser acionado. Os gatilhos de crise devem ser atualizados periodicamente, a fim de facilitar a identificação e necessidade de estabelecimento de outros cenários de crise e o envolvimento de suas respectivas equipes para tratamento. Destacam-se:

- Ataque cibernético envolvendo os ativos do centro de operação, sem mitigação por mais de uma hora;
- Ataque cibernético com impacto na integridade de dados de sistemas SCADA;
- Indisponibilidade de sistemas de segurança de proteção de perímetro com RTO previsto superior a uma hora;
- Indisponibilidade de sistema de segurança de proteção da rede operativa com RTO previsto superior a dezoito horas; e
- Confirmação de incidente de segurança da informação envolvendo vazamento de credenciais.

Com a ocorrência de qualquer um dos gatilhos de crise descritos acima, imediatamente o CISO e/ou Diretor de Tecnologia deverá ser consultado sobre o acionamento do Facilitador de Crise (Dir. de Comunicação).

Na avaliação de um incidente de segurança da informação não mapeado previamente e que se detecte um alto potencial de impacto no negócio, o CISO e/ou Diretor de Tecnologia deverá ser consultado sobre o acionamento do Facilitador de Crise (Dir. de Comunicação).

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 29 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Em um cenário de crise, o Gestor de Continuidade de Negócios deverá ser comunicado para avaliação e, se aplicável, acionamento de PCN. A comunicação deve ser realizada por e-mail e confirmada através de ligação telefônica. O e-mail de comunicação deverá seguir modelo disposto no anexo II e enviado da caixa de e-mails do SOC ou da Equipe de Segurança da Informação.

Para casos de Crise Estratégica, deve ser consultado o documento 17922 (Gestão de Crise).

6.9 Contenção, Erradicação e Recuperação

O propósito da contenção é evitar a exposição e reduzir o risco de impacto promovido por um evento ou incidente de segurança da informação na rede operativa. Existem alguns incidentes como vírus, *worms* ou ataques de código malicioso, que podem propagar-se rapidamente e causar grandes danos. Para o devido tratamento dos incidentes de segurança da informação, estratégias e instruções de trabalho específicas para responder a diferentes eventos e/ou incidentes de segurança da informação devemos consultar o Playbooks OT.

Itens que devem considerar:

- Quaisquer impactos adicionais que possam existir nos sistemas operativos/serviços;
- Tempo e recursos necessários para conter o incidente
- Eficácia da solução de contenção (por exemplo, contenção parcial vs total)
- Duração da permanência da solução (por exemplo, solução temporária vs solução permanente).

A grande maioria dos incidentes de segurança da informação exigem contenção, de modo que considerar esta ação logo no início do tratamento evita que o incidente sobrecarregue os recursos ou aumente os danos causados no ambiente sistêmico da organização. A contenção fornece o tempo necessário para o desenvolvimento de uma estratégia adequada de remediação, reduzindo possíveis danos ao ambiente sistêmico. O plano de recuperação deve especificar a abordagem para a recuperação de redes, sistemas OT e aplicações assim que a contenção e a correção estiverem concluídas.

Ao desenvolver o Plano de Recuperação, deve-se analisar:

- Como os sistemas serão restaurados para a operação normal e prazos esperados?
- Como os sistemas serão monitorados para garantir que não sejam mais comprometidos e estejam funcionando como esperado?

Para cada tipo de incidente deve existir uma instrução de resposta planejada e documentada quando viável, que atenda às necessidades de segurança da informação do Grupo CPFL, levando-se em conta as ameaças envolvidas.


Incidentes não mapeados poderão ocorrer, e neste caso, procedimentos de detecção e resposta a incidentes de segurança da informação adequados deverão ser providenciados consecutivamente, atualizando documentações pertinentes.

6.10 Contenções críticas

Para ações de contenção consideradas críticas na rede operativa, faz-se necessária a aprovação do Gerente de Segurança da Informação e da Operação/Engenharia do Grupo CPFL. São exemplos de contenções críticas:

- Isolamento de segmentos de redes;

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 30 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

- Desativação de serviços de tecnologia (sistemas e softwares); e/ou serviços não essenciais;
- Deslocamento in loco dos times responsáveis;
- Bloqueio de acessos; e
- Retiradas de ativos da rede;

6.11 Contramedidas

Contramedidas também podem ser adotadas para mitigar/evitar continuidade e reincidências de ataques provenientes dos mesmos ofensores na rede operativa. São exemplos de contramedidas:

- Inserção de *blacklists* de plataformas de segurança;
- Inserção de quarentenas de plataformas de seguranças;
- Mapeamento de protocolos e portas e serviços não essenciais;
- Bloqueios via ACL; e/ou
- Reanalise/Varredura do ambiente;


6.12 Comunicação, Notificação de Incidentes de Segurança da Informação e Acionamento de Áreas Correlatas

A comunicação aos stakeholders e priorização será definida pelo líder responsável pelo incidente, e deverá seguir as seguintes premissas:

Stakeholder	Quem lidera o contato
ONS	Regulação Técnica e Comercial, Operação com apoio de Segurança da Informação e aprovação do Grupo de Crise: Time Estratégico (Grupo Executivo) e Pós-Operação (Se necessário)
ANEEL	Regulação Técnica e Comercial, Pós-Operação com apoio de Segurança da Informação e aprovação do Grupo de Crise: Time Estratégico (Grupo Executivo).
Mídia	Comunicação e do Encarregado de Proteção de Dados (se violação ou vazamento de dados pessoais)
Investidores	Relação com Investidores com apoio do Encarregado de Proteção de Dados (se violação ou vazamento de dados pessoais)
SAC	Comercial com o apoio do Encarregado de Proteção de Dados (se violação ou vazamento de dados pessoais)
Delegacia de Crimes Cibernéticos	Segurança da Informação com o apoio do Jurídico e do Encarregado de Proteção de Dados (se violação ou vazamento de dados pessoais)
Clientes externos	Comercial com apoio de Comunicação

