PORTARIA TRT/GP/DGCA Nº 176/2016

Define a Política de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região.

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

CONSIDERANDO a observância das recomendações do Tribunal de Contas da União - TCU (Acórdãos TCU - Plenário - n.º 1.603/2008, 2.471/2008 e 663/2009), no que diz respeito à implantação de modelos de governança de Tecnologia da Informação (TI) que incluam planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI;

CONSIDERANDO a observância e adoção das recomendações da norma ISO-IEC 27002;

R E S O L V E:

Revogar as portarias TRT/GP/DGCA nº 692/2011, 376/2013 e 109/2015, e definir a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 24ª Região, nos termos do presente ato.

CAPÍTULO I
DAS DIRETRIZES GERAIS

Art. 1º. A Política de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região obedecerá às seguintes diretrizes:

I. Estabelecer e promover ações para garantir a confidencialidade, integridade e

Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).

disponibilidade das informações da instituição armazenados em meio computacional;

II. Mitigar os riscos associados à dependência da organização em relação ao uso massivo da TI;

III. Definir as atribuições e responsabilidades relativas ao processo de trabalho "Gerenciar Segurança da Informação" para estabelecer e promover a aplicação da Política de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 2º. Para fins deste ato, considera-se:

I. **Ativos de TIC**: qualquer mecanismo ou dispositivo de software ou hardware que compõem a infraestrutura da rede de dados do TRT24;

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 através 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. **Segurança da Informação**: conjunto de medidas que tem como objetivo o estabelecimento dos controles necessários

Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).

à preservação da confidencialidade, integridade e disponibilidade das informações durante sua criação, uso ou armazenamento, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou intencionais;

VI. **Confidencialidade**: garantia de que a informação seja acessível apenas às pessoas autorizadas;

VII. **Integridade**: garantia de exatidão e completeza da informação e dos métodos de armazenamento e/ou processamento;

VIII. **Disponibilidade**: garantia de que as pessoas autorizadas tenham acesso às informações;

IX. **Usuário de TIC:** todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em qualquer unidade organizacional do TRT da 24ª Região.

CAPÍTULO III
DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art. 3º. O Comitê Técnico de Segurança da Informação será composto pelos seguintes membros:

I. Um magistrado pertencente ao Comitê de Governança de TIC, nomeado por meio de portaria da Presidência do Tribunal;

Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).

II. Diretor-Geral de Coordenação Administrativa;

III. Diretor da Secretaria de Coordenação Judiciária;

IV. Diretor da Coordenadoria de Tecnologia da Informação e Comunicações;

V. Chefe do Setor de Segurança da Informação.

§1º. A coordenação do cSEG-TRT24 caberá ao magistrado nomeado, conforme definido no inciso I do caput.

CAPÍTULO IV
DOS RESPONSÁVEIS E RESPONSABILIDADES

Art. 4º. Cabe ao Coordenador do Comitê Técnico de Segurança da Informação exercer os papéis e as responsabilidades definidas no processo de trabalho **Gerenciar Segurança da Informação**:

I. Papel do Dono do Processo

a. Assegurar o sucesso do desenho e garantir a execução do processo de trabalho;

b. Promover a integração com outros processos de trabalho;

c. Realizar avaliação de desempenho e resultados do processo;

d. Promover o treinamento dos executores do processo;

II. Papel do Comitê Técnico de Segurança da Informação

a. Aprovar a Política de Segurança da Informação;

b. Aprovar os relatórios de segurança.

Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).

Art. 5º. Cabe ao responsável pelo Setor de Segurança da Informação exercer os papéis e as responsabilidades definidas no processo de trabalho **Gerenciar Segurança da Informação**:

I. Papel de Gerente do Processo

a. Planejar e coordenar todas as atividades necessárias para executar, monitorar, relatar informações e produzir dados dos indicadores de desempenho do processo.

II. Papel do Setor de Segurança

a. Elaborar/revisar anualmente as normas da Política de Segurança da Informação;

b. Executar os planos táticos da PSI;

c. Registrar os controles do processo;

d. Elaborar relatórios de segurança.

