Sumário

Histórico de Revisão			
Versão	**Data**	**Responsável**	**Aprovação**
00	08/12/2014	DGC	RD nº 05/324ª de 08/12/2014

Informações Adicionais

Este Instrumento Normativo revoga a CSIC 001 - Norma para Controle de Acesso Lógico aos Recursos Computacionais da EPE, aprovada pela RD 04/223ª de 16/09/2011, vigente até esta data.

1. Objetivo

Estabelecer as regras que norteiam as atividades de Controle de Acesso Lógico e Segurança Física na Empresa de Pesquisa Energética (EPE).

2. Campo de Aplicação

Aplica-se a todas as áreas da EPE.

3. Definições e Siglas

3.1. Definições

Acesso – Ato de ingressar, transitar, conhecer ou consultar a informação, seja local, ou remotamente, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

Área Segura – São salas trancadas ou um conjunto de salas dentro de um perímetro físico de segurança, que podem ser trancadas e que disponham de arquivos de aço trancáveis ou cofres. A localização de uma área segura deve levar em conta os riscos e vulnerabilidades e devem contemplar os regulamentos e normas relevantes de saúde e segurança e considerar eventuais ameaças à segurança causadas por instalações vizinhas, como infiltrações, vazamento de água proveniente de outra área etc.

Ativos de Informação – Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Bloqueio de Acesso – Processo que tem por finalidade suspender temporariamente o acesso.

Contas de Serviço – Contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, *script* etc.) sem qualquer intervenção humana no seu uso.

Credenciamento de Acesso – Processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia.

Credenciais ou Contas de Acesso – Identificações concedidas por autoridade competente após o processo de credenciamento de acesso, que permitam habilitar determinada pessoa, sistema ou

organização ao acesso. A credencial pode ser física como crachá, cartão, credencial biométrica ou lógica como identificação de usuário e senha.

Contêineres dos Ativos de Informação – O contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado.

Custodiante do ativo de informação **–** É o responsável pelos contêineres dos ativos de informação e pela aplicação dos níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação.

Equipamentos - Instrumentos necessários para determinada função.

Exclusão de Direito de Acesso – Processo que tem por finalidade suspender definitivamente o acesso.

Exclusão de Conta de Acesso – Processo que tem por finalidade o cancelamento do código de identificação e do perfil de acesso.

Gestão de Riscos de Segurança da Informação e Comunicações – Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Gestor do ativo de informação **–** indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

Identificação do Usuário ou Nome do Usuário – forma pela qual o usuário é conhecido no ambiente de informática da EPE. O usuário recebe as permissões de utilização dos recursos computacionais em função de sua Identificação, que deve ser validada com o uso de uma Senha.

Menu – Lista de opções ou entradas postas à disposição do usuário, que aparece no vídeo de um terminal de computador com as funções que este poderá realizar por meio de um programa ou de um *software*.

Necessidade de Conhecer – Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

Perfil de Acesso – Conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

Perímetro de Segurança – Áreas que podem ser compostas por diferentes dimensões, equipamentos e tipos de controle de acesso físico para as instalações ou áreas críticas. Podem ser delimitadas por paredes, portas de entrada controladas por cartão ou balcão de recepção com recepcionista, etc.

Quebra de Segurança – Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações.

Tratamento da Informação – Recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Usuário – Qualquer empregado ocupante de cargo efetivo, cargo em comissão, cedido, prestador de serviço terceirizado, estagiário ou qualquer outro indivíduo que tenha acesso, de forma autorizada, aos recursos computacionais da EPE.

3.2. Siglas

CFTV – Circuito Fechado de Televisão

CPD – Centro de Processamento de Dados

SIC – Segurança da Informação e Comunicações

4. Documentos de Referência

- GSI IN1 NC7/2014: Estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades de toda a Administração Pública Federal.
- ABNT NBR ISO/IEC 27002:2013: Fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.
- Política de Segurança da Informação e Comunicações: Estabelece orientações estratégicas sobre as práticas de Segurança da Informação e Comunicações adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.

5. Descrição

5.1. Controle de Acesso Lógico

Conjunto de procedimentos, recursos e meios utilizados pela Empresa com a finalidade de conceder ou bloquear o acesso aos ativos de informação a usuários autorizados ou não.