Legislação	Quando reportar	Prazo de notificação	Modelo de
------------	-----------------	----------------------	-----------

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 31 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

 <p>CPFL ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT


			notificação
RESOLUÇÃO NORMATIVA A ANEEL Nº 964	<p>Art. 6º Os agentes devem notificar a equipe de coordenação setorial designada dos incidentes cibernéticos de maior impacto que afetem de maneira substancial a segurança das instalações, a operação ou os serviços aos usuários ou de dados.</p> <p>§ 1º A notificação do incidente cibernético de maior impacto deve incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso.</p> <p>§ 2º A notificação do incidente cibernético de maior impacto não exclui o atendimento de outras obrigações de comunicação previstas em leis, normas e regulamentos.</p> <p>§3º A notificação deve ser realizada assim que o agente tiver ciência do incidente e de sua dimensão.</p> <p>III - os dados das equipes de prevenção, tratamento e resposta a incidentes cibernéticos.</p>	No início da etapa do pós-incidente	Carta Sigilosa
Rotina ONS RO- CB.BR.01	<p>4.6.2 item B Todos os alertas devem ser reportados imediatamente à equipe responsável definida na política de segurança do agente;</p> <p>4.6.6. Incidentes cibernéticos que afetem ativos do ARCiber devem ser informados ao ONS;</p>	No início da etapa do pós-incidente	Carta Sigilosa

As regras abaixo de comunicação de incidentes de segurança da informação deverão ser seguidas, levando em conta a criticidade do incidente:

Criticidade	Plano de comunicação
Alta (3)	Resumo a cada 30 minutos às partes envolvidas na fase crítica e a cada hora durante a fase de resolução.
Média (2)	Resumo a cada hora às partes envolvidas na fase crítica e a cada turno na fase de resolução.
Baixa (1)	Resumo diário às partes envolvidas.

O Grupo CPFL deverá notificar a equipe de Coordenação Setorial da ANEEL designada para cuidar dos incidentes cibernéticos de maior impacto, os quais afetam de maneira significativa e

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 32 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

substancial a segurança das instalações, a operação, os serviços aos usuários ou dados dos ambientes e estações. Essa notificação de incidente cibernético de maior impacto incluirá a análise da causa e impacto, bem como incluir as ações mitigatórias que deverão ser anotadas, referente a cada caso.

Assim que, o Grupo CPFL tiver ciência do incidente e de sua dimensão, deverá ser enviada a notificação de incidente cibernético. O envio dessa notificação não exclui a obrigatoriedade do Grupo CPFL ao atendimento e cumprimento das obrigações previstas em leis, normas e regulamentos.

6.13 Coleta de Provas e Processos de Cadeia de Custódia

Ao reunir evidências, mantenha um registro detalhado que documente claramente como todas as evidências foram coletados. Isso deve incluir quem coletou ou manipulou as provas, a hora e a data (incluindo fuso horário) foram coletadas e manuseadas, e os detalhes de cada item coletado (incluindo o localização física, número de série, número do modelo, nome do host, endereço MAC (controle de acesso à mídia), Endereço IP e valores de hash).


Procedimentos para a identificação, coleta de vestígios e evidências, preservação da integridade destas informações e respectiva cadeia de custódia devem ser adotados para que, em caso de necessidade, sejam utilizadas em processos investigatórios ou de cunho forense na rede operativa. Os procedimentos de coleta, manipulação e custódia devem considerar os seguintes tópicos, mas não devem estar limitados a:

- *Backup* de sistemas scada, arquivos, diretórios, bases de dados em mídia/local;
- Cópias de tela de consoles e/ou sistemas de informação;
- Cópia de imagem de estações/servidores virtualizados;
- Relatórios impressos via ferramentas de Segurança;
- E-mails enviados e recebidos;
- Endereços IP;
- Diagrama da rede operativa;
- Arquivos de *log* de auditoria;
- Imagens de CFTV;
- Fotos;
- Utilização de ferramentas para análise forense;
- Documentos abertos pelo Centro de Operações PAE e LST;
- Chats de ferramentas de comunicação interna/externa;

A coleta de evidências será efetuada respeitando procedimentos seguros tanto de coleta como de guarda delas. Nos casos em que houver a necessidade de punição interna, deve contar com um representante do Departamento de Recursos Humanos e/ou Departamento Jurídico dependendo da gravidade do incidente, o Gestor de Segurança da Informação pode optar também pela presença de um auditor externo independente.

A coleta de evidências será efetuada respeitando procedimentos seguros tanto de coleta como de guarda delas. Nos casos em que houver a necessidade de medidas disciplinares, deve contar com um representante do Departamento de Recursos Humanos e/ou Departamento Jurídico dependendo da gravidade do incidente, o Gestor de Segurança pode optar também pela presença de uma consultoria externa independente.

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 33 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

6.14 Confidencialidade de Ocorrências e Incidentes de Segurança da Informação

O conteúdo do evento de segurança da informação de rede operativa deve ser tratado como confidencial e estar restrito somente às equipes responsáveis pelo tratamento do evento. Caso o registro seja anônimo, este deverá restringir-se exclusivamente às equipes responsáveis pelo tratamento, e armazenar os dados das equipes de prevenção, tratamento e resposta do incidente cibernético.

