PORTARIA TRT/GP/DG Nº 180/2024

Define a Política de Gestão de TIC para a Continuidade de Negócios do Tribunal Regional do Trabalho da 24ª Região – PGTICN.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO, no uso de suas atribuições regimentais,

CONSIDERANDO as necessidades de recuperação das atividades de tecnologia da informação e comunicações após uma interrupção;

CONSIDERANDO a Resolução Administrativa Nº 32/2024, que define a Política de Segurança da Informação e atribui à Presidência do Tribunal a responsabilidade pela publicação de atos complementares;

CONSIDERANDO a aprovação pelo Comitê de Segurança da Informação e Proteção de Dados, em reunião ordinária de 18 de janeiro de 2024, da proposta de minuta para o presente normativo,

R E S O L V E:

DEFINIR a Política de Gestão de TIC para a Continuidade de Negócios no âmbito do Tribunal Regional do Trabalho da 24ª Região – TRT da 24ª Região, nos termos desta Portaria.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

CAPÍTULO I
DAS DEFINIÇÕES

Art. 1º Para fins desta Portaria, considera-se:

I - **Ativos de TIC**: qualquer mecanismo ou dispositivo de *software* ou *hardware* que compõem a infraestrutura tecnológica do TRT da 24ª Região;

II - **Ativos críticos do negócio**: ativos de TIC que suportam a operação dos processos críticos do negócio;

III - **Processos críticos do negócio**: o conjunto de atividades por intermédio das quais a instituição produz valor para os seus clientes;

IV - **Infraestrutura básica de segurança**: conjunto de ativos críticos do negócio necessários para suportar os processos críticos do negócio;

V - **Continuidade de TI**: capacidade estratégica e tática da instituição planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de TIC dos processos críticos, de forma a manter suas operações em um nível aceitável, previamente definido;

VI - **Estratégia de Gestão de TIC para a Continuidade de Negócios**: abordagem da instituição que garante a recuperação dos ativos de TIC e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;

VII - **Plano de Continuidade de TI**: conjunto de planos de ações destinadas a restabelecer os processos de TI críticos para o negócio, dentro do prazo máximo de interrupção previsto na Estratégia de Gestão de TIC para a Continuidade de Negócios do TRT da 24ª Região;

VIII - **Manual de Execução do Plano de Continuidade de TI**: documento técnico descritivo das atividades relativas à execução dos Planos de Teste, *Backup* e Comunicação;

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

IX - **Nuvem:** Infraestrutura de tecnologia para armazenamento de dados, serviços, soluções e sistemas, em ambiente externo ao *data center* do TRT da 24ª Região;

X - **On-premisse:** Infraestrutura de tecnologia para armazenamento de dados, serviços, soluções e sistemas, no ambiente do data center do TRT da 24ª Região.

CAPÍTULO II
PRINCÍPIOS E DIRETRIZES GERAIS

Art. 2º A Política de Gestão de TIC para a Continuidade de Negócios do Tribunal Regional do Trabalho da 24ª Região obedecerá aos seguintes princípios:

I - garantir a continuidade das operações de TI críticas para a organização, mesmo após um desastre;

II - manter a disponibilidade de informações em um nível aceitável para a organização, mesmo após um desastre;

III - promover a gestão de continuidade por meio do uso das melhores informações disponíveis, linguagem comum e da adoção de boas práticas de governança corporativa;

IV - estabelecer o Processo "Gerenciar Continuidade de TI" como o processo institucional contínuo e interativo, formulado para gerenciar a continuidade dos ativos de TIC para garantir a continuidade de negócios do TRT da 24ª Região.

Art. 3º São elementos estruturais da Política de Gestão de TIC para a Continuidade de Negócios:

I - o Comitê de Segurança da Informação e Proteção de Dados (CSEGINF);

II - a Estratégia de Gestão de TIC para a Continuidade de Negócios;

III - o Plano de Continuidade de TI (PContTI); e

IV - o Processo "Gerenciar Continuidade de TIC".

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

CAPÍTULO III

DO PROCESSO DE TRABALHO

Art. 4° As atividades executadas no âmbito da Política de Gestão de TIC para a Continuidade de Negócios deverão observar os procedimentos descritos no processo de trabalho "**Gerenciar Continuidade de TIC**", disponível no *site* do Portal de Governança de TIC do TRT da 24ª Região, item "Políticas e Processos de Trabalho".