5.1.1. Papéis e Responsabilidades

Superintendência de Tecnologia da Informação - STI

- Definir, implementar e gerenciar um sistema de controle de acesso para todos os ativos de informação da EPE, não importando sua localização física.
- Prover o controle e a autenticação das conexões externas dos usuários e viabilizar a segurança da informação quando for necessária a utilização de computação móvel e demais recursos de trabalho remoto.
- Estabelecer procedimentos que garantam a segurança da informação para o acesso aos sistemas (*logon*).
- Prover a segurança da informação quando da utilização de programas utilitários que sejam capazes de sobrepor os controles dos sistemas e aplicações.
- Assegurar que o acesso à informação e às funções dos sistemas de aplicação, por parte dos usuários, seja baseado nos requisitos de restrição de acesso do negócio.
- Criar contas de serviço observando-se a premissa do menor privilégio possível, os requisitos do negócio, e o resultado da análise de risco.
- Monitorar o acesso e o uso dos sistemas para os fins desta Norma.

Gestor do ativo de informação

- Descrever o ativo de informação.
- Definir as exigências de segurança da informação e comunicações do ativo de informação.
- Definir procedimentos e critérios de acesso das informações, observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes.
- Propor regras específicas ao uso das informações.
- Indicar os riscos que podem afetar os ativos de informação.

- Comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários.
- Buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento.
- Realizar uma análise crítica dos direitos de acesso dos usuários, autorizando ou não o acesso.
- Autorizar o acesso às informações sob sua gestão somente para o pessoal baseado estritamente nas necessidades de conhecimento.

Custodiante do ativo de informação

- Manter a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, de acordo com os requisitos de segurança e os direitos de acesso definido pelo Gestor da Informação.

Usuários

- Zelar pela integridade e confidencialidade de suas credenciais de acesso aos recursos computacionais da EPE (identificação de usuário e senha).
- Zelar e contribuir para um efetivo controle de acesso aos recursos computacionais da EPE, de forma a prevenir o acesso não autorizado aos ativos informacionais e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.
- Assegurar a segurança da informação ao utilizar computação móvel e demais recursos de trabalho remoto.

5.1.2. Detalhamento

O processo de concessão de credenciais de acesso aos ativos de informação da EPE deve levar em conta os resultados da análise de risco de Segurança da Informação e Comunicações e o processo de concessão de acesso à informação deve levar em conta a autenticidade dessas credenciais de acesso.

5.1.2.1. Criação ou Bloqueio de Conta de Acesso

A solicitação para criação ou bloqueio de contas de acessos de usuários, quando do início ou término da prestação de serviço, pode ser realizada pelas áreas do quadro abaixo.

A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento de acesso para qualquer usuário.

Área Responsável pela Solicitação de Criação ou Bloqueio de Conta de Acesso	Categorias de Usuário Para os Quais Pode Solicitar a Criação ou Bloqueio de Conta de Acesso
Área de Recursos Humanos da Superintendência de Recursos Logísticos (SRL)	Empregados, Cedidos e Estagiários
Superintendentes e outros hierarquicamente equiparados	Prestador de Serviço Terceirizado
Diretor da área a que o usuário estiver vinculado	Outros usuários

5.1.2.2. Exclusão de Conta de Acesso

A exclusão de conta de acesso de um usuário somente poderá ser executada caso sua identificação não tenha sido criada corretamente e não existam registros de *logs* gerados pelos acessos aos ativos de informação da organização. Caso tenha ocorrido pelo menos um registro de acesso aos ativos de informação, a conta de acesso deve ser bloqueada indefinidamente.

5.1.2.3. Análise Crítica do Direito de Acesso

Cabe ao Gestor da Informação realizar a cada 6 (seis) meses uma análise crítica dos direitos de acesso do usuário aos ativos de informação sob sua gestão. Nos casos de ativos de informações sigilosos, esta análise deve ser feita a cada 3 (três) meses.

5.1.2.4. Integridade e Confidencialidade das Credenciais de Acesso

A fim de zelar pela integridade e confidencialidade de suas credenciais de acesso e efetivamente contribuir para a efetiva gestão do controle de acesso aos recursos computacionais e informacionais da EPE, o Usuário deve seguir as seguintes regras:

- Manter a confidencialidade de sua senha pessoal.
- Trocar de senha na primeira vez que utilizar a conta de acesso aos sistemas.
- Solicitar uma nova senha, quando do esquecimento.
- Evitar o registro das senhas em qualquer meio.
- Alterar a senha sempre que existir qualquer indicação de possível comprometimento de sua confidencialidade.
- Criar senhas que sejam fáceis de lembrar, mas que não sejam baseadas em elementos que outras pessoas ou possíveis invasores possam facilmente adivinhar, ou deduzir, a partir de informações pessoais, como, por exemplo:

- Nome do usuário;
- Identificador do usuário (ID), mesmo que seus caracteres estejam embaralhados;
- Nome de membros de sua família ou de amigos íntimos;
- Nomes de pessoas ou lugares em geral;
- Nome do sistema operacional ou da máquina que está sendo utilizada;
- Datas significativas, como a do nascimento próprio, de um filho, esposa, etc.;
- Números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
- Placas ou marcas de veículos;
- Palavras que constam de dicionários em qualquer idioma;
- Letras ou números repetidos.