Um termo de confidencialidade (NDA), deverá ser aceito e assinado eletronicamente, logo no início da fase de Tratamento, e sempre que se adicionar alguma parte ao processo. É proibido o uso de celulares na sala de crise. Ao solicitar acesso em alguma subestação ou pop de comunicação não deve ser informado se tratar de um incidente de segurança cibernético.

6.15 Plano de Ação de Remediação

Na etapa de Plano de Ação de Remediação, deve considerar:

- Quais ações são necessárias para resolver o incidente?
- Que recursos são necessários para resolver o incidente (se ainda não estão incluídos no CSIRT)?
- Existem recursos externos adicionais que você pode precisar?
- Quem é responsável pelas ações de remediação?
- Quais sistemas/serviços devem ser priorizados?
- Quais sistemas/serviços serão afetados durante o processo de remediação?
- Como esses sistemas serão afetados?
- Qual o tempo de resolução esperado?

6.16 Centralização e Acionamento/Escalonamento de Áreas Correlatas e/ou externas

A área de Segurança da Informação, para os casos necessários, fará o acionamento dos envolvidos na resposta ao incidente em um War Room.


Contatos apropriados serão mantidos com autoridades, grupos de segurança de stakeholders externos e fóruns que tratem de questões relativas aos incidentes de segurança da informação em rede operativa, somente quando for estritamente necessário.

Após a contenção do incidente, a erradicação pode ser necessária para eliminar componentes do incidente, como exclusão de *malware* e desativação e trocas de senhas de contas de usuário violadas, remoção de ativos de telecomando da rede operativa, bem como auxiliar na identificação e mitigação de todas as vulnerabilidades que foram exploradas. Durante a erradicação, é importante identificar todos os sistemas afetados dentro da organização, a fim de corrigi-los. Para alguns incidentes, a erradicação não é necessária devido a controles e mitigações compensatórias ou é executado durante a etapa de recuperação.

Na etapa de Recuperação, os administradores do ambiente restauram os sistemas para a operação normal, e confirmam se os sistemas estão funcionando corretamente, e caso necessário, corrigem possíveis vulnerabilidades, a fim de evitar a reincidência do incidente ocorrido ou mitigam as vulnerabilidades aplicando restrição de rede e isolamento do contexto.

Existem casos em que a contenção, erradicação e recuperação podem falhar, não acontecer dentro dos requisitos de negócio estabelecidos ou não ser eficaz o suficiente para mitigar o

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 34 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

incidente. Esses casos serão classificados como 'crise' e tratados dentro da Gestão de Crises da organização.

6.16.1 Escalonamento e desescalamento

Nessa tabela abaixo está incluso os gatilhos e/ou limites de escalonamento e desescalamento e as autoridades de tomada de decisão.

Classificação do Incidente	Ação	Gatilhos para escalonamento e desescalada	Nível mínimo de autoridade
Alto (a)	Escalar para Crise	6.6 Criticidade do Incidente	Diretor de Tecnologia
	Desescalar para classificação médio		
Médio (a)	Escalar para Classificação Alta	6.6 Criticidade do Incidente	CSIRT Leader
	Desescalar para Baixo	6.6 Criticidade do Incidente	CSIRT Leader
Baixo (a)	Escalar para classificação Médio	6.6 Criticidade do Incidente	SOC OT

6.17 Atividades Pós-Incidente

Uma das etapas mais importantes no processo de resposta a incidentes de segurança da informação na rede operativa é a aprendizagem e aprimoramento. A equipe de resposta a incidentes deve evoluir para refletir novas ameaças, aprimorar tecnologias e crescer com as 'lições aprendidas'. Reuniões de apresentação das 'lições aprendidas' envolvendo todas as áreas afetadas podem ser extremamente úteis para melhorar as medidas de segurança e o próprio processo de tratamento. A reunião deve, preferencialmente, ser realizada logo após o final do incidente de segurança da informação, e alguns questionamentos serão de extremo valor. Os questionamentos necessários estão descritos no item 6.21 do presente documento. Um *checklist* fornecendo as principais etapas a serem executadas no tratamento de incidentes de segurança da informação pode ser consultado no anexo I. Ao utilizá-lo, o usuário deve se atentar que as etapas podem variar conforme o tipo e natureza do incidente.

Os incidentes devem ter os respectivos registros, as análises da causa e do impacto, bem como o controle dos efeitos de incidentes de maior impacto para as atividades do Grupo CPFL, abrangendo inclusive informações recebidas de empresas prestadoras de serviços a terceiros.


6.18 Análises Pós-incidente

Análise pós-incidente envolve a condução de análise das ocorrências ou incidentes, e as respectivas ações de resposta adotadas para referência futura. Tal procedimento auxilia na obtenção do melhor entendimento das ameaças e vulnerabilidades constatadas, de forma a possibilitar ações de proteções mais efetivas.

