PODER JUDICIÁRIO FEDERAL
Tribunal Regional do Trabalho da 2ª Região

ATO GP nº 10/2015

Institui a Política de Controle de Acesso Físico ao Datacenter e às instalações de TI no âmbito do Tribunal Regional do Trabalho da 2ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir que os requisitos de segurança da informação sejam alcançados no controle de acesso físico às instalações de TI deste Tribunal,

RESOLVE:

Art. 1º. Instituir a Política de Controle de Acesso Físico às instalações de TI no âmbito do Tribunal Regional do Trabalho da 2ª Região.

Art. 2º. Para os efeitos deste Ato aplicam-se as seguintes definições:

I. Biometria: método de autenticação baseado em medidas biológicas, como, por exemplo, leitores de impressão digital e reconhecimento de íris;

II. Instalações de TI: salas onde se encontram alocados os recursos computacionais corresponsáveis pelo processamento de informações, incluindo infraestrutura de apoio, como equipamentos de redes, telecomunicações e UPS;

III. Estoques: salas onde ficam armazenados os equipamentos de TI novos ou destinados à manutenção;

IV. Armários: espaços destinados a abrigar infraestrutura de rede nos edifícios do Tribunal, ou para abrigar reservas técnicas – equipamentos que podem ser utilizados em substituição a equipamentos que estão com problemas.

V. Datacenters: instalações projetadas para abrigar e proteger os principais recursos computacionais responsáveis pelo armazenamento e processamento de informações, bem como sua infraestrutura de apoio (equipamentos de telecomunicação e de fornecimento de energia);

VI. Perímetros de segurança: áreas protegidas por barreiras tais como paredes, portões e/ou entradas com controle de acesso ou balcões de recepção com recepcionistas;

VII. PIN: acrônimo para *Personal Identification Number*. Número de identificação pessoal que permite a autenticação do usuário para a utilização de determinado recurso;

VIII. UPS: acrônimo para *Uninterruptible Power Supply*. Fonte de alimentação secundária que entra em ação quando há uma queda no fornecimento de energia da rede elétrica, garantindo assim, por um determinado período de tempo, a não interrupção do funcionamento dos recursos a ele interligados.

Dos Locais dos Datacenters e Instalações de TI

Art. 3º. Os locais dos Datacenters, Estoques e Instalações de TI deverão estar protegidos por perímetros de segurança, evitando ainda que suas entradas e acessos fiquem próximos a locais de circulação pública.

Art. 4º. As entradas e acessos aos Datacenters, Armários, Estoques e Instalações de TI deverão possuir a menor indicação possível da sua finalidade, isto é, sem letreiros ou indicações evidentes que identifiquem a presença das atividades de processamento ou armazenamento de informações.

Da Autenticação e Permissões de Acesso

Art. 5º. O acesso aos Datacenters, Armários, Estoques e Instalações de TI deve ser restrito apenas a pessoas autorizadas, devendo as mesmas portar algum tipo de identificação visível.

Art. 6º. A autenticação do acesso aos Datacenters e Estoques deve ser feita, sempre que possível, por meio de biometria e vinculada a sistema de controle de acesso.

§1º. Caso não seja adotada a biometria, a autenticação deve ser feita mediante cartão de acesso acrescido do PIN.

§2º. O acesso às Instalações de TI e aos Armários será concedido por pessoa responsável pela sala, que deve possuir as chaves de abertura respectivas.

Art. 7º. Terão permissão de acesso aos Datacenters, Armários, Estoques e Instalações de TI:

I. Servidores deste Tribunal cujo ingresso a esses locais seja estritamente necessário ao desenvolvimento das atividades atribuídas a seu cargo ou função;

II. Seguranças e bombeiros que deverão ser previamente cadastrados nos sistemas de acesso;

III. Empresas e prestadoras de serviços terceirizadas, contratadas por este Tribunal para o gerenciamento das operações de TI e;

IV. Visitantes devidamente acompanhados por um servidor autorizado deste Tribunal.

§ 1º. Deverá haver, durante as 24 horas do dia, pelo menos um segurança com acesso aos Datacenters.

§ 2º. Em nenhuma hipótese visitantes receberão credenciais de acesso aos Datacenters.