- Alterar a senha em intervalos regulares e evitar a reutilização de senhas antigas.
- Escolher suas próprias senhas.
- Selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que o obrigue a registrá-la em qualquer outro meio para não serem esquecidas.
- Encerrar as sessões ativas ou utilizar-se do mecanismo de bloqueio de acesso (tela de proteção com senha) quando precisar se afastar dos equipamentos, mesmo que seja por um período curto.

É vedado a todo usuário:

- Incluir senhas em processos automáticos de acesso a sistemas, por exemplo, armazenadas em macros ou nos navegadores da WEB.
- Revelar credenciais de acesso ou permitir o acesso a ativos de informação por terceiros por meio dessas credenciais.

5.1.2.5. Acesso e Utilização de Computação Móvel

Para viabilizar a segurança da informação ao acessar e utilizar computação móvel e demais recursos de trabalho remoto, o usuário deve:

- Efetuar o acesso remoto às informações do negócio, pela internet, utilizando-se dos recursos de computação móvel da instituição, após o processo de identificação e autenticação bem-sucedido e com os mecanismos de controle de acesso apropriados.
- Evitar ao máximo o acesso à rede de comunicação da EPE a partir de equipamento de terceiros.

- Levar em conta a ameaça de acesso não autorizado à informação, ou aos recursos informacionais sob sua responsabilidade, por outras pessoas na residência ou local de trabalho remoto.
- Efetuar o processo correto de desconexão quando conectado a partir de um computador remoto.

5.1.2.6. Estações de Trabalho e Outros Ativos de Informação

A implementação de um processo de controle de acesso para gerenciar as permissões de acesso a todas as estações de trabalho e outros ativos de informação utilizados na Empresa, não importando sua localização física, deve contemplar os seguintes requisitos gerais:

- Possibilitar o gerenciamento do direito de acesso aos diversos ativos de informação.
- Conceder os direitos de uso exclusivamente conforme a necessidade.
- Estabelecer e manter um processo de autorização e registro de todos os direitos de acesso concedidos.
- Contemplar o treinamento dos usuários quanto às boas práticas de segurança na seleção e uso de senhas.
- Fornecer um identificador único (conta de acesso) para cada usuário da rede de computadores da Empresa, de forma que cada usuário possa ser identificado e feito responsável por suas ações.
- Garantir que as senhas dos usuários dos recursos computacionais da EPE, quando digitadas, não sejam mostradas na tela de seus respectivos computadores.
- Garantir que as senhas sejam armazenadas de forma segura, por meio de criptografia, não permitindo a leitura das mesmas.
- Manter sistema que possibilite o registro de senhas anteriores e bloqueio da utilização das mesmas.
- Alterar as senhas padrões definidas pelos fabricantes de equipamentos programáveis ou configuráveis, tão logo o equipamento tenha sido energizado.
- Entregar ao usuário, obtendo sua ciência, Termo de Responsabilidade por Ativos de Informação descrevendo seus deveres e obrigações de acesso aos ativos de informação da EPE.
- Permitir o acesso somente com os procedimentos de autorização concluídos.
- Garantir que o acesso a qualquer recurso computacional esteja sujeito a um processo formal de autorização.
- Atualizar o direito de acesso de usuários que tenham mudado de função ou bloquear o direito de acesso de usuários que tenham cessado o vínculo com a EPE.

- Estabelecer procedimentos para a proteção dos ativos de informação contra *software* malicioso.
- Prever a realização de auditoria e monitoração da segurança.
- Prever a preservação de log de acesso e de tentativas mal sucedidas de acesso aos ativos de informação.
- Garantir que a necessidade de bloqueio de acesso do terminal de computador, por inatividade, seja compatível com os riscos de segurança da área e os riscos relacionados aos usuários do terminal.
- Garantir que a necessidade de desconexão aos sistemas *web*, por inatividade, seja compatível com os riscos de segurança da área, a classificação da informação que está sendo manuseada e as aplicações que estão sendo utilizadas.