Sempre que possível, as análises deverão considerar os seguintes aspectos:

- Ações recomendadas para prevenir futuras ocorrências semelhantes;
- Informação urgente necessária e a forma de obtenção;

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 35 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

- Ferramentas adicionais utilizadas ou necessárias no processo de identificação e erradicação;
- Autonomia na preparação e resposta ao incidente de segurança da informação;
- Comunicação adequada;
- Dificuldades práticas;
- Outras experiências obtidas;
- Tempo de deslocamento até o local do incidente;
- Análise de causa-raiz;
- Revisão/varredura em ambientes similares onde ocorrido o incidente;
- Atualização periódica da planilha de casos de falso-positivo e exceções;
- Revisão dos contatos de acionamento da matriz RACI e árvore de acionamento;

6.18.1 Lições Aprendidas

Uma Revisão Pós-Incidente (PIR) é uma revisão detalhada realizada após ter sofrido um incidente de segurança cibernética na rede operativa. Pode incluir um sendo realizado imediatamente após recuperar redes operativas e sistemas de um incidente de segurança cibernética ou realizado após o relatório do incidente for concluído, como dentro de duas semanas.

Principais perguntas a serem consideradas:

- Quais foram as causas do incidente e quaisquer problemas de resposta a incidentes?
- O incidente poderia ter sido evitado? Como?
- O que funcionou bem na resposta ao incidente?
- Como melhorar nossa resposta para futuros incidentes?


6.19 Análise de Causa-raiz

A análise de causa-raiz é a atividade do processo de tratamento pós-incidente, onde e/ou quando é necessário identificar os reais motivos da causa do incidente de segurança ocorrido. Em geral, os principais motivos de causa-raiz de um incidente de segurança são:

- Falha humana: o ser humano é inerente ao erro. Em um processo em que foram tomadas todas as medidas de segurança e adoção de controles tecnológicos, o fator humano faz parte de uma ação de risco. O erro e falha provocados por um ser humano devem ser considerados;
- Falha de *software*: novas vulnerabilidades ou vulnerabilidades conhecidas que não tenham correções disponibilizadas e aplicadas podem ser a causa-raiz de incidentes de segurança da informação;
- Falha de *hardware*: assim como a falha de *software*, problemas advindos da ausência de atualizações de *firmware* ou mesmo falhas oriundas de superaquecimento e erros de projetos também podem ser causa-raiz de incidentes de segurança da informação; e
- Falha de processo: controles apropriados devem ser aplicados em todas as partes vulneráveis de um determinado processo. Um processo mal desenhado pode ser a causa-raiz de um incidente de segurança da informação.

OBS: Imediatamente após a identificação e validação da causa-raiz, os riscos e controles pertinentes devem ser inseridos no Sistema de Gestão de Riscos do Grupo CPFL, quando aplicável.

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 36 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

6.20 Base de Conhecimento de Incidentes de Segurança da Informação

Os conhecimentos obtidos através da análise e tratamento de incidentes de segurança da informação da rede operativa devem ser documentados e armazenados em repositório e chamados que possibilite sua consulta futura, com intuito de:

- Reduzir a probabilidade ou impactos em incidentes futuros;
- Report de CSIRT;
- Aplicação de MITRE ATT&CK;
- Padrão de Uso e Comportamento da Rede OT;
- Identificar incidentes recorrentes;
- Monitorar e quantificar os tipos, volumes e custos de incidentes de segurança da informação;
- Ser considerado no processo de revisão da Política de Segurança Cibernética;
- Capacitar e conscientizar, através de campanhas de segurança da informação, adotando-se o devido cuidado com a preservação da confidencialidade.

A ocorrência de um incidente cuja detecção e resposta não tenham sido previstos, deverão ser usados como oportunidade de enriquecimento da base de conhecimento de incidentes de segurança da informação do Grupo CPFL e dos casos de uso vigentes.

6.21 Relatório de Incidente de Segurança da Informação (CSIRT report)

O objetivo da documentação é de registrar o incidente contendo todas as informações sobre o timeline e ações tomadas durante a ocorrência, desta forma a Gerência de Segurança da Informação (EIS) fica responsável por criar e atualizar o relatório do Incidente de Segurança da Informação.

Apenas colaboradores autorizados devem ter acesso aos incidentes e o relatório deve ser armazenada em local seguro, com acesso exclusivo da área.

Para documentar o incidente, importante incluir no documento nº do incidente, pessoa responsável, destinatários e prazos.


Os relatórios de situação podem conter as seguintes informações:

- Data e hora do incidente
- Status do incidente
- Tipo e classificação de incidentes
- Escopo e Impacto
- Severidade
- Assistência externa necessária
- Ações tomadas para resolver o incidente
- Dados de contato para o Gerente de Segurança da Informação e o pessoal-chave do CSIRT
- Data e hora da próxima atualização.

Ao finalizar a análise de um incidente de segurança da informação classificado como de criticidade Alta, uma reunião deverá ser realizada entre os envolvidos no tratamento do incidente, a fim de determinar os seguintes pontos:

- Exatamente o que aconteceu e em que momento;
- Como a equipe e sua coordenação se saíram durante o tratamento do incidente de segurança?;
- Todos os procedimentos efetuados durante a análise do incidente de segurança foram devidamente documentados?;

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 37 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

- Os procedimentos efetuados foram adequados?;
- Os procedimentos efetuados foram seguidos?;
- Quais localidades e região da Rede OT ocorreu o incidente?
- Durante o tratamento do incidente, foi possível identificar a necessidade de informações não antes mapeadas?;
- Foram identificadas ações indevidas durante o processo, que acabaram por inibir a devida recuperação do ambiente?;
- Quais ações poderão ser aprimoradas para o tratamento de incidente semelhante?;
- Como o compartilhamento de informações com outras organizações e/ou entidades pode auxiliar na melhoria do processo de tratamento do incidente de segurança da informação?;
- O incidente de segurança da informação ocorrido foi necessário a comunicação junto aos órgãos reguladores? (ONS/Aneel)
- Quais ações corretivas foram identificadas de forma a evitar ou diminuir sensivelmente a ocorrência futura de incidentes de segurança da informação semelhantes?;
- Quais precursores ou indicadores devem ser observados futuramente para detecção de incidentes de segurança da informação semelhantes?; e
- Quais ferramentas e/ou recursos adicionais serão necessários para detectar, analisar e mitigar incidentes de segurança da informação futuros?

