MANUAL DE CONTINGENCIAMENTO DE T.I.

Procedimentos a serem adotados em caso de incidentes na área de informática e Tecnologia da Informação

Resumo

O Plano de Contingência desempenha um papel significativo na continuidade das atividades críticas da organização, orientando na preparação para eventos imprevisíveis, e buscando minimizar seus impactos.

IlhabelaPrev

Controle Interno

Sumário

1. OBJETIVOS

O Manual de Procedimentos de T.I. do Instituto de Previdência dos Servidores Públicos do Município de Ilhabela - IlhabelaPrev tem o propósito de padronizar a realização das atividades envolvidas na gestão de T.I, demonstrando de forma simplificada os passos a serem seguidos.

O Manual contribui de forma significativa na redução de riscos, principalmente operacionais, traduzindo-se em um instrumento de orientação e controle para as atividades de T.I.

A elaboração e a implementação deste instrumento convergem com as diretrizes propostas pelo Manual do Pró-Gestão dos Regimes Próprios de Previdência Social, instituído pela Portaria MPS nº 185/2015, voltadas as Melhores Práticas em Procedimentos de T.I. Dentro deste contexto, essa ferramenta é capaz de potencializar o compromisso da gestão com a transparência. Os procedimentos deste manual são aplicáveis na gestão dos projetos e procedimentos de T.I. do IlhabelaPrev, observando as legislações específicas dos órgãos reguladores. Ele deve ser aperfeiçoado permitindo a realização das atividades de forma mais eficiente.

1.1 Aplicação e Procedimento de contingência geral de TI no IlhabelaPrev

Este documento se aplica a todos os serviços e sistemas de Tecnologia da Informação que são providos no IlhabelaPrev.

Os servidores do IlhabelaPrev devem tentar mitigar os impactos que porventura venham a ocorrer decorrentes de emergências ou emergências que afetem os sistemas, equipamentos ou infraestrutura de TI. Todos os servidores do IlhabelaPrev são responsáveis por informar o especialista em TI contratado caso detectem algum tipo de emergência ou hipótese acidental que ocorram em alguma das áreas sensíveis do IlhabelaPrev.

2. DEFINIÇÕES

ADMINISTRADOR DO PLANO DE CONTINGÊNCIA:	Responsável pela manutenção e atualização dos dados e procedimentos necessários à plena operacionalidade do Plano de Contingência;
ÁREA VULNERÁVEL:	Área atingida pela extensão dos efeitos provocados por um evento de falha, como exemplo a gestão de benefícios do IlhabelaPrev.
ÁREAS SENSÍVEIS:	Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências da emergência. Dentre elas, encontra-se todo corpo administrativo do IlhabelaPrev, DataCenter e demais locais que possuam equipamentos de informática.
ATIVIDADE:	processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;
ATIVIDADES CRÍTICAS:	atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;
BACKUP:	Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento
CENÁRIOS:	Possíveis Incidentes que possam ocorrer, detalhando as estratégias de recuperação, buscando ser o mais breve possível nessas recuperações minimizando os impactos na continuidade das atividades.
CONTINGÊNCIA:	Situação de risco com potencial de ocorrer, inerente as atividades, serviços e equipamentos, e que ocorrendo se transformará em uma emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer.

DESASTRE:	evento repentino que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período recuperação superior aos estimados em casos de incidentes requer recursos para aquisições de equipamentos e contratação de serviços.
ESPECIALISTA EM TECNOLOGIA DA INFORMAÇÃO	O Especialista em Tecnologia da Informação do IlhabelaPrev é o contratado responsável por operacionalizar e garantir o pleno funcionamento dos processos inerentes à Sistemas de informação, Backup, e Planos contingenciais.
ESTRATÉGIA DE CONTINUIDADE:	abordagem de uma organização que garanta a sua recuperação e continuidade ao se defrontar com um desastre, ou outro incidente maior ou interrupção de negócios;
INCIDENTE:	fato inesperado evento que tenha causado algum dano no equipamento interrompendo a execução de alguma atividade crítica por um período. Sendo esses incidentes: X Falha de hardware (Placas, processadores, Memórias e Discos Rígidos, Falha Cooler podem causar superaquecimento); X Falhas de Softwares e arquivos (Atualizações que podem causar incompatibilidade, Virus, arquivos corrompidos; X Bugs no sistema operacional.
SERVIDOR:	Um computador ou programa que fornece um tipo específico de serviço ao programa cliente executando em outros computadores;
TI:	Tecnologia da Informação;
TITULAR:	pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

3. NÍVEIS DE INCIDENTES

Nível I – Hipótese acidental que pode ser controlada pela equipe de TI e que não afeta o andamento do trabalho do servidor. Por exemplo: Problemas com equipamentos periféricos de computadores.

Nível II – Hipótese acidental que impede a utilização do equipamento ou sistema e acaba impedindo a continuação do trabalho pelo servidor. Por exemplo: Problema com o funcionamento do computador (não liga, travado etc.) ou ainda sistemas offline impedindo o uso dele.