5.1.2.7. Controle e Autenticação do Acesso Remoto

Com a finalidade de prover o controle e a autenticação do acesso remoto pelo usuário, e viabilizar a segurança da informação, quando for necessária a utilização de computação móvel e demais recursos de trabalho remoto, é necessário:

- Determinar o nível de proteção e o método de autenticação requerido somente após uma avaliação de risco.
- Prover recursos de criptografia para o acesso remoto do usuário.
- Estabelecer proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nos recursos móveis.
- Criar e manter proteção adequada contra perda, furto ou roubo de informações; caso uma dessas situações ocorra, deve ser possível executar a recuperação rápida e fácil das informações.
- Efetuar treinamento especialmente direcionado à segurança e utilização de equipamentos móveis, aos respectivos usuários.
- Permitir o acesso remoto aos recursos computacionais da rede da EPE somente após autorização do Superintendente do usuário solicitante.
- Provisionar equipamento de comunicação apropriado que inclua métodos seguros de acesso remoto.
- Revogar os direitos de acesso remoto quando cessarem as atividades de trabalho remoto.
- Proteger computadores e sistemas de comunicação que estejam instalados com recursos que permitem o diagnóstico remoto para manutenção.

- Verificar a real necessidade de interligação ou compartilhamento de recursos de rede e de processamento de informações entre parceiros de negócios.
- Implementar um sistema de autenticação dos equipamentos que podem ter acesso às facilidades de comunicação de rede.

5.1.2.8. Utilização de Programas Utilitários

Com o objetivo de prover a segurança da informação, quando da utilização de programas utilitários que sejam capazes de sobrepor os controles dos sistemas e aplicações, deve-se:

- Utilizar procedimentos de autenticação para utilitários de sistema.
- Limitar a utilização dos utilitários de sistemas a um número mínimo de usuários confiáveis e autorizados.
- Efetuar o registro de cada uso dos utilitários de sistema.
- Definir e documentar todos os níveis de autorização necessários para os utilitários de sistema.
- Remover todos os *softwares* utilitários e demais sistemas desnecessários.

5.1.2.9. Restrição de Acesso do Negócio

A fim de assegurar que o acesso à informação e às funções dos sistemas de aplicação, por parte dos usuários, seja baseado nos requisitos de restrição de acesso do negócio e dos respectivos sistemas e serviços, os sistemas aplicativos devem contemplar as seguintes regras:

- Fornecer menus para controlar o acesso às funções dos sistemas de aplicação.
- Restringir o conhecimento de informações ou funções da aplicação às quais o usuário não tem autorização de acesso, por meio da elaboração de manuais de utilização de sistemas de aplicação direcionados às necessidades do usuário.
- Controlar os direitos dos usuários de leitura, escrita, deleção e execução.
- Assegurar que as saídas dos sistemas de aplicação que tratam informações sensíveis contenham somente informações relevantes a essas saídas e sejam enviadas para terminais e locais autorizados.

5.2. Segurança Física

Dispõe sobre a importância da prevenção contra o acesso físico não autorizado que pode causar danos e interferências com as instalações e informações da Empresa.

5.2.1. Papéis e Responsabilidades

Superintendência de Recursos Logísticos - SRL

- Prevenir o acesso não autorizado, dano ou interferência às instalações físicas da EPE.
- Proteger as áreas e perímetros de segurança internos por controles de entrada apropriados.
- Zelar pela segurança patrimonial da empresa, particularmente quando da presença de terceiros nas dependências da Empresa.

Superintendência de Tecnologia da Informação - STI

- Prover o suporte de TIC na implementação das regras de segurança física.

Gestor de Segurança da Informação e Comunicações - GSIC

- Estabelecer os requisitos de segurança física necessários a garantir a SIC.
- Monitorar continuamente a eficiência e efetividade das medidas de segurança física que afetam a SIC.

Usuários

- Utilizar credencial de acesso físico ostensivo (crachá) em local visível quando nas dependências da Empresa.
- Zelar pela proteção e preservação das instalações físicas da Empresa.

5.2.2. Detalhamento

5.2.2.1. Acesso as Instalações

Ao adentrar as instalações da empresa e durante todo o tempo em que nela permanecer, o empregado da EPE, pessoal terceirizado ou outro colaborador conveniado deve portar sua credencial de acesso (crachá) em local visível.

Os visitantes devem ser identificados nas áreas de recepção e devem receber um selo de identificação para ser colocado em local visível.

Os empregados da EPE devem interpelar qualquer pessoa estranha que não esteja acompanhada e qualquer pessoa que não esteja usando uma identificação visível para saber se a mesma esta perdida, encaminhando-a à área de recepção mais próxima.

