 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento Perda de Equipamento de TI

Sumário

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

1.OBJETIVO

Procedimento a ser seguido quando houver perda/furto ou roubo de equipamentos de TI.

2.ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas do **Grupo CPFL**.

2.2. Área

Todas as áreas do **Grupo CPFL**.

3.DEFINIÇÕES

MFA: Multi Factor Authentication é um método para autenticação onde exige do usuário informar dois ou mais fatores de confirmação para acessar algum recurso computacional.


SOC: Security Operations Center, Centro de Operações de Segurança) Trata-se de uma forma de denominar a plataforma que registra qualquer problema de segurança digital. Com muita agilidade, o sistema também recolhe, armazena e analisa relatórios para corrigir qualquer vulnerabilidade.

WIPE: Limpeza do sistema operacional do seu dispositivo, ou seja, uma parte da memória interna do seu smartphone é apagada.

4.DOCUMENTOS DE REFERÊNCIA

- Diretrizes de Segurança da Informação (GED 14369)
- Norma de Classificação da Informação (GED 18744)

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19302	Instrução	1.0	Emerson Cardoso	14/09/2022	1 de 6

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento Perda de Equipamento de TI

5. RESPONSABILIDADES

Colaborador

- Comunicar superior imediato sobre a perda/furto/roubo imediatamente

Gestor imediato

- Comunicar Segurança da Informação sobre o ocorrido;
- Solicitar novo equipamento;

Segurança da Informação

- Realizar o Checklist de Ações desse procedimento;


Time EndUser

- Realizar as ações solicitadas pelos times internos;

6. REGRAS BÁSICAS

Checklist de Ações		
#	Ação	Status
Furto		
1.	Suspender a conta do usuário prejudicado	
2.	Solicitar o reset da conta do usuário (ANEXO I)	
3.	Colocar a máquina em estado de isolamento para iniciar investigação (Buscar dispositivo no 365 Defender, reticências, Isolar Dispositivo) (ANEXO II)	
4.	Valida quais usuários que estão logados na máquina nos últimos 30 dias (Security)	
5.	Retira a máquina em estado de isolamento (Buscar dispositivo no 365 Defender, reticências, Isolar Dispositivo) (ANEXO II)	
6.	Ativar WIPE (Solicitar exclusão completa dos dados do dispositivo por meio do Intune (ANEXO III)	
7.1	Validar se usuário tem MFA ativado (ANEXO IV)	
7.2.	Caso não esteja ativado, ativar.	
8.	Ativar monitoramento com as regras de monitoramento do dispositivo. (ANEXO V)	
9.	Ativar a conta novamente	
10.	Comunicar o time de N1 em casos de alertas. (soc@nava.com.br)	
Roubo		
1.	Suspender a conta do usuário prejudicado	
2.	Solicitar o reset da conta do usuário	
3.	Colocar a máquina em estado de isolamento para iniciar investigação	

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19302	Instrução	1.0	Emerson Cardoso	14/09/2022	2 de 6


 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento Perda de Equipamento de TI

4.	Valida quais usuários que estão logados na máquina nos últimos 30 dias (Security)	
5.	Retira a máquina em estado de isolamento (Buscar dispositivo no 365 Defender, reticências, Isolar Dispositivo) (ANEXO II)	
4.	Ativar WIPE (Solicitar exclusão completa dos dados do dispositivo por meio do Intune (ANEXO III))	
5.1	Validar se usuário tem MFA ativado	
5.2.	Caso não esteja ativado, ativar.	
5.3.	Solicitar reset do MFA	
6.	Validar últimas ações/acessos/validar logs	
7.	Ativar monitoramento com as regras de monitoramento do dispositivo.	
	Ativar a conta novamente	
8	Comunicar o time de N1. (soc@nava.com.br)	

Checklist de Ações - Estratégicas, Informativas e Lembretes

#	Ação	Equipe/Pessoa
1.	Comunicar o incidente com o equipamento ao superior imediato	Colaborador
2.	Comunicar Segurança da Informação (seginfo@cpfl.com.br) e abrir chamado solicitando novo equipamento.	Gestor imediato/Colaborador
3.	Solicitar a suspensão da conta do usuário prejudicado	Blue Team
4.	Suspender a conta do usuário prejudicado	EndUser
5.	Solicitar o reset da conta do usuário	Blue Team
6.	Resetar a senha da conta do usuário	EndUser
6.1	Colocar a máquina em estado de isolamento (Buscar dispositivo no 365 Defender, reticências, Isolar Dispositivo)	Blue Team
6.2.	Ativar WIPE	Blue Team/SOC Nava N3
6.3.	Abrir chamado para (TI_Suporte_N2_Windows) solicitando a exclusão completa dos dados do dispositivo, por meio do Intune. (ANEXO III)	Blue Team
6.4.	Atendimento do chamado da solicitação 6.3	SOC N3 Nava
6.5.	Validar se usuário tem MFA ativado	Blue Team
7.	Ativar MFA (Dentro de Grupos no AAD, usuário tem que estar no grupo de MFA)	Blue Team/Infraestrutura TI
8.	Solicitar reset do MFA	Blue Team
9.	Resetar MFA da conta	Infraestrutura TI
10	Validar últimas ações/acessos/validar logs	Blue Team
11	Ativar monitoramento com as regras de monitoramento do dispositivo.	Blue Team
12	Comunicar o time de N1. (soc@nava.com.br)	Blue Team
13.	Entrega do novo equipamento	EndUser

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19302	Instrução	1.0	Emerson Cardoso	14/09/2022	3 de 6

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento Perda de Equipamento de TI


7.CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Norma de SI	Eletrônico (GED)	Restrição de acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

8.ANEXOS

ANEXO I

Assunto

 SI (Incidente) - Incidentes de Segurança

Título +


! Reset de Senha

Descrição


Bom dia.