CAPÍTULO IV

DOS RESPONSÁVEIS E DAS RESPONSABILIDADES

Art. 5° A responsabilidade sobre a execução das atividades previstas no processo de trabalho "**Gerenciar Continuidade de TIC**" caberá aos seguintes responsáveis:

I - ao Magistrado designado no âmbito da Política de Segurança da Informação caberá a responsabilidade pelas atividades atribuídas ao papel de "**Comitê de Segurança da Informação**";

II - ao Secretário de Tecnologia da Informação e Comunicações caberá a responsabilidade pelas atividades atribuídas ao papel de "**Dono do Processo**";

III - ao Chefe da Divisão de Proteção de Dados e Segurança da Informação caberá a responsabilidade pelas atividades atribuídas aos papéis de "**Gerente do Processo**" e de "**Divisão de Proteção de Dados e Segurança da Informação**";

IV - aos servidores integrantes da Divisão de Infraestrutura de TIC caberá a responsabilidade pelas atividades atribuídas ao papel de "**Divisão de Infraestrutura de TIC**";

V - aos fornecedores de soluções de TIC e empresas contratadas para suporte de soluções e aplicações em nuvem caberá a responsabilidade por atividades do processo externo denominado "equipe técnica contratada";

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

VI – ao Desembargador Presidente do TRT da 24ª Região caberá a responsabilidade pelas atividades atribuídas ao papel de "**Grupo de Gestão de Crises Cibernéticas**".

Parágrafo Único. a designação dos servidores responsáveis pelas atividades do papel "**Divisão de Infraestrutura de TIC**" será feita por Ordem de Serviço interna, sendo registradas na ferramenta ITSM disponível pela Secretaria de Tecnologia da Informação e Comunicações (SETIC), ou por integrantes da Equipe de Tratamento e Resposta a Incidente de Segurança Cibernética – ETIR, definida na Política de Gestão de Incidentes de Segurança da Informação.

CAPÍTULO V
DO ÂMBITO E DA APLICAÇÃO

Art. 6º A Política de Gestão de TIC para a Continuidade de Negócios aplica-se à Infraestrutura Básica de Segurança (Anexos I e II) e aos processos e ativos críticos de negócio definidos no âmbito da Política de Segurança da Informação.

Parágrafo Único. As plataformas de infraestrutura em nuvem contratadas para armazenamento de ativos críticos de negócio integram a infraestrutura básica para os fins aos quais se destinam esta Portaria.

CAPÍTULO VI
DA ESTRATÉGIA DE GESTÃO DE TIC PARA A CONTINUIDADE DE NEGÓCIOS

Art. 7º A Estratégia de Gestão de TIC para a Continuidade de Negócios consiste na execução de atividades que garantam um adequado gerenciamento de crise provocada por um incidente grave de segurança da informação.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

Parágrafo Único. Considera-se iniciada uma crise cibernética quando estabelecida pelo menos uma das seguintes características:

I – quando verificado grave dano material ou de imagem;

II – a eventual persistência das ações de resposta por longo período, mensurado pelos limites de tolerância definidos neste normativo;

III - impactar ou impedir a execução da atividade finalística do Tribunal; ou

IV - atrair grande atenção da mídia e da população em geral.

Art. 8° A Estratégia de Gestão de TIC para a Continuidade de Negócios utilizará a Infraestrutura Básica de Segurança para garantir a redundância dos serviços e informações que suportam os processos e ativos críticos do negócio, observando-se os requisitos:

I - os ativos de TI do *site backup* deverão ser dimensionados em capacidade de armazenamento e desempenho de processamento, de modo a garantir 100% da replicação dos dados dos processos de negócio críticos e 50% da capacidade de desempenho dos ativos de TI do *site* principal;

II - os ativos de TI de armazenamento do *site backup* deverão ser mantidos em estado constantemente sincronizado aos seus ativos correspondentes no *site* principal, de forma a evitar a necessidade de recuperação de *backup* de dados de fitas de armazenamento;

III - os ativos de TI relativos ao serviço de comunicação de rede (interno e externo) do *site backup* deverão ser mantidos ativados e configurados de forma a minimizar o tempo de restabelecimento dos processos críticos; e

IV - o *site backup* deverá assumir o papel de *site* principal sempre que a interrupção do *site* principal

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

ultrapassar o limite previsto para a interrupção máxima dos processos críticos do negócio.