6.22 Parecer, Recomendações de Segurança

Com base no relatório final de incidente de segurança da informação, ações preventivas deverão ser conduzidas, a fim de evitar a recorrência do incidente identificado.

Fica a critério da área de Segurança da Informação, avaliar se o incidente tratado será divulgado para as demais áreas do Grupo CPFL ou se tal informação será apresentada apenas no âmbito da Diretoria. A divulgação externa dos registros efetuados necessita de aprovação por parte do Comitê de Segurança da Informação.


Caso de incidentes de segurança da informação com impacto no ambiente ARCiber ou envio de informação crítica para ONS a comunicação para a agência reguladora ANEEL deve ser realizada pela equipe de Regulatório do Grupo CPFL com apoio de Segurança da Informação e aprovação do Grupo de Crise: Time Estratégico (Grupo Executivo).

6.23 Melhoria Contínua

Todas as oportunidades para melhoria do ambiente sistêmico devem ser aproveitadas, com base nos incidentes ocorridos. Aspectos de segurança como prevenção, detecção e resposta a incidentes podem e devem ser aprimorados. Minimamente, as oportunidades abaixo deverão ser avaliadas no pós-incidente, visando o aspecto de melhoria contínua:

- Avaliações de risco;
- Mapeamento do ambiente;
- Segurança de ativos de tecnologia;
- Segurança da rede de computadores;
- Acesso físico aos equipamentos;
- Pentests internos para segurança do ambiente;
- Tempo de deslocamento para cada base;
- Equipamentos obsoletos e sem contatos de suporte;
- Conscientização, exercícios e treinamento de usuários.

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 38 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

7. CONTROLE DE REGISTROS


Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Não aplicável	Não aplicável	Não aplicável	Não aplicável	Não aplicável	Não aplicável

8. ANEXOS

Anexo I – Checklists Rede Operativa


Contato Fornecedores				
#	Fornecedor / Ferramenta	Responsável	Contato	Equipe
1	Nava	Guilherme Nascimento (Gerente de Contas)	guilhermes.nascimento@nava.com.br 11 91165-3723	Operação Arquitetura
		Wesney Silva (Suporte Fortigate)	wesney.silva@nava.com.br mss@nava.com.br 11 99940-4526	
		Marcelo Cardelli de Camargo (Suporte Fortigate)	marcelo.cardelli@nava.com.br mss@nava.com.br 11 98765-1613	
2	Deloitte	Renato Fugazza (Gerente de Conta)	rfugazza@deloitte.com 11 97202-0657	IDM
3	Microsoft	Marco Monteiro (Gerente de Conta)	mmonteiro@microsoft.com 21 99465-3009	Operação
4	Telecom	Saturnino Pereira (Gerente Técnico)	saturnino.pereira@atelecom.com.br 61 3316-4030	Operação
		Joao Ricardo (Gerente de Projetos)	joao.ricardo@atelecom.com.br 61 3316-4042 61 99176-0949	
5	Cloudflare	Jorge Vergés (Gerente de Contas)	jverges@cloudflare.com +1 561 4796660	Operação Arquitetura
		Suporte	support@cloudflare.com 49495922	
6	Cisco	Patricia Rosas (Gerente de Contas)	parosas@cisco.com 21 97629-7233	Operação Arquitetura
		Suporte a Firewall	0 800 891 4972	

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 39 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

 <p>CPFL ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

7	Algosec	Anderson Matias Mello (Gerente de Contas)	anderson.mello@algosec.com 11 98734-7225	Arquitetura
		Suporte Algosec	https://portal.algosec.com/en/support/my_support_cases	
8	Compugraft	Sergio Petená (Gerente de Contas)	sortez@compugraf.com.br 11 98437-4140	Arquitetura
		Suporte	atendimento@compugraf.com.br 11 3323-3322	
9	Senha Segura	Suporte	https://suporte.senhasegura.com.br/ 11 3069-3930	GRC
		Felipe Maia (Coordenador de Suporte)	11 94274-2766	
		Vinicius Roiz (Coordenador de Serviços)	11 98787-6057	
		Pablo Ocerin (Gerente de Tecnologia)	11 97090-2449	
10	Axur	Camila Farias (Gerente de conta)	camila.farias@axur.com 51 99321-1909	Threat Intel
		Thiago Bordini (CISO)	thiago.bordini@axur.com 11 97037-5801	
11	Scorecard	Fabio Maciel (Solutions Architect)	fabio.maciel@securityscorecard.io 57 315 276 3626	Threat Intel
12	Rapid7	Marco Valdes (Gerente Sênior de Sucesso do Cliente)	marco_valdes@rapid7.com	Threat Intel
		Natalia Fernandino (Executivo de Contas)	natalia_fernandino@rapid7.com	
13	TrustSis Consultoria	Claudio Rocha (Sócio Diretor Comercial)	claudio.rocha@trustsis.com 11 98962-1019	GRC
		William Pantaleão (Socio diretor Operacional)	william.pantaleao@trustsis.com 11 98042-6696	
		Marco Jacomini (Gerente Geral AMS)	marco.jacomini@trustsis.com 11 98679-0205	