A fim de prevenir o acesso não autorizado, dano ou interferência às informações e instalações físicas da EPE, deve-se tomar as seguintes medidas:

- Situar as áreas críticas ou sensíveis da Empresa em locais seguros com perímetro de segurança definido, assim como manter barreiras de segurança e controles de entrada apropriados em volta dessas áreas.
- Levar em consideração os riscos identificados na definição do grau de proteção dos perímetros de segurança e demais instalações físicas da empresa.
- Verificar a existência de falhas de segurança no perímetro ou áreas críticas que permitam o comprometimento da segurança física.
- Proteger devidamente as portas externas contra o acesso não autorizado, com mecanismos de controle, barras, alarmes, fechaduras e etc..
- Garantir que a empresa tenha uma área de recepção com pessoal ou outro meio de controle do acesso físico.
- Garantir que o acesso à empresa somente ocorra com pessoal expressamente autorizado.
- Assegurar que nos CPDs e na sala de processamento e armazenamento de documentos do Centro de Documentação (CEDOC), as barreiras físicas sejam estendidas do piso bruto ao teto bruto, para impedir o acesso não autorizado, o isolamento contra propagação de fogo e contaminação ambiental.
- Garantir a instalação e utilização de portas corta-fogo no perímetro de segurança das áreas críticas ou sensíveis, equipadas com alarme e fechamento automático.
- Controlar e restringir o acesso físico às áreas de armazenamento de informações e às instalações de equipamentos sensíveis somente a pessoal autorizado.
- Utilizar controle de autenticação por biometria para autorizar e validar todos os acessos.
- Armazenar as trilhas de auditoria de todos os acessos em local seguro.
- Monitorar a utilização, por parte dos usuários, da credencial de acesso físico (crachá) em local visível.
- Rever e atualizar regularmente os direitos de acesso a áreas críticas e sensíveis.

5.2.2.2. Realização de Trabalhos em Áreas Seguras

Com a finalidade de assegurar a SIC, por ocasião da realização de trabalhos em áreas seguras, as seguintes medidas devem ser observadas:

- Divulgar a existência de uma área segura e das atividades nela executadas só quando for realmente necessário.

- Utilizar controles de acesso para o pessoal ou para terceiros que trabalham dentro da área segura.
- Evitar o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para não dar oportunidade a atividades mal intencionadas.
- Permitir atividades de terceiros somente quando autorizado e a atividade possa ser monitorada por empregado do quadro próprio da Empresa.
- Trancar e inspecionar periodicamente as áreas seguras desocupadas.
- Criar barreiras e perímetros adicionais de controle de acesso físico entre áreas com diferentes requisitos de segurança dentro do perímetro de segurança.
- Proibir a presença de equipamento fotográfico, de vídeo, áudio ou gravação, a não ser com autorização.

5.2.2.3. Realização de Entregas e Carregamentos

Deve-se controlar e isolar os equipamentos de processamento de informações nas áreas de entrada e saída de materiais para evitar o acesso não autorizado.

Além disso, deve-se determinar, por meio de uma avaliação dos riscos, os requisitos de segurança para tais áreas com o fim de restringir o acesso a pessoal identificado e autorizado e projetar ou escolher área de armazenagem provisória (quando pertinente) de forma que os materiais possam ser descarregados/carregados sem que o pessoal externo tenha acesso indevido a EPE.

Todo o material recebido/expedido deve ser registrado ao dar entrada/saída na Empresa.

5.2.2.4. Segurança Física dos Equipamentos

Para assegurar a proteção dos equipamentos, é necessário:

- Proteger os equipamentos fisicamente contra as ameaças à sua segurança e dos perigos ambientais.
- Planejar a localização e disposição dos equipamentos, de modo a reduzir o risco das ameaças e perigos do meio-ambiente e as oportunidades de acesso não autorizado.
- Criar controles especiais para proteção contra perigos ou acesso não autorizado e para preservar os equipamentos de apoio, como o suprimento de corrente e a infraestrutura de cabeamento.
- Posicionar os equipamentos de processamento e armazenagem de informações que manuseiam dados sensíveis de modo a minimizar o risco de olhares indiscretos durante o uso.
- Isolar os itens que requerem proteção especial a fim de garantir o nível apropriado de proteção.

- Adotar controles para minimizar o risco de ameaças potenciais, incluindo furto, incêndio, fumaça, água (ou falha no abastecimento), poeira, vibração, efeitos químicos, interferência no suprimento de força e radiação eletromagnética.
- Proibir comer, beber e fumar nas instalações de processamento de informações ou em sua proximidade.
- Monitorar as condições ambientais quanto a fatores que podem afetar negativamente a operação dos equipamentos de processamento de informações.
- Considerar o impacto de um acidente em instalações próximas, como por exemplo, um incêndio no prédio vizinho ou em outras empresas localizadas no mesmo prédio, vazamento de água do telhado, ou dos andares acima da EPE, ou uma explosão na rua.
- Proibir a identificação dos equipamentos de processamento de informações sensíveis nas listas de pessoal e listas telefônicas internas ou em locais acessíveis ao público.