Art. 9º Os limites de tolerância definidos em função do tipo do serviço prestado pela instituição, do impacto nos negócios e da capacidade de investimento na arquitetura de segurança, devem ser medidos a partir da indisponibilidade do *site* principal ou de algum de seus componentes e observar os seguintes parâmetros:

I - tolerância máxima à interrupção de processos de negócio:

a. sistemas judiciais: 48 horas;

b. sistemas administrativos: 48 horas.

II - tolerância máxima à perda de dados dos processos:

a. sistemas judiciais: últimos 15 minutos;

b. sistemas administrativos: últimos 15 minutos.

III – tolerância máxima à perda de desempenho:

a. sistemas judiciais: 50% do normal;

b. sistemas administrativos: 50% do normal.

Parágrafo único. O parâmetro **"tolerância máxima"** representa o tempo, perda de dados ou de desempenho máximos que a instituição pode suportar, antes da ativação do *site backup*.

Art. 10. Os SLAs de disponibilidade devem ser aplicados aos seguintes processos críticos do negócio:

I - sistemas judiciais (plataforma ORACLE): 99% da disponibilidade esperada; e

II - sistemas judiciais (plataforma PostgreSQL): 99% da disponibilidade esperada.

Art. 11. A recuperação e/ou restauração dos processos críticos do negócio, em função da infraestrutura básica de segurança, deverá considerar as seguintes possibilidades, observando-se os limites de tolerância estabelecidos:

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

I - recuperação e/ou restauração a partir de processos e serviços redundantes, disponíveis em serviços de backup em nuvem, caso o armazenamento esteja nesse ambiente;

II - recuperação e/ou restauração a partir de processos e serviços redundantes, disponíveis no *site backup*; e

III - recuperação e/ou restauração a partir de dados disponíveis em mídias de armazenamento.

§ 1º A recuperação a partir de serviço de backup em nuvem e do *site backup* deverá ser utilizada preferencialmente para restaurar as condições normais imediatamente anteriores à ocorrência do evento que causou a interrupção das operações.

§ 2º A recuperação de dados disponíveis a partir de fitas de armazenamento deverá ser utilizada preferencialmente para recuperar dados de momentos específicos do tempo ou nos casos em que as informações disponíveis no *site backup* não forem suficientes.

CAPÍTULO VII
DO PLANO DE CONTINUIDADE DE TI

Art. 12. O Plano de Continuidade de TI terá como escopo garantir a capacidade de respostas tempestivas à interrupção dos processos críticos do negócio atendidos pela Estratégia de Gestão de TIC para a Continuidade de Negócios do TRT da 24ª Região.

Parágrafo único. O tratamento dos riscos, no escopo da Estratégia de Gestão de TIC para a Continuidade do Negócio, será realizado pela análise de riscos definida na Política de Gestão de Riscos de TI.

Art. 13. O Plano de *Backup*, descrito no Anexo III, define o conjunto de procedimentos relacionados à produção de cópias de segurança e a eventual restauração dos dados armazenados.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

Art. 14. O Plano de Contingência, descrito no Anexo IV, define um conjunto de ações corretivas para tornar possível a continuidade das operações das áreas de negócio após a ocorrência de um evento que impossibilite a utilização parcial ou total do ambiente corporativo.

Art. 15. O Plano de Testes, descrito no Anexo V, define o conjunto de procedimentos de verificação e validação das ações previstas nos **Planos de Contingência** e de ***Backup* e Retenção de Dados.**

Art. 16. Os detalhes técnicos relativos a execução dos planos serão descritos no **Manual de Execução do Plano de Continuidade de TI**, observando-se os seguintes critérios:

I - por questão de segurança, o documento deverá ser mantido sob sigilo e disponível apenas aos responsáveis pelas tarefas;

II - o documento deverá ser guardado em formato impresso ou gravado digitalmente em mídia de conexão tipo USB e armazenada no cofre de mídias da SETIC; e

III - o documento deverá ser atualizado no mínimo 1 (uma) vez por ano ou sempre que houver demanda para revisão.

CAPÍTULO VIII
DO PLANTÃO DE TIC

Art. 17. O plantão da área de tecnologia da informação terá como escopo fornecer o atendimento emergencial no que se refere à disponibilidade dos ativos críticos de TI.

§ 1° Serão considerados ativos críticos para atendimento emergencial, os serviços apontados no Anexo IV.

§ 2° O Plano de Contingência, definido no ANEXO IV, deverá ser aplicado, no que couber, em resposta às situações de emergência, inclusive na restauração de ativos de TIC necessários que integram a infraestrutura básica de segurança definida no ANEXO I.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

§ 3° A escala do plantão deverá oferecer cobertura total nos períodos de finais de semana, feriados, recessos e quaisquer outros fora do expediente normal.