Colaborador teve seu computador corporativo furtado. Peço a gentileza de resetar a senha vinculada a conta:
Vitor Halter Andrade - vitor.andrade@cpfl.com.br
Matricula 02015809

Grupo de Suporte *

 TI_Perfil_AD

ANEXO II



n21026402

Ativo

Confidencialidade de dad...

Ativo

Gerenciar marcas

Ir para a busca

Isolar dispositivo

Restringir a execução do aplicativo

Executar a verificação de antivírus

Dispositivo resumo

<

Visão geral

Alertas


Cronograma

Reco

ANEXO III

Chamado

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19302	Instrução	1.0	Emerson Cardoso	14/09/2022	4 de 6

 Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento Perda de Equipamento de TI

Assunto

SI (Incidente) - Incidentes de Segurança

Título *

Wipe do Dispositivo

Descrição *

Boa tarde,

Conforme SC-4625384-P6K6N0 o dispositivo N21026402 foi furtado e mediante a isso é requisitada a exclusão completa dos dados do dispositivo através do Intune. Realizar WIPE completo.

Fila

Grupo de Suporte *

TI_Suporte_N2_Windows

Opção Intune

Desativar Apagar Excluir Bloqueio remoto Sincronizar Redefinir senha Reiniciar Coletar o diagnóstico

Tem certeza de que deseja apagar N21026402

A restauração de fábrica retorna o dispositivo às configurações padrão. Ela remove todos os dados pessoais e corporativos, bem como todas as configurações do dispositivo. Você pode escolher se deseja manter este dispositivo registrado e a conta de usuário associada a ele. Você não poderá reverter esta ação. Tem certeza de que deseja reiniciar este dispositivo?


☐ Apagar o dispositivo, mas manter o estado de registro e a conta de usuário associada

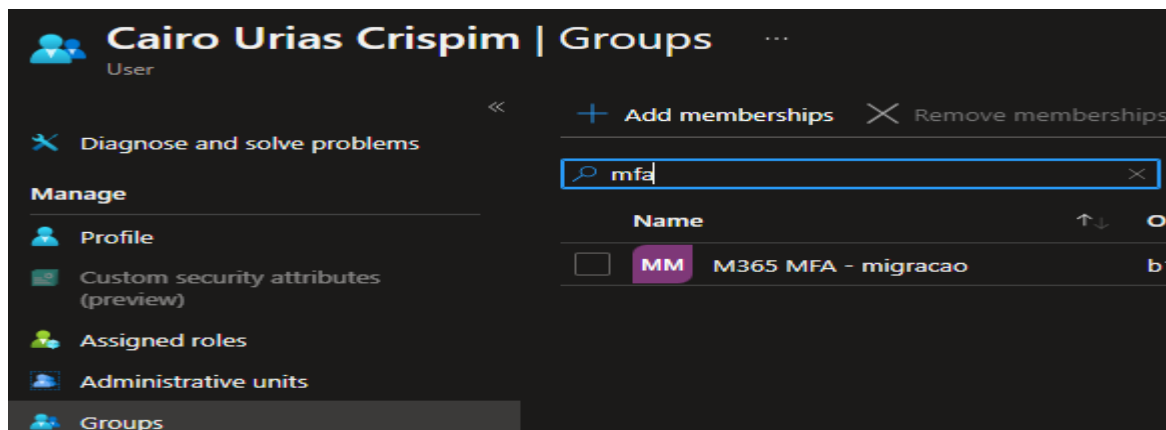
☐ Apague o dispositivo, e continue a apagar mesmo que o dispositivo fique sem energia. Se você selecionar esta opção, saiba que ela pode impedir que alguns dispositivos executando o Windows 10 e posteriores sejam reiniciados.

Apagar Cancelar

ANEXO IV

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19302	Instrução	1.0	Emerson Cardoso	14/09/2022	5 de 6

 <i>Uso Interno</i>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento Perda de Equipamento de TI



ANEXO V

<input type="checkbox"/> Severity ↑↓	↑↓ Name ↑↓	Rule type ↑↓	Status ↑↓
<input type="checkbox"/> High	Monitoramento de Conta Comprometida	Scheduled	Enabled
<input type="checkbox"/> High	Monitoramento de Dispositivo Furtado	Scheduled	Enabled

ANEXO VI

PLAYBOOK.XLS

9.REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIS	Mateus Augusto Pereira Rocha
Paulista	EIS	Cairo Urias Crispim
Paulista	EIS	Felipe Rafael de Almeida

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não aplicável	Não aplicável	Documento em versão inicial

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19302	Instrução	1.0	Emerson Cardoso	14/09/2022	6 de 6