5.2.2.5. Proteção de Informações e de Recursos de Processamento

Visando evitar exposição ou roubo de informações e de recursos de processamento da informação das salas e instalações, deve-se:

- Adotar procedimentos para garantir a política de mesa limpa e tela limpa.
- Posicionar equipamentos críticos em local não acessível ao público.
- Escolher salas discretas e que indiquem o mínimo possível a sua finalidade, sem sinais visíveis, dentro ou fora da sala, que identifiquem a presença de atividades de processamento de informações.
- Evitar a divulgação de detalhes da arquitetura da rede em acessos externos.
- Posicionar funções e equipamentos de suporte, equipamentos como fotocopiadoras e fax, num local apropriado dentro da área segura.
- Implantar sistemas apropriados de detecção de intrusos, instalados segundo padrões profissionais, e testados regularmente para cobrir todas as portas externas.
- Dispor alarme armado permanentemente nas áreas não ocupadas.
- Dispor equipamentos administrados pela organização fisicamente separados dos equipamentos administrados por terceiros.
- Armazenar de modo seguro e a uma distância adequada de uma área segura os materiais perigosos ou combustíveis.
- Armazenar os suprimentos em grande volume dentro de uma área segura, somente sendo requisitados à medida que forem sendo utilizados.

- Posicionar a uma distância segura os equipamentos e mídia de backup, para que não sejam danificados em caso de um acidente no site principal da organização.

5.2.2.6. Suprimento de Energia Elétrica e Água

A fim de garantir o suprimento adequado de eletricidade que atenda às especificações dos fabricantes dos equipamentos, evitando-se quedas e oscilações de tensão frequentes e sobrecargas, deve-se:

- Manter plantas atualizadas da rede elétrica.
- Utilizar múltiplas fontes de alimentação para evitar que o suprimento dependa de uma única fonte, sempre que possível.
- Fornecer suprimento de energia à prova de interrupções (sistema *no break*) para os equipamentos dos CPDs e para os ativos críticos e/ou sensíveis.
- Providenciar um plano de contingência indicando as ações a serem tomadas em caso de falha do *no break*.
- Realizar testes periódicos dos equipamentos de suprimento de energia elétrica regulada, de acordo com as recomendações dos fabricantes, para assegurar que tenham a capacidade adequada.
- Localizar as chaves de força de emergência perto das saídas de emergência das salas de equipamentos.
- Ter iluminação de emergência para o caso de falta de energia elétrica.
- Verificar periodicamente se as instalações elétricas do prédio e as instalações destinadas aos equipamentos de energia da EPE estão em boas condições e não oferecem perigo.
- Garantir exclusividade das instalações elétricas no CPD.
- Manter um plano de manutenção para a rede elétrica.

E quanto às condições gerais de segurança relacionados com suprimento de água, deve-se:

- Manter plantas atualizadas da rede hidráulica.
- Retirar qualquer encanamento, exceto o necessário, do piso ou teto falso em áreas sob ou sobre as áreas seguras.
- Garantir escoamento de água e drenagem adequada para impedir inundação nas áreas seguras.

5.2.2.7. Segurança do Cabeamento

Quanto à segurança do cabeamento, deve-se:

- Dar proteção adequada às linhas de força e as linhas de telecomunicações.

- Proteger o cabeamento de rede contra interceptação não autorizada ou danos por meio da utilização de dutos, evitando trajetos que passem por áreas públicas.
- Separar os cabos de força dos cabos de comunicações para evitar interferências.
- Utilizar dutos blindados e salas ou caixas trancadas em pontos de inspeção e pontos terminais.
- Planejar o uso de rotas ou meios de transmissão alternativos.

5.2.2.8. Utilização de Equipamentos Fora das Instalações

Quanto à segurança dos equipamentos fora das instalações da EPE, deve-se:

- Adotar procedimentos de segurança para todo ativo (todas as formas de computadores pessoais, agendas eletrônicas, telefones celulares, papel ou outros meios) que ficam na posse da pessoa para trabalho a domicílio ou que são transportados para fora do local normal de trabalho.
- Proporcionar grau de segurança equivalente ao do equipamento utilizado no site para os mesmos fins, levando em conta os riscos do trabalho fora das instalações da organização.
- Supervisionar equipamentos e as mídias retiradas das instalações da organização, sempre que possível.
- Transportar os computadores portáteis como bagagem de mão e disfarçados sempre que possível, quando em viagem.
- Observar a qualquer tempo, as instruções do fabricante para a proteção dos equipamentos (ex.: proteção contra a exposição a campos eletromagnéticos intensos).
- Ter uma cobertura de seguros adequada para proteger o equipamento quando fora do site.