§ 4° O plantonista será acionado por meio de contato telefônico em aparelho fornecido pelo Tribunal Regional do Trabalho da 24ª Região, devendo para isso manter o aparelho ligado, em condições de uso e dentro da área de cobertura de sinal durante o período do plantão.

§ 5° A escala do plantão será proposta pela Divisão de Infraestrutura de TI, em sistema de rodízio, de acordo com a conveniência da unidade, e publicada na *intranet* do Tribunal.

§ 6° É responsabilidade do plantonista a convocação de integrantes da ETIR ou de outros servidores da SETIC que possam ser necessários à solução do incidente, de acordo com o ativo crítico indisponível.

§ 7° As eventuais atuações do plantonista, ou quaisquer outros servidores da SETIC convocados, deverão ser informadas ao Secretário da SETIC que procederá o envio das justificativas para apreciação da Presidência e providências de compensação ou pagamento em pecúnia, conforme regras de normatização de plantão administrativo.

CAPÍTULO IX
DAS ATIVIDADES EXTRAORDINÁRIAS

Art. 18. A execução de atividades extraordinárias terá como objetivo garantir a máxima disponibilidade dos ativos de TIC estratégicos do ANEXO I.

§ 1° O Plano de Contingência, definido do ANEXO IV, deverá ser aplicado, no que couber, em respostas às situações de emergência.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

§ 2º A execução de atividades extraordinárias será informada em processo administrativo para o Secretário da SETIC, que fará as devidas justificativas e encaminhará à apreciação da Presidência.

§ 3º As atividades extraordinárias poderão ser executadas por qualquer servidor da SETIC, desde que observado o disposto no *caput* e nos parágrafos anteriores.

§ 4º Após a execução das atividades o Secretário da SETIC procederá à certificação para providências de compensação ou pagamento em pecúnia, conforme regras de normatização de atividades extraordinárias e plantão administrativo.

CAPÍTULO X

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 19. Ficam revogadas as disposições contrárias a este normativo, notadamente a Portaria TRT/GP/DG Nº 235/2022.

Art. 20. Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação e Proteção de Dados.

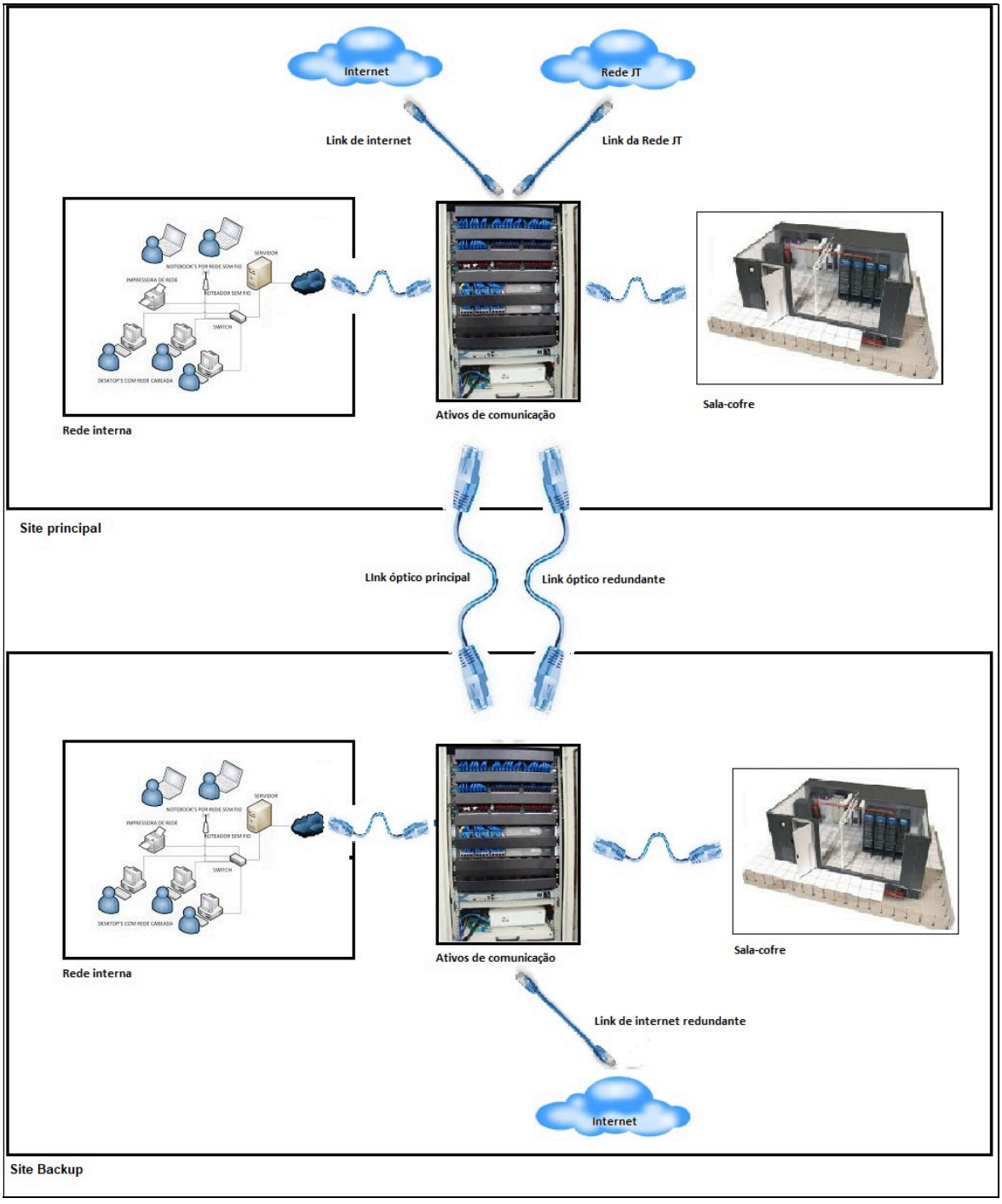
Art. 21. Esta Portaria entra em vigor na data de sua publicação.

