SISPREV-TO

Contingência

INTERRUPÇÃO DE ERNERGIA ELÉTRICA

ACIONAR O ADMINISTRADOR DO EDIFÍCIO SATÉLITE, A LOCATTO IMÓVEIS OU EMPRESA ENERGÉTICA FORNECEDORA, CONVOCAR ELETRICISTA → VERIFICAR SE AUTONOMIA DOS NOBREAKS DO DATA CENTER E DOS USUARIOS QUE POSSUEM NOOBREAK FOI ACIONADA → VERIFICAR ORIGEM E REESTABELECER A ENERGIA → FIM

FALHA NO SISTEMA WEB DO INTITUTO

O SISTEMA WEB DO INSTITUTO É GERENCIADO ATUALMENTE PELA ASPPREV → VERIFICAR SE ORIGEM DA FALHA É NA REDE DO INSTITUTO → CASO CONFIRME FALHA NO SITEMA ASPPREV, COMUNICAR PARA QUE RESTABELEÇAM ACESSO DO INTITUTO → FIM

FALHA DE ACESSO A PASTA CENTRAL DA REDE

VERIFICAR ORIGEM DA FALHA

- ESTRUTURA INTERNA DA REDE → ESTRUTURA DE REDE DO SISPREV
- REDE ISOLADA → CONFIGURAÇÃO DE REDE ESTAÇÃO
- HARDWARE → IR PARA FALHAS DE HARWARE

ESTRUTURA DE REDE DO SISPREV / CONFIGURAÇÃO DE REDE ESTAÇÃO → RESTAURAR CONFIGURAÇÕES DE REDE DE ACORDO COM O MANUAL → FIM

COMPROMETIMENTO DOS ARQUIVOS DA PASTA CENTRAL DE REDE

VERIFICAR CAUSA

- ATAQUES CIBERNÉTICOS
- ATAQUES INTERNOS
- FALHA DE HARWARE

ATAQUES CIBERNÉTICOS / ATAQUES INTERNOS / FALHA DE HARWARE → RESTAURAR CONFIGURAÇÕES DE REDE DE ACORDO COM O MANUAL → FIM

- DESAPARECIMENTO DE ARQUIVOS → VERIFICAR SE FOI MOVIDO PARA OUTRA PASTA → RESTAURAR ARQUIVOS NECESSÁRIOS A PARTIR DE ÚLTIMO BACKUP VÁLIDO → FIM

ATAQUES INTERNOS

DESLIGAR EQUIPAMENTOS COM BACKUPS → IDENTIFICAR ORIGEM DO ATAQUE → BLOQUEAR ACESSO DO ATACANTE → CHECAR COM FUNCIONARIOS POSSIBILIDADE DE CONHECIMENTO DE SENHA DE ACESSO DE OUTROS USUÁRIOS → RELIGAR BACKUPS → VERIFICAR QUAIS DADOS FORAM AFETADOS → RESTAURAR BACKUPS → FIM

ATAQUES CIBERNETICOS

VERIFICAR TIPO DE MALWARE

- RANSONWARE → COMUNICAR AOS FUNCIONARIOS DO INSTITUTO → DESLIGAR TODOS OS COMPUTADORES → IDENTIFICAR DADOS COMPROMETIDOS → IDENTIFICAR MAQUINAS INFECTADAS → RESTAURAR MAQUINAS → RESTAURAR ARQUIVOS DO BACKUP INTEGRO → FIM
- DEMAIS MALWARES → DESLIGAR SERVIDOR DHCP → VERIFICAR INTEGRIDADE SERVIDORES → IDENTIFICAR QUAIS MAQUINAS FORAM INFECTADAS → REMOVER MAQUINAS INFECTADAS FISICAMENTE DA REDE → REMOVER MALWARE DAS MAQUINAS INFECTADAS → RELIGAR SERVIDOR DHCP → RECUPERAR ARQUIVOS DANIFICADOS PELO MALWARE → FIM

FALHAS DE HARDWARE

FALHA NOS DESKTOPS

PREPARAR EQUIPAMENTO DE RESERVA → SUBSTITUIR EQUIPAMENTO COM DEFEITO → RECUPERAR DADOS LOCAIS NO HD DO EQUIPAMENTO → CONFIGURAR NOVO EQUIPAMENTO PARA INGRESSO NO DOMINIO LOCAL → PROVIDENCIAR CONSERTO DO EQUIPAMENTO COM DEFEITO → FIM

FALHA EM SWITCHS

AVALIAR O TIPO DE DANO → SUBSTITUIR EQUIPAMENTO POR RESERVA → PROVIDENCIAR CONSERTO OU SUBTITUIÇÃO DEFINITIVA DO SWITCH → FIM

FALHA EM SERVIDORES

AVALIAR O TIPO DE DANO → REALIZAR MANUTENÇÃO NO SERVIDOR QUE APRESENTAR FALHA → VERIFICAR SE EXISTE ALGUM BACKUP DE MÁQUINA VIRTUALIZADA E RESTAURA-LO. → CASO CONSTATADO DANO IRREPAREAVEL PROVIDENCIAR NOVO SERVIDOR OU PEÇA → FIM

FALHA NO SISTEMA DE CONTABILIDADE

ACIONAR O SUPORTE DO SISTEMA SONNER → CASO HAJA PROBLEMAS NA INTERNET, VERIFICAR TIPO DE FALHA. → EM CASO DE FALHA NO HARDWARE, VERIFICAR TIPO DE FALHA, SUBSTITUIR EAUIPAMENTOS → FIM

CÓPIA DE SEGURANÇA

1.Verificar se Houve Backup do dia anterior → Houve erro?

- Não → Copiar backup para HD externo e remove-lo para outro local fisico seguro
- Sim → Analisar log de erro e corrigir → Copiar backup para HD externo e remove-lo para outro local fisico seguro

Copiar backup para HD externo e remove-lo para outro local fisico seguro → 19:00 Horas Inicializa Execução de Backup no servidor de **Backup:**\\Backup\BACKUP USUARIOS\PASTA CENTRAL → FIM