CAPÍTULO V
DO ÂMBITO E DA APLICAÇÃO

Art. 6º. A Política de Segurança da Informação aplica-se a todos aqueles autorizados a fazer uso dos ativos de TIC administrados pela Coordenadoria de Tecnologia da Informação e Comunicações – CTIC, bem como, no que couber, ao relacionamento do TRT da 24ª Região com outros órgãos públicos ou entidades públicas ou privadas.

Art. 7º. A aplicação da Política de Segurança da Informação deverá observar no mínimo os seguintes processos e ativos críticos do negócio:

I. Processos críticos do negócio:

Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).

a. Sistemas judiciais: Processo Judicial Eletrônico (PJe), Judice I e II, eVoto, Cálculo, Protocolo, Audiências;
b. Sistemas administrativos: GestorePAE, GestoreWeb, SGRH, Folha de Pagamentos e SIGEO.

II. Ativos críticos do negócio:
a. Site principal;
b. Site backup;
c. Serviço de banco de dados de produção (Postgree e Oracle);
d. Serviço de File system (capital e interior);
e. Serviço de internet/intranet;
f. Serviço de email;
g. Conexão de fibra óptica principal;
h. Conexão de fibra óptica redundante;
i. Ativos de rede (switches).

Art. 8º. A Infraestrutura Básica de Segurança terá os níveis de tolerância e SLAs de disponibilidade definidos no âmbito da Política de Gestão da Continuidade de Negócios, e será composta pela arquitetura apresentada no ANEXO I.

CAPÍTULO VI
DOS INSTRUMENTOS NORMATIVOS

Art. 9º. As ações desenvolvidas no âmbito da Política de Segurança da Informação deverão observar os seguintes instrumentos normativos:

I. Política de Gestão de Riscos;
II. Política de Controle de Ativos;
III. Política de Controle de Acessos Físicos;

Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).

IV. Política de Controle de Acessos Lógicos;

V. Política de Controle de Incidentes de Segurança;

VI. Política de Gestão da Continuidade de Negócios.

CAPÍTULO VII
DOS PROCESSOS DE TRABALHO

Art. 10º. As atividades executadas no âmbito da Política de Segurança da Informação deverão observar os procedimentos descritos nos processos de trabalho:

I. Gerenciar Segurança da Informação

II. Gerenciar Riscos de TIC;

III. Gerenciar Controle de Ativos;

IV. Gerenciar Controle de Acessos Físicos;

V. Gerenciar Controle de Acessos Lógicos;

VI. Gerenciar Controle de Incidentes de Segurança;

VII. Gerenciar Gestão da Continuidade de Negócios.

CAPÍTULO VIII
DA COMUNICAÇÃO

Art. 11º. A comunicação a respeito da Política de Segurança da Informação será direcionada aos usuários de TIC do Tribunal Regional do Trabalho da 24ª Região, de acordo com a conveniência da instituição, através dos seguintes meios:

I. A comunicação entre os envolvidos nos processos de trabalho deverá utilizar o processo administrativo correspondente ao Processo Gerenciar Segurança da Informação;

Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).

II. A comunicação ao público interno deverá utilizar meios eletrônicos de envio, tais como email e malote digital.

Art. 12º. A comunicação a respeito da Política de Segurança da Informação será realizada sempre que ocorrer qualquer revisão da mesma ou de acordo com as atividades previstas no fluxo dos processos de trabalho.

Parágrafo único: eventos de quebra de segurança serão comunicados aos responsáveis pelas unidades envolvidas e ao Comitê de Segurança da Informação, se for o caso.