João Marcelo Balsanelli
Desembargador Presidente

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

ANEXO I

Infraestrutura básica de segurança



Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

ANEXO II

Características da Infraestrutura Básica

de Segurança da Informação

1 DAS CARACTERÍSTICAS DE INFRAESTRUTURA

1.1 A infraestrutura de TI do TRT da 24ª Região conta com 2 (dois) *sites* geograficamente separados:

1.1.1 *Site* principal: localizado no prédio-sede do TRT da 24ª Região;

1.1.2 *Site backup*: localizado no prédio do Fórum Trabalhista de Campo Grande.

1.2 Recursos de TI instalados no *site* principal:

1.2.1 Bancos de dados *Oracle e PostgreSQL*;

1.2.2 *Storage* de produção;

1.2.3 *File System*;

1.2.4 Sala-cofre;

1.2.5 Cofres térmicos para armazenamento de mídias.

1.3 Recursos de TI instalados no *site* Backup:

1.3.1 Bancos de dados de redundância (*standby*).

1.4 A infraestrutura de TI do TRT da 24ª Região poderá contar com serviços contratados para o armazenamento em nuvem de:

1.4.1 Bancos de dados *Oracle e PostgreSQL*;

1.4.2 Estruturas de aplicações em nuvem;

1.4.3 Servidor de e-mail e de arquivos compartilhados;

1.4.4 Aplicação de Serviços ITIL;

1.4.5 Servidores antivírus;

1.4.6 Outras soluções de TIC viáveis para esse tipo de infraestrutura.

1.5 Os procedimentos, detalhes técnicos e temporalidade serão definidos de acordo com o tipo da aplicação e descritos no Manual de Execução do Plano de Continuidade de TI.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

ANEXO III

PLANO DE BACKUP

1 DAS CARACTERÍSTICAS DO BACKUP DE DADOS

1.1 Escopo restrito aos dados armazenados nos servidores e dispositivos que compõem as soluções de banco de dados.

1.2 Não fazem parte do escopo os serviços relacionados abaixo:

1.2.1 Bancos de dados de testes e homologação;

1.2.2 Pastas de dados temporários e arquivos temporários;

1.2.3 Qualquer tipo de conteúdo das estações de trabalho.

1.3 Os procedimentos, detalhes técnicos e temporalidade serão definidos de acordo com o tipo da aplicação e descritos no Manual de Execução do Plano de Continuidade de TI.

2 DOS RECURSOS E INFRAESTRUTURA

2.1 Os componentes da infraestrutura do TRT da 24ª Região para a realização do *backup* são:

2.1.1 *Storages* de dados;

2.1.2 *Tape Library*;

2.1.3 Fitas de *backup*;

2.1.4 Servidores de banco de dados *standby*;

2.1.5 Cofre de armazenamento de mídias;

2.1.6 *Software* Bacula.