Nível III – Hipótese acidental que impede o uso de sistemas ou equipamentos de todo o IlhabelaPrev, impedindo assim o desenvolvimento do trabalho de todos os servidores. Por exemplo: Falha na conexão com a internet ou queda de energia elétrica ou ainda problema técnico em algum servidor de rede que controla a conexão interna do IlhabelaPrev.

4. PRINCIPAIS RISCOS

O quadro abaixo define os principais riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência

Riscos	***Parâmetros***
Interrupção de energia elétrica	Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 60 (sessenta) minutos. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuito, incêndio e infiltrações.
Indisponibilidade de rede	Rompimento de cabos decorrente de execuções de obras internas, desastres ou acidentes.
Falha humana	Acidente ao manusear equipamentos
Falha de hardware	Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório
Ataque externo	Ataque virtual que comprometa o desempenho, acesso aos dados ou configuração dos serviços essenciais

4.1. Interrupção de energia elétrica:

Os moradores de Ilhabela reclamam constantemente da queda e da falta de energia, principalmente, quando chove e venta na ilha.

Em caso de queda no abastecimento de energia elétrica, a concessionária de energia deve ser avisada por um dos seguintes canais:

Canais de atendimento ao cliente:

Site: www.elektro.com.br

App: Elektro (navegação gratuita, disponível para Android e iOS)

WhatsApp: (19) 2122-1696

SMS: 28116

Call Center: 0800 701 01 02

4.2. Problemas de conexão:

4.2.1 Rede Interna

O Setor de TI identificará por meio de um sistema de monitoramento, que emitirá um alerta com a descrição do incidente, os dispositivos envolvidos e em qual departamento do IlhabelaPrev está ocorrendo o problema; identificar e corrigir a causa do problema;

Caso o problema de conexão seja em todo o IlhabelaPrev, verifica se os servidores de endereços DHCP (protocolo de configuração dinâmica de host) e de autenticação estão funcionando adequadamente. Informar a previsão do conserto ou solução aos demais servidores.

4.2.2 Problema de Conexão com a Internet

Realizar testes de comunicação com:

• Servidor externo via IP (ping 8.8.8.8) – em caso de sucesso, indica que deve ser um problema na resolução

do DNS.

• Firewall do gateway lhabelaPrev (ping 10.0.0.1) – em caso de sucesso, indica que deve ser algum problema com os links de internet.

Identificar a causa do problema: Detectado problema externo de internet, abrir um chamado de suporte com nossa prestadora de serviço (Atual Giga+).

Informar a previsão do conserto ou solução aos demais servidores.

4.2.3 Problemas Físicos com Cabeamento da Rede Interna

Detectar a causa do problema por meio de testes no cabeamento; detectado problema de cabeamento de rede, refazer a conexões;

Verificar as demais ligações caso seja em um rack com switch e testar;

Caso haja necessidade, agendar ou efetuar a troca dos cabos que estão apresentando falhas;

Detectado problema de cabeamento de fibra, informar a Giga+.

4.2.4 Ataques Cibernéticos

Caso seja detectado um ransonware em atividade (ou grande possibilidade de):

- Comunicar todos os servidores (funcionários) no local

- Desligar todos os computadores, incluindo os servidores (desligamento bruto, sem finalização do SO)

- Através de boot com SO 'externo', identificar quais máquinas estão infectadas. Providenciar limpeza das máquinas (se possível, removendo o malware, ou caso não seja possível, tentar restaurar backup da máquina se for o caso, e como última alternativa refazer uma instalação limpa no computador)

- Verificar qual último backup íntegro

- Restaurar arquivos do backup

Caso seja detectado outro tipo de malware:

- Desconectar computadores dos servidores (funcionários) da rede fisicamente (desligar os switches do IlhabelaPrev)

- Desligar o servidor (backup local no IlhabelaPrev – local físico = sede do IlhabelaPrev)

- Verificar integridade dos servidores

- Identificar todas as máquinas infectadas e iniciar processo de remoção do malware

- Com servidores limpos, ir reconectar apenas as máquinas 'limpas' à rede, para retomada do serviço

- Após todos os computadores limpos, religar equipamento do servidor

- Recuperar arquivos danificados pelo malware

4.2.5 Ataques Internos

- Desligar equipamentos com backups (para evitar perda dos backups)

- Identificar origem do ataque

- Desativar acessos do atacante

- Checar todas as sessões ativas do atacante e finalizá-las

- Após certeza de bloqueio dos acessos do atacante, checando com funcionários possibilidade de conhecimento de senha de outros usuários, religar equipamentos de backup

- Fazer levantamento dos dados danificados e restaurar dos backups

5. POLÍTICA E PROCEDIMENTO PARA BACKUP

5.1. Backup

Os servidores foram configurados para que diariamente, entre meia-noite e 06:00 horas, sejam realizadas as atividades de Backup de arquivos localizados no Google Drive para um Hard Drive interno.