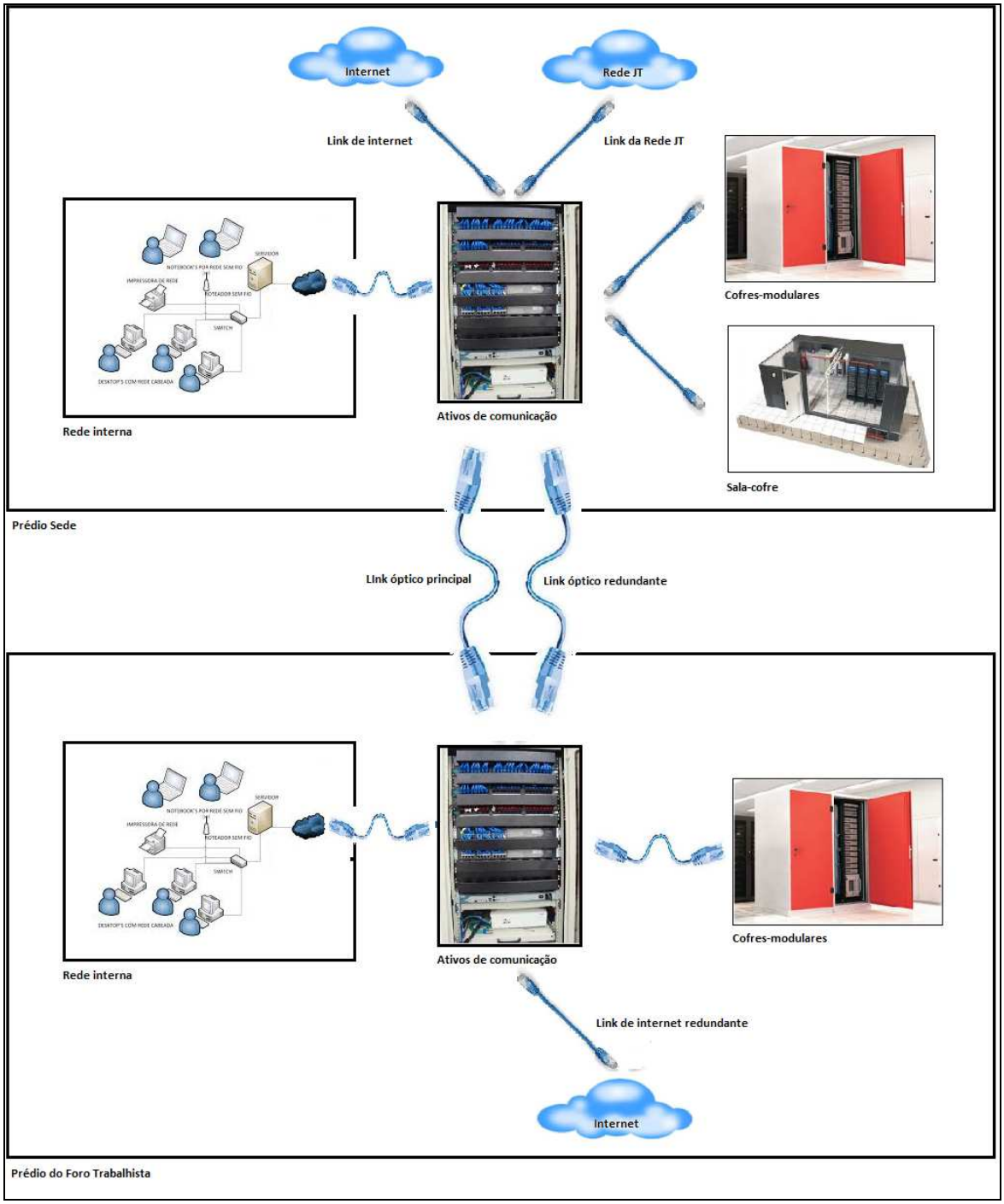
Art. 13º. Esta portaria entra em vigor na data de sua publicação.

Nery Sá e Silva de Azambuja
Desembargador Presidente

Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).

ANEXO I

Infraestrutura básica de segurança



Documento produzido e assinado eletronicamente (Certificado A1) por NERY SÁ E SILVA DE AZAMBUJA em 12/12/2016 12:18:17.
Documento disponível em www.trt24.jus.br (Identificador ID:1932334).