3 DA ESTRATÉGIA E DOS PROCEDIMENTOS

3.1 Serão avaliados os custos de manutenção de *backup* extras das informações, dando-se preferência ao armazenamento em duplicidade dos dados críticos para o negócio como, por exemplo, os relativos aos processos judiciais e administrativos eletrônicos;

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

3.2 Infraestruturas armazenadas em nuvem terão o serviço de *backup* garantido pelas empresas contratadas, sendo opção do TRT da 24ª Região a realização de cópias locais, *on-premisse*, ou em outra solução de backup distinta do fornecedor da solução em nuvem, em especial para dados críticos, como os armazenados em sistemas gerenciadores de bancos de dados;

3.3 O *backup* do banco de dados de produção será realizado das seguintes formas:

3.3.1 *Backup on-line*: Os bancos de dados de produção serão configurados de forma a gerar arquivamento de *logs* (arquivos que armazenam as informações sobre todas as alterações ocorridas em tempo real) para executar *backup online* de forma transacional visando a manter um banco redundante e sincronizado com a produção, além da possibilidade de recuperação do estado do banco em qualquer momento do tempo (PITR – Point in Time Recovery). O objetivo será garantir a recuperação rápida do último *status* do banco de produção em caso de desastre, sem a necessidade de recuperação dos dados em fitas. A base será replicada para um *site backup* utilizando se um banco *standby* do tipo físico e aplicação constante dos *archive logs* gerados na produção;

3.3.1.1 Os bancos de dados em nuvem terão o armazenamento de backup no ambiente de nuvem, quando for o caso, e terá uma versão *standby* armazenada no ambiente do *data* center do TRT da 24ª Região;

3.3.2 *Backup* em fitas: será executado de acordo com agendamento diário, mensal, semanal e anual, feito em um único ponto, por meio de agente Bacula. O objetivo será manter o histórico do status do banco

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

ao longo do tempo, além de possibilitar auditorias caso necessário.

3.4 O *backup* dos arquivos compartilhados do serviço em nuvem seguirá as políticas do ambiente contrato, que possibilita recuperação imediata de arquivos excluídos com até 30 dias após a exclusão, além das garantias de backups em caso de incidente, fornecidas em contrato firmado com o TRT da 24ª Região;

3.5 O *backup* dos *e-mails* pessoais e institucionais será realizado pelo contratante.

4 DO ARMAZENAMENTO DAS FITAS DE *BACKUP*

4.1 Os procedimentos de operação e armazenamento das fitas será diário, de segunda a sexta-feira, e será executado por um dos servidores da Divisão de Infraestrutura de TI.

5 DA RECUPERAÇÃO DE DADOS

5.1 Os dados de banco de dados armazenados nas fitas serão recuperação mediante demanda ou de acordo com cronograma de testes de recuperação;

5.2 Os dados relativos aos demais serviços serão recuperados mediante demanda, por meio de solicitação ao secretário da SETIC;

5.3 A solicitação deverá ser feita por meio de chamado à Central de Serviços;

5.4 Para todos os casos, será sempre analisada, primeiramente, a possibilidade de obtenção da informação necessária pelo meio mais ágil a depender da criticidade da informação perdida e da urgência da sua prestação.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

ANEXO IV

PLANO DE CONTINGÊNCIA

TRATAMENTO DE INCIDENTES CRÍTICOS

2 DOS PROCEDIMENTOS EMERGENCIAIS MÍNIMOS

2.1 Em caso de emergência, a integridade das pessoas, ativos e informações, necessariamente nesta ordem, terá prioridade sobre a disponibilidade dos serviços, observando-se os seguintes procedimentos:

2.1.1 garantir a segurança de pessoas não envolvidas nas atividades de contingência, se for o caso;

2.1.2 desativar os ativos críticos para evitar danos;

2.1.3 acionar o plantonista da SETIC;

2.1.4 acionar os recursos humanos previsto no item 2.2;

2.1.5 acionar os recursos previstos no item 3.2;

2.1.6 assim que possível comunicar a indisponibilidade, conforme definido no Plano de Comunicação da Política de Gestão de Incidentes de Segurança da Informação.

2.2 Os serviços armazenados em nuvem deverão ser suspensos caso sua conexão com os ativos críticos interrompidos possam causar danos, ou vice-versa, podendo ser mantidos em execução em caso contrário, para acesso alternativo pela rede externa ao TRT da 24ª Região (internet).