Art. 8º. Todos os funcionários de empresas e prestadoras de serviços terceirizadas, ao prestarem suporte ou atenderem ocorrência dentro do Datacenter, de Armários, de Estoques ou de Instalações de TI, deverão efetuar cadastro pessoal - informando além de seus dados pessoais, qual organização representam, qual o propósito de adentrar ao local e quais atividades serão desenvolvidas - e retirar um crachá de identificação na recepção do edifício.

Art. 9º. A concessão de permissões de acesso aos Datacenters será efetuada pela Seção de Segurança em Tecnologia da Informação, mediante solicitação formal feita pelo gestor da Coordenadoria em que o servidor estiver lotado.

§ 1º. Havendo mudança na situação funcional do servidor, na qual o acesso aos Datacenters não seja mais necessário, o gestor de sua Coordenadoria deve comunicar imediatamente o fato à Seção de Segurança em Tecnologia da Informação para que seja efetuada a revogação das permissões de acesso.

§ 2º. Havendo mudança na situação funcional de empregados terceirizados, na qual o acesso aos Datacenters não seja mais necessário, a área responsável deverá comunicar o fato à Seção de

Segurança em Tecnologia da Informação, no prazo máximo de 2 (dois) dias, para que seja efetuada a revogação das permissões de acesso.

Art. 10. A Seção de Segurança em Tecnologia da Informação deve, anualmente, efetuar revisão e atualização das permissões de acesso aos Datacenters.

Art. 11. A concessão de permissões de acesso aos Estoques será efetuada pela Coordenadoria de Atendimento, mediante solicitação formal feita pelo gestor da Coordenadoria em que o servidor estiver lotado.

§ 1º. Havendo mudança na situação funcional do servidor, na qual o acesso aos Estoques não seja mais necessário, o gestor de sua Coordenadoria deve comunicar imediatamente o fato à Coordenadoria de Atendimento para que seja efetuada a revogação das permissões de acesso.

§ 2º. Havendo mudança na situação funcional de empregados terceirizados, na qual o acesso aos Estoques não seja mais necessário, a área responsável deverá comunicar o fato à Coordenadoria de Atendimento, no prazo máximo de 2 (dois) dias, para que seja efetuada a revogação das permissões de acesso.

Art. 12. A Coordenadoria de Atendimento deve, anualmente, efetuar revisão e atualização das permissões de acesso aos Estoques.

Art. 13. Constatada a presença de qualquer pessoa que não esteja portando uma identificação visível nos Datacenters, Armários, Estoques ou Instalações de TI, a Secretaria de Segurança Institucional deverá ser imediatamente avisada/acionada.

Da monitoração, detecção e alarme

Art. 14. O sistema de controle de acesso físico aos Datacenters e Estoques deverá armazenar registros de auditoria que permitam recuperar, no mínimo, a identificação dos envolvidos, a data e hora dos eventos e as tentativas de acesso não autorizado.

Art. 15. Os Datacenters, Estoques e Instalações de TI deverão possuir câmeras de vigilância cobrindo todos os pontos de suas instalações, tendo suas imagens armazenadas em mídia, de forma que possam ser resgatadas em caso de alguma ocorrência ou auditoria.

Art. 16. Um sistema de monitoração e detecção de intrusos deve ser implementado e deve operar de forma que envie mensagens de alerta a uma estação de gerenciamento remota na ocorrência de eventos como abertura e fechamento de portas, falhas nos sistemas de trancas e quaisquer outros que coloquem em risco o controle de acesso aos Datacenters.

Considerações finais

Art. 17. Fica estabelecido o prazo de 180 dias para adequação da prática vigente a esta política, contados a partir da data de publicação deste Ato.

Art. 18. O descumprimento das normas referentes a esta política poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais.

Art. 19. As diretrizes e procedimentos adotados no âmbito deste Regional devem observar as disposições contidas neste Ato, a legislação vigente e, em especial, a seguinte referência normativa:

I. ABNT NBR ISO/IEC 27002:2005: norma que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta norma proveem diretrizes gerais sobre as metas geralmente aceitas para a gestão de segurança da informação.

Publique-se e cumpra-se.
São Paulo, 23 de março de 2015.

SILVIA REGINA PONDÉ GALVÃO DEVONALD
Desembargadora do Trabalho Presidente do Tribunal

PUBLICADO NO
DIÁRIO OFICIAL ELETRÔNICO DO TRT 2ª REGIÃO
EM 26 / 03 / 2015