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 40 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------


	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

	Débora Mulatinho (Arquitetura e Compliance)	debora.mulatinho@trustsis.com 21 99888-2475	
	Thalles Horovitz (Gestor Demandas)	thalles.horovitz@trustsis.com 11 99731-9288	
	Fagner Perez (Gestor Operação)	fagner.perez@trustsis.com 11 96144-0504	

Checklist de Ações - Tratamento de Incidentes de Segurança da Informação		
#	Ação	Tempo
1.	Isolar os sistemas	Primeira Hora
2.	Preservar e garantir que o backup esteja integro e funcional	Primeira Hora
3.	Identificar ameaça e ponto de entrada	Segunda Hora
4.	Identificar os sistemas afetados	Terceira Hora
5.	Definição de hipóteses para solução do incidente e testes	Mesmo dia
6.	Mitigar a ameaça	Mesmo dia
7.	Restaurar os sistemas afetados em um ambiente de quarentena	Mesma semana
8.	Hardening do ambiente de quarentena	Mesma semana
9.	Migrar ambiente para produção	Mesma semana
10.	Lições aprendidas e correções definitivas	Em 15 dias

Checklist de Ações - Tratamento de Incidentes de Segurança da Informação		
#	Ação	Status
Deteccção e Análise		
1.	Determinar se ocorreu um incidente	
1.1	Análise dos precursores e indicadores	
1.2	Busca de informações correlatas	
1.3	Realizar pesquisas (ex. mecanismos de pesquisa, base de conhecimento)	
1.4	Após validar a ocorrência do incidente, iniciar e documentar a investigação e coleta de evidências	
2.	Priorizar o tratamento do incidente com base nos fatores relevantes (impacto funcional, informações de impacto, esforço para recuperação do ambiente etc.)	
3.	Reportar o incidente internamente e aos participantes e demais entidades externas apropriados	
4.	Abrir uma Sala de Crise convidando os respectivos stakeholders envolvidos na resposta do incidente.	
Contenção, Erradicação e Recuperação		
5.	Adquirir, preservar, proteger e documentar as evidências	


N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 41 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	---------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

6.	Conter o incidente	
7.	Erradicar o incidente	
7.1	Identificar e mitigar todas as vulnerabilidades que foram exploradas	
7.2	Remover <i>malware</i> , artefatos inadequados e demais componentes	
7.2.1	Caso não seja possível remoção de malware, tomar ações de mitigação do risco	
7.3	Se outros <i>hosts</i> afetados forem descobertos, como por exemplo novas infecções por <i>malware</i> , repetir a etapa de 'Detecção e Análise' e então avançar para a etapa de 'Contenção, Erradicação e Recuperação'.	
8.	Recuperação do incidente	
8.1	Retornar os sistemas afetados ao seu estado normal de operação	
8.2	Confirmar se os sistemas afetados estão funcionando corretamente	
8.3	Se necessário, implementar monitoramento adicional, a fim de procurar atividades futuras relacionadas ao incidente.	
Atividades Pós-incidente		
9.	Realizar e acompanhar ações de médio e longo prazo definidos durante a fase de "Recuperação"	
10.	Criar um relatório de acompanhamento	
11.	Realizar reunião de 'Lições Aprendidas'	

Preparação da Resposta a Incidentes		
Item	Descrição	Status
Comunicação e Facilities para a resposta a incidentes		
1	Informações de contato da Rede OT (Incluindo empresas da Transmissão, Distribuição e Geração)	
2	Escalation contact list	
3	Mecanismos de reporte do incidente (tels, email, app de comunicação)	
4	Comunicação de incidente crítico/alto junto a ONS	
5	Sistema para registro do Incidente	
6	War Rooms para comunicação central e coordenação	
7	Sistema para armazenamento das evidências	
Hardware e Software para Análise do Incidente (jump kit)		
1	Equipamentos para forense e backups (preservação)	
2	Equipamentos para análise e testes	
3	Outros equipamentos (portáteis)	
4	Analizador de protocolos e sniffers	
5	Softwares para forense	
6	Equipamentos para coleta e armazenamento de evidências	
Recursos para Análise do Incidente (jump kit)		
1	Port lists, incluindo mais usadas por malwares	

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 42 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------


	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

2	Documentação (OS, protocolos, IDS/IPS, AV, ..)	
3	Baselines	
4	Diagramas de Redes e lista de assets críticos	
5	Hashes dos arquivos críticos (para acelerar a resposta ao incidente)	

Checklist de Ações - Estratégicas, Informativas e Lembretes			
#	Ação	Fornecedor / Ferramenta	Equipe
1	Acionar Fornecedores	Nava	Operação Arquitetura
2	Acionar Fornecedores	Deloitte	IDM
3	Acionar Fornecedores	Microsoft	Operação
4	Acionar Fornecedores	Cloudflare	Operação Arquitetura
5	Acionar Fornecedores	Cisco	Operação Arquitetura
6	Acionar Fornecedores	Compugraft	Arquitetura
7	Acionar Fornecedores	Senha Segura	GRC
8	Acionar Fornecedores	Axur	Threat Intel
9	Acionar Fornecedores	Scorcard	Operação
10	Acionar Fornecedores	Rapid7	Operação
11	Acionar Fornecedores	TrustSis	GRC
12	Decisão de derrubar a interface externa do Firewall (Internet)	-	Blue Team
13	Cadastrar os IOCs coletados	ATP / SIEM / Firewall / WAF	Blue Team
14	Lembre-se dos demais DataCenters - Jundiai / SUL / DR	-	Todos
15	Confirmar os últimos backups	DataCenters e Azure	Todos
16	Alterar todas as senhas	AD / Azure AD / Plataformas afetadas	Blue Team