2.3 Fazem parte das atividades de contingência os seguintes recursos:

2.3.1 Responsáveis pelos recursos da organização:

2.3.1.1 Diretor-Geral;

2.3.1.2 Gabinete de Manutenção e Projetos.

2.3.2 Responsáveis pelos recursos materiais ou ambientais necessários para suportar as atividades de contingência:

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

2.3.2.1 plantonista de TI, telefone (67) 99976-3459;

2.3.2.2 apoio especializado (bombeiros, brigadistas, unidade de segurança, etc), conforme o caso;

2.3.2.3 apoio médico (se for o caso).

3 DA INTERRUPÇÃO DOS SERVIÇOS

3.1 Os procedimentos deste documento serão aplicáveis somente aos serviços em ambiente de produção da infraestrutura básica (ANEXO I), para os seguintes cenários:

3.1.1 Interrupção programada: aquela previamente agendada e que será executada de forma planejada:

3.1.1.1 Será executada fora do horário de expediente, em janela de tempo compatível com a complexidade da demanda;

3.1.1.2 Deverá ser autorizada pelo secretário da SETIC;

3.1.1.3 Será comunicada aos clientes internos com antecedência mínima de 72 horas;

3.1.1.4 Será comunicada aos clientes externos (*pop* de advertência no *site*), com antecedência mínima de 72 horas;

3.1.1.5 Em casos de feriados, deverão ser observadas as coincidências entre as datas de dias não úteis da capital, interior e a rede bancária;

3.1.1.6 Manutenções emergenciais poderão ser feitas com intervalo menor, desde que com a adequada autorização do proprietário do serviço, do Secretário de TIC, ou de um integrante estratégico da administração do TRT da 24ª Região, a depender da amplitude de usuários impactados;

3.1.2 Interrupção não programada: aquela de causa não prevista e que será executada de forma emergencial:

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

3.1.2.1 os procedimentos deverão priorizar a garantia da integridade dos dados da instituição;

3.1.2.2 a comunicação aos clientes internos e externos será realizada de acordo com os recursos disponíveis em função da natureza da interrupção, conforme Plano de Comunicação da Política de Incidentes de Segurança da Informação;

3.1.2.3 a interrupção será realizada no menor prazo possível, mesmo em horário de expediente, em resposta a qualquer ocorrência ou evento que não possa ser adiado e de forma a garantir a integridade dos dados da instituição.

4 DO RESTABELECIMENTO DOS SERVIÇOS

4.1 Para fins de restabelecer os serviços necessários para a continuidade do negócio será considerado como serviço essencial, com prioridade sobre os demais, os bancos de dados de produção.

4.2 Depois de restabelecidos os bancos de dados, serão priorizados os seguintes sistemas e serviços, em sequência de prioridade:

4.2.1 serviços de autenticação;

4.2.2 serviços de *Internet* e Rede JT;

4.2.3 Processo Judicial Eletrônico (sistema PJe);

4.2.4 *Site* principal;

4.2.5 geração de guias (SISCONDJ e SIF);

4.2.6 sistema administrativo (sistema PROAD);

4.2.7 recursos humanos (sistema SIGEP – base de dados Oracle);

4.2.8 produção de atos e portarias (sistema Actu);

4.2.9 sistema de Folha de Pagamento;

4.2.10 gestão de patrimônio (sistema SCMP);

4.2.11 *Intranet*.

4.3 As aplicações armazenadas em nuvem que tiverem relação com os sistemas e serviços do item anterior, deverão

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

seguir a mesma sequência de restauração, caso haja a interrupção do seu todo ou parte, a depender de funcionamentos dependentes da rede do TRT da 24ª Região, como no caso de execução protegida de guias de pagamento e levantamento (SISCONDJ e SIF) que possuem proteção parcial para execução em rede interna do TRT da 24ª Região.

4.4 Os serviços de *e-mail* e compartilhamento de arquivos (armazenados em ambiente de nuvem) deverão ter seu funcionamento independente da rede de dados do TRT da 24ª Região, e, caso necessária a intervenção, preferencialmente restabelecidos logo após os demais serviços listados.

5 DO RESTABELECIMENTO *DOS SITES* PRINCIPAL E DE *BACKUP*

5.1 Fica estabelecido como *site* principal aquele localizado no prédio sede e como *site backup* aquele localizado no prédio do Fórum Trabalhista de Campo Grande.