5.2. Servidores do IlhabelaPrev: Restauração E Teste

A restauração de dados deve ser solicitada ao departamento de TI e será realizada de acordo com os procedimentos específicos dele. A verificação e o teste de restauração, serão realizados sempre que possível por meio de um software de backup, configurado para verificar automaticamente as condições do backup.

5.3. Ordem para o Desligamento dos Servidores

1. Acessar o ambiente virtual e desligar primeiramente os servidores virtuais de serviços/web;
2. desligar os demais dispositivos: servidor, Central Wi-Fi, PABX e Firewall.

5.4. Ordem para Religar os Servidores

1. Ligar os equipamentos: servidor, Central Wi-FI, PABX e Firewall; ligar os servidores físicos; verificar se as Máquinas ligaram;
2. caso não tenham sido ligadas automaticamente, verificar a causa e ligar manualmente;
3. realizar testes de acesso à internet, autenticação e demais sistemas web do IlhabelaPrev.

6. COMUNICAÇÃO

Para qualquer outro tipo de problema que envolva a TI, como impressoras, problemas de acesso que envolvam login e senha etc.

Os passos a serem seguidos são:

Informar o problema ao Profissional de TI;

Após o atendimento, o solicitante é informado da conclusão/resolução do problema;

6.1. Quem Deve Comunicar

Qualquer servidor que detecte qualquer tipo de problema ou anomalia, referente aos sistemas, equipamentos e/ou infraestrutura de TI.

6.2. A Quem Comunicar

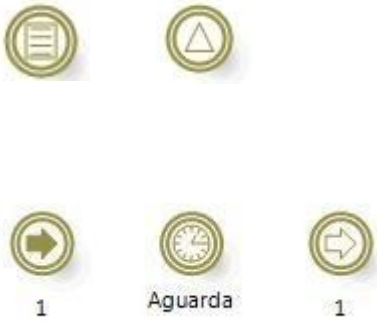
A comunicação deve ser feita para o profissional especialista em TI contratado, e, em caso muito específico conforme risco, informar a presidência.

6.3. Como Comunicar

Através do WhatsApp (12) 98254-8095, ou e-mail para o endereço lauro@lauroinformatica.com.br.

7. NOTAÇÃO PARA MODELAGEM DE PROCESSOS DE NEGÓCIOS

Os fluxogramas utilizados neste manual foram elaborados na versão gratuita do software Bizagi (disponível em https://www.bizagi.com/pt), e utilizam a seguinte notação:

DEFINIÇÃO	REPRESENTAÇÃO GRÁFICA
Piscina é um espaço que contém os passos do processo. Qualquer diagrama tem pelo menos uma piscina. O nome dado à piscina é o nome do processo.	
A raia é representada por um retângulo nomeado e é utilizada para organizar e delimitar as diferentes atividades de um mesmo setor.	
O subprocesso é representado por um retângulo, que simboliza uma etapa de um processo formado pela realização sequencial de um determinado conjunto de atividades afins.	
A atividade é representada por um retângulo arredondado e simboliza uma determinada quantidade de tarefas que devem ser efetuadas dentro de um processo.	
O evento de início é representado por um círculo e simboliza o começo da execução do processo. O evento de fim é representado por um círculo com borda em negrito e simboliza o final do processo.	
Os eventos intermediários são representados por círculos que simbolizam a interligação de atividades na mesma página do fluxo. Estes eventos sinalizam tanto saídas como entradas, no caso de saídas as setas são preenchidas, enquanto nas entradas as setas são vazias. Caso haja mais de uma interligação dentro do fluxo os círculos possuirão cores diferentes, de forma a facilitar a visualização. Os eventos intermediários podem também sinalizar uma ação específica, como por exemplo: Evento intermediário com especificação de tempo: indica um tempo de espera dentro do processo, sendo demonstrada por um relógio dentro do círculo; Evento intermediário condicional: é usado quando a sequência do fluxo depende de uma condição	

DEFINIÇÃO	REPRESENTAÇÃO GRÁFICA
de negócio específica; Evento intermediário dependente de sinal: é usado para representar o envio ou o recebimento de sinais, sendo representado por um triângulo dentro do círculo.	
Os gateways podem representar a escolha entre duas ou mais atividades adjacentes ou as possíveis rotas condicionais geradas por uma decisão. Os gateways podem representar também atividades desempenhadas de forma paralela. A condicional é representada por um losango, que pode ser preenchido por um ×, enquanto o paralelismo é representado por um losango preenchido por uma cruz. Um gateway também permite que caminhos diferentes se transformem em apenas um caminho resultante. Outro exemplo é o gateway exclusivo baseado em eventos, que divide rotas que são tomadas paralelamente, mas após a ocorrência de uma das atividades esperadas (uma das rotas), apenas um caminho é tomado; o(s) outro(s) se torna(m) inativo(s).	
A linha de fluxo é representada por uma linha com uma seta e é utilizada para demonstrar a ordem sequencial na qual cada atividade é desempenhada.	
Uma associação é usada para associar informações e Artefatos com Objetos de fluxo. É representada por uma linha descontínua.	

9. FLUXOGRAMA DOS PROCEDIMENTOS DE CONTINGENCIA DE T.I.