Checklist de Ações - Momento De Um Incidente			
WAF (Web Application Firewall)			
#	Ação	Ambiente	Equipe
1.1	Alterações nos últimos dias	CyberVision	Blue Team
1.2	Análises de IPs suspeitos - Reputação - Atividades	CyberVision	Blue Team
1.3	Análises de IPs suspeitos - Reputação - E-mail	CyberVision	Blue Team
1.4	Comportamento anormal de DDoS	CyberVision	Blue Team
1.5	Comportamento anormal em todas as URLs	CyberVision	Blue Team


N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 43 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	---------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

1.6	Habilitar motivação de atividade suspeita	CyberVision	Blue Team
1.7	O que foi bloqueado	CyberVision	Blue Team
1.8	Se suspeita de ataque ativar UNDER_ATTACK	CyberVision	Blue Team
1.9	Verificar logs de qual transação foi aceita	SIEM	Blue Team
1.10	Verificar se foi alterada algumas regras de bloqueio	CyberVision	Blue Team
1.11	Verificar se há alguma credencial inclusa ou alterada	CyberVision	Blue Team
AntiDDoS			
2.1	Habilitar notificação de atividade suspeita	FMC	Blue Team
Windows Server e Estação			
3.1	Avaliar a necessidade de clonar a máquina	Local	Blue Team
4.1	Certifique-se de que o sistema não foi movido para um grupo de trabalho ou domínio diferente.	Local / AD	Blue Team
4.2	Examine as tarefas executadas pelo serviço do TaskManager	Local	Blue Team
4.3	Examine os arquivos de log e eventos.	Local / CyberVision / SIEM	Blue Team
4.4	Examine todas as conexões / sistemas /hosts que o ambiente se comunicou - Interno e Externo	CyberVision	Blue Team
4.5	Procure associações de grupo incorretas.	Local	Blue Team
4.6	Procure direitos de usuário incorretos.	Local / CyberVision / SIEM	Blue Team
4.7	Procure por arquivos incomuns ou ocultos.	Local	Blue Team
4.8	Verifique a configuração e a atividade da rede.	Local / CyberVision / SIEM	Blue Team
4.9	Verifique se há aplicativos não autorizados a partir da inicialização.	Local	Blue Team
4.10	Verifique se há compartilhamentos não autorizados.	Local/CyberVision	Blue Team
4.11	Verifique se há contas de usuários e grupos estranhos.	Local	Blue Team
4.12	Verifique se há permissões alteradas em arquivos ou chaves de registro.	Local / CyberVision / SIEM	Blue Team
4.13	Verifique se há processos não autorizados e processos suspeitos	Local / SysInternals	Blue Team
Linux e Unix			
5.1	Análise a intrusão	CyberVision	Blue Team
5.2	Buscar a mesma vulnerabilidade nos demais Assets	CyberVision	Blue Team

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 44 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

5.3	Examine as tarefas executadas pelo serviço crontab	-	Blue Team
5.4	Examine as tarefas executadas pelo serviço em execução (PS)	-	Blue Team
5.5	Examine os arquivos de log e eventos.	SIEM	Blue Team
5.6	Examine todas as conexões / sistemas /hosts que o ambiente se comunicou - Interno e Externo	CyberVision	Blue Team
5.7	Procure associações de grupo incorretas.	-	Blue Team
5.8	Procure direitos de usuário incorretos.	-	Blue Team
5.9	Procure ferramentas e dados deixados pelo intruso.	-	Blue Team
5.10	Procure modificações feitas no software do sistema e nos arquivos de configuração.	-	Blue Team
5.11	Procure modificações nos dados.	-	Blue Team
5.12	Procure por arquivos incomuns ou ocultos.	-	Blue Team
5.13	Procure sinais de um Sniffer de rede.	CyberVision	Blue Team
5.14	Recupere o controle do sistema. Algumas opções incluem desconectar o sistema da rede e fazendo uma cópia de imagem do (s) disco (s) do sistema.	-	Blue Team
5.15	Revise os arquivos de registro.	-	Blue Team
5.16	Verifique a configuração e a atividade da rede.	CyberVision	Blue Team
5.17	Verifique os binários do sistema com algo como Tripwire.	-	Blue Team
5.18	Verifique os sistemas afetados em outras sub redes locais ou sites remotos.	CyberVision	Blue Team
5.19	Verifique outros sistemas na rede local.	CyberVision	Blue Team
5.20	Verifique se há alterações nas políticas do usuário ou do computador.	-	Blue Team
5.21	Verifique se há aplicativos não autorizados a partir da inicialização.	-	Blue Team
5.22	Verifique se há compartilhamentos não autorizados	-	
5.23	Verifique se há contas de usuários e grupos estranhos.	-	
5.24	Verifique se há permissões alteradas em arquivos ou chaves de registro.	-	
5.25	Verifique se há processos não autorizados.	-	
Ambiente Rede Operativa			
6.1	Checar se teve algum alerta que está no Firewall procedente deste ambiente	Firewall	Blue Team
6.2	Checar se teve algum alerta que está no CyberVision procedente deste ambiente	Cyber Vision	Blue Team
6.3	Checar se teve algum alerta que está no FortiNet procedente deste ambiente	Fortinet	Blue Team