5.2.2.9. Segurança no Descarte ou na Reutilização de Equipamentos e Materiais

No descarte ou na reutilização de equipamentos e materiais que contenham qualquer tipo de informação, deve-se atentar aos cuidados necessários conforme o tipo de equipamento e material e a informação neles contidos.

Deve-se destruir fisicamente ou sobrescrever de maneira segura (ao invés de se usar a função *delete*) os sistemas de armazenagem que contenham informações sensíveis. Devem-se verificar todos os itens de equipamento que contenham mídia de armazenagem, como por exemplo, discos rígidos, para garantir que todos os dados sensíveis e softwares licenciados tenham sido retirados ou sobrescritos antes do descarte ou reutilização. Os dispositivos de armazenagem danificados devem ser avaliados quanto às informações neles contidos, para determinar a conveniência de serem consertados, descartados ou destruídos.

Os materiais que contenham informações (CDs, papel etc..) devem ser destruídos de forma a impedir sua recomposição.

5.2.2.10. Mesa Limpa e Tela Limpa

Fica estabelecida a política de mesa limpa para documentos e mídia de armazenagens removíveis e tela limpa para os recursos de processamento da informação, de forma a reduzir riscos de acesso não autorizado, perda e danos à informação classificada em qualquer grau de sigilo, durante e fora do horário normal de trabalho.

As seguintes regras devem ser observadas no que diz respeito à adoção da mesa limpa e tela limpa:

- Não expor em cima de mesas documentos e mídias contendo informações classificadas em qualquer grau de sigilo, que possam ser danificadas, furtadas, ou destruídas em caso de catástrofes, como incêndios, inundações ou explosões.
- Armazenar documentos e mídia de computador em armários e estantes apropriadas e trancadas ou em outras formas de mobília de segurança, quando não estiverem em uso, principalmente fora do horário de expediente.
- Trancar informações empresariais sensíveis ou críticas em um cofre ou arquivo à prova de fogo quando não em uso, principalmente quando não houver ninguém no escritório.
- Proteger computadores pessoais e terminais de computador, bem como as impressoras por bloqueios de teclas, senhas ou outros controles, quando não estiverem em uso.
- Proteger postos de correspondência recebida e enviada e as máquinas de fax que não contemplem a presença constante de um operador.
- Proteger copiadoras contra o uso não autorizado fora do horário normal de expediente.
- Retirar informações sensíveis ou confidenciais, quando impressas, das impressoras imediatamente após a impressão.

5.2.2.11. Equipamentos de Prevenção e Combate a Incêndios

Quanto aos equipamentos de prevenção e combate a incêndios, produtos e locais críticos, deve-se:

- Manter a compatibilidade dos equipamentos de prevenção e combate a incêndios com o ambiente onde podem vir a ser necessários.
- Prover uma quantidade suficiente de equipamentos, mantendo-se uma margem para contingência.
- Distribuir os equipamentos em locais adequados e garantir o acesso livre aos mesmos.
- Conferir a validade das cargas dos equipamentos de combate a incêndio periodicamente.

- Instalar sensores e alarmes e mola para fechamento automático nas portas de incêndio.
- Instalar detectores de fumaça sob o piso falso, no teto e no sobre teto.
- Dispor os equipamentos distantes das linhas de transmissão de alta voltagem.
- Prover cestas de lixo de metal com tampa com objetivo de abafar princípios de incêndio.

5.2.2.12. Condições Gerais de Segurança da Edificação

A fim de zelar pela segurança da edificação, deve-se:

- Remover o lixo diariamente.
- Verificar periodicamente a necessidade de efetuar dedetização e desratização.
- Proibir a execução de trabalho que gerem poeira na área dos equipamentos, sem que sejam tomados os cuidados necessários para a execução dos mesmos.
- Manter trancados os quadros de conexões telefônicas e distribuição do cabeamento de rede e garantir que o acesso somente seja permitido ao pessoal autorizado.
- Manter e testar os detectores de fumaça de forma programada.
- Instalar sensores de temperatura e umidade do ar.
- Verificar a necessidade de suplementar os recursos condominiais com quadros de controle que detectem e localizem rapidamente fogo e fumaça.
- Utilizar placas do piso falso que sejam facilmente removíveis a fim de facilitar a verificação de fogo e fumaça.
- Manter marcações no piso para facilitar a localização dos detectores.
- Manter plantas de localização dos extintores e detectores.
- Manter sensoriamento de portas, janelas, dutos e supervisão predial.
- Ter uma sala central de controle de segurança bem localizada e com qualificação pessoal, mesmo que seja a do condomínio.
- Efetuar monitoramento do perímetro e áreas externas à empresa via CFTV.
- Prover a proteção adequada ou estabelecer perímetros de segurança para estações de trabalho e servidores não monitorados por um longo período de tempo (CPD), principalmente no que diz respeito ao acesso não autorizado.
- Manter a área do CPD em local não visível da rua.
- Manter as portas do CPD fechadas e com acesso controlado.
- Instalar alarmes para informar à vigilância ou a quem de direito, a violação de portas e acessos a áreas do CPD.