5.2 Em caso de evento catastrófico com perda total do *site* principal:

5.2.1 o *site backup* deverá ser "promovido" a *site* principal;

5.2.2 Os serviços redundantes deverão ser "promovidos" a serviços de produção de forma a restabelecer a disponibilidade dos sistemas;

5.2.3 Os *links* de dados da rede JT e de *Internet* deverão ser movimentados para o novo *site* principal.

5.3 Em caso de perda somente dos equipamentos do *site* principal:

5.3.1 Os serviços redundantes deverão ser movimentados para o *site* principal de forma a aproveitar as características de infraestrutura e segurança do ambiente,

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

respeitados os períodos de indisponibilidade dos serviços;

5.3.2 Os serviços redundantes deverão ser "promovidos" a serviços de produção de forma a restabelecer a disponibilidade dos sistemas na ordem de prioridade estratégica descrita acima.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

ANEXO V

Plano de Testes

***Backup* VMs e E-mail (EMC -> Huawei -> EMC)**

1. DAS CARACTERÍSTICAS DOS TESTES

1.1. Os testes têm como objetivo o exercício constante dos procedimentos previstos nos **Planos de Contingência** e de ***Backup* e Retenção de Dados**;

1.2. Os procedimentos deverão testar a recuperação a partir de:

1.2.1. dispositivos de redundância *online*;

1.2.2. mídias de gravação.

1.3. Todos os testes serão realizados pela ETIR sendo documentados pela Divisão de Proteção de Dados e Segurança da Informação, devendo constar as seguintes informações:

1.3.1. data do teste;

1.3.2. Serviço testado (banco de dados, *file system* ou *e-mail*);

1.3.3. tipo e tamanho da amostra testada;

1.3.4. resultado obtido (sucesso total ou falha);

1.3.5. evidências da execução.

1.4. Os procedimentos, detalhes técnicos e temporalidade serão definidos de acordo com o tipo da aplicação e descritos no Manual de Execução do Plano de Continuidade de TI.

2. DOS RECURSOS E INFRAESTRUTURA

2.1. Os testes serão executados utilizando-se a seguinte infraestrutura:

2.1.1. armazenamento em nuvem;

2.1.2. *storage* de *backup*;

2.1.3. bancos de dados Dataguard e/ou Réplicas;

2.1.4. *Tape Library* de *backup*;

2.1.5. fitas de *backup* de dados;

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

2.1.6. cofres de segurança de mídias.

3. DOS TESTES DE RECUPERAÇÃO DE DADOS E ATIVAÇÃO

3.1. Os dados recuperados durante os testes deverão ser eliminados como forma de evitar múltiplas versões de arquivos e racionalizar a ocupação do espaço de armazenamento disponível.

3.2. Os dados recuperados deverão ser testados por meio do acesso realizado pelas aplicações clientes, em ambiente apartado da produção.

3.2.1. Para o serviço de banco de dados, considera-se ativada a restauração a partir do sucesso de acesso pelas aplicações clientes e pelo serviço de *website* do TRT da 24ª Região;

3.2.2. Para o serviço de compartilhamento de arquivos e de e-mail, considera-se ativada a restauração dos arquivos conforme serviço disponibilizado pela contratada a disponibilidade para os usuários a partir da conta dos mesmos.

4. NOTIFICAÇÃO DOS TESTES

4.1. O agendamento dos procedimentos de testes será através da ferramenta ITSM ~~ITIL~~.

4.2. Os testes deverão ser feitos no mínimo uma vez ao ano, com negociação de prazos de execução com o secretário de TIC e os integrantes da ETIR.

4.3. Ao final dos testes as evidências da execução deverão ser armazenadas em pasta compartilhada, ou anexadas nos chamados da ferramenta ITSM abertos.

5. PRODUÇÃO DE EVIDÊNCIAS

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).

5.1. Todos os testes deverão ser comprovados mediante apresentação de evidências devidamente documentadas e informadas à Divisão de Segurança da Informação e Proteção de Dados.

5.2. Para fins de comprovação da execução dos procedimentos serão aceitas evidências no formato de fotos, vídeos, documentos, *logs* de aplicação ou qualquer outro meio que permita a identificação e *time* stamp do procedimento.

Cópia digital inserida por JOÃO MARCELO BALSANELLI (Certificado A1) em 06/09/2024 16:53:10.
Documento disponível em www.trt24.jus.br (Identificador ID:2446318).