 <p>CPFL ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

6.4	Checar se teve algum alerta que está no Cofre de Senhas procedente deste ambiente	Cofre de senhas	Blue Team
NAC			
7.1	Em implementação	Fortinac	Arquitetura
SIEM			
8.1	Analisar Dashboards	SIEM	Blue Team
8.2	Investigar os alertas	SIEM	Blue Team
8.3	Investigar os logs	SIEM	Blue Team
SCANS			
9.1	Avaliar a necessidade de fazer um SCAN pontual	IVM	Red Team
Cofre de Senha			
10.1	Checar se senhas estão integro	Cofre de Senhas	GRC
Usuário			
10.1	O que o usuário estava fazendo durante o incidente?		Todos
10.2	O usuário notou alguma coisa estranha no computador nessa época?		Todos
10.3	O usuário recebeu alguma atualização de software?		Todos
10.4	O usuário percebeu uma mudança no desempenho do computador?		Todos
10.5	O usuário usa o computador para funções não relacionadas ao trabalho?		Todos
10.6	Em caso afirmativo, qual (is) função (ões)?		Todos

Anexo II - Modelo de E-mail

Enviado de:	
Enviado para:	
Assunto:	
Prioridade:	
Ticket:	
Afetação:	
Resumo inicial:	
Impacto:	
Próxima comunicação:	

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 46 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

 <p>CPFL ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Anexo III - Protocolo de Comunicação de Incidente de Segurança da Informação da Rede Operativa

Classificação: Confidencial

Tipo de Comunicação

- ☐ Completa
☐ Parcial


Se comunicação parcial:

- ☐ Preliminar
☐ Complementar

Descrição do Incidente
Descreva de forma resumida como o incidente de segurança da informação ocorreu.
[Resposta.]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após ciência do incidente?
[Resposta].

Contato em caso de dúvidas		
Nome	Telefone/Ramal	E-mail
[Nome].	[Telefone/Ramal].	[E-mail].

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Anexo IV - Termo de Confidencialidade – Partes envolvidas

Utilizar o modelo abaixo como um acordo de sigilo e confidencialidade, para todos que atuarem na tratativa de um incidente de Segurança da Informação ou Privacidade. Poderá ser enviado por e-mail, com a resposta também eletrônica do aceite do termo.

Assunto do e-mail:

[Acordo de Sigilo] Incidente de Segurança da Informação - <<DATA/HORA>>

ACORDO DE CONFIDENCIALIDADE – INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Eu, _____, portador da identidade RG nº _____, expedido pelo órgão _____, ocupante do cargo _____, comprometo-me a:

a) Tratar com estrita confidencialidade toda informação, documentada ou não, recebida ou obtida por mim durante minha participação no tratamento deste incidente;

b) Não revelar, não divulgar, não reproduzir, não publicar constatações, relatórios, pareceres, conclusões, resultados das atividades executadas e quaisquer outras informações referentes a este incidente, das quais tenha participado ou tive acesso, e que devem ficar restritas ao grupo envolvido nas atividades de tratamento.


c) Como consequência da minha adesão a este acordo, permito o monitoramento da Empresa no que se refere ao meu uso dos Recursos de TI por esta disponibilizados pela CPFL.

Declaro estar ciente de que uma violação deste acordo poderá resultar em uma ação disciplinar, dependendo dos fatores envolvidos, assim como obrigações civis e criminais.

Campinas, _____ de _____ de _____

Assinatura

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 48 de 50
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	------------------------

 <p>CPFL ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Anexo V – Canais de Notificação de Incidentes

Canal	Situação	Detalhes
Notificação Interna	Quebra das Políticas de Segurança da Informação e/ou Políticas de Privacidade do Grupo CPFL	seginfo@cpfl.com.br.
Equipe de coordenação o setorial designada dos incidentes cibernéticos de maior impacto que afetem de maneira substancial a segurança das instalações, a operação ou os serviços aos usuários ou de dados Aneel		Enviar tudo o que está acontecendo na sala como confidencial
	Reposta e Tratamento de Incidentes de Segurança no Brasil	CERT.br - Centro de Estudos, Reposta e Tratamento de Incidentes de Segurança no Brasil http://www.cert.br

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome	Data
Paulista	EIS	Mateus Rocha	01/06/2023
Paulista	EIS	Leandro Carmo	01/06/2023
Renováveis	EIS	Emerson Cardoso	01/06/2023
RGE	EIS	Victor Bastos	01/06/2023

N.Documento: 19521	Categoria: Tático	Versão: 2.0	Aprovado por: Emerson Cardoso	Data Publicação: 26/12/2023	Página: 49 de 50
-----------------------	----------------------	----------------	-------------------------------------	-----------------------------------	------------------------

Tipo de Documento: Procedimento

Área: EIS-GERENCIA DE SEGURANCA DE TI

Título do Documento: Plano de Resposta a Incidentes de Segurança da Informação rede OT

Piratininga	ROP	Rolands Sarreta Menezes	20/09/2023
RGE	ROS	Rodrigo Bertani	20/09/2023
Piratininga	ROPT	Rodrigo Mazo Rocha	20/09/2023
Paulista	ROP	Alexandre Rodrigues Lopes	20/09/2023
Paulista	ROP	Luiz Carlos Bigon	20/09/2023
CPFL-T	MOO	José Eduardo M. Cereja	20/09/2023
CPFL-T	MOO	Júlio de Azambuja Borges	20/09/2023

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não aplicável	Não aplicável	Documento em versão inicial
1.0	10/07/2023	Revisão geral do documento