- Manter um serviço de vigilância de 24 horas, inclusive nos fins de semana e feriados.
- Verificar as saídas de emergência em relação à usabilidade periodicamente.
- Efetuar rodízio periódico entre os (as) recepcionistas.
- Manter uma rede de iluminação bem distribuída e de boa qualidade com iluminação de emergência.
- Fornecer manual ao corpo de vigilantes ou agentes prediais com procedimentos de emergência.
- Manter um sistema de claviculário na área de serviços gerais.
- Manter um controle rigoroso das chaves das portas.
- Dispor de quadros de luz e iluminação em locais adequados.
- Manter o controle da temperatura nas imediações do perímetro.

5.2.2.13. Monitoração de CFTV

A monitoração das instalações da EPE por CFTV visa à proteção dos ativos físicos e informacionais, devendo ser ao mesmo tempo compreensiva e privativa.

Para isso, o sistema de monitoração deve:

- Manter a privacidade das áreas de uso individual como a estação de trabalho.
- Cobrir todas as áreas de circulação, entradas e saídas.
- Cobrir todas as áreas de acesso restrito, tanto externa como internamente.
- Permitir a captura detalhada e resumida das imagens monitoradas.
- Possibilitar a retenção das imagens capturadas por um período não inferior a dois anos.
- Anunciar ostensivamente os locais sendo monitorados.

.A visita às imagens capturadas deve guiar-se pelo seguinte:

- Ocorrer somente quando houver indícios de incidentes de segurança e para a verificação da eficácia do sistema.
- Ser feita sempre por mais de uma pessoa, concomitantemente.
- Ter um registro de quem acessou, quando e com que fim, bem como das imagens visitadas.

5.2.2.14. Condições Gerais de Segurança com Evacuações

Quanto às condições gerais de segurança relacionados com evacuações, deve-se:

- Manter um procedimento de evacuação.
- Manter as saídas de emergência livres e desimpedidas e em boas condições.
- Manter iluminação de emergência e sinalização adequada (efetuar testes regularmente).

- Manter telefones internos de emergência para comunicação de sinistros.
- Manter um sistema de alarme para fazer a evacuação do prédio, mesmo que seja a do condomínio.

5.2.2.15. Segurança de Ar-Condicionado

Quanto às questões de segurança relacionadas ao ar-condicionado, deve-se:

- Garantir a qualidade das instalações e manutenção dos equipamentos e em nível de ruído satisfatório.
- Eliminar a possibilidade de entrada de gases através dos dutos de ar-condicionado.
- Garantir que as chaves de emergência desliguem o sistema de ar-condicionado.
- Garantir que o sistema de climatização seja exclusivo e que não seja compartilhado com área e/ou tipo de equipamentos inadequados.
- Garantir que o dimensionamento do equipamento de ar-condicionado seja adequado.
- Garantir que as aberturas externas (troca de ar) proporcionem uma adequada renovação.
- Utilizar *dampers* corta-fogo e gases no interior dos dutos.
- Instalar os equipamentos de ar-condicionado em compartimentos fechados (com acesso somente ao pessoal autorizado).
- Proteger as tomadas de ar contra contaminação.
- Verificar a necessidade de existirem alarmes nos sistemas de ar-condicionado.
- Utilizar dutos do ar condicionado de material retardante da propagação de fogo.
- Proteger os instrumentos de comando do sistema de ar-condicionado prevenindo o acesso não autorizado.
- Manter plantas com especificações de toda a rede de ar-condicionado.

5.2.2.16. Manutenção e Retirada de Equipamentos e Bens

Quanto à manutenção e à retirada de bens e equipamentos, deve-se:

- Fornecer manutenção correta aos equipamentos para assegurar sua disponibilidade e integridade permanente, com a periodicidade e especificações recomendadas pelo fabricante.
- Somente realizar a manutenção e os reparos dos equipamentos através de pessoal de manutenção autorizado, habilitados e treinados para isso.
- Manter um registro de todos os defeitos suspeitos ou reais e de toda a manutenção preventiva e corretiva executada.

- Não permitir a saída de equipamentos, informações ou software da EPE sem autorização.
- Registrar a saída e a devolução dos equipamentos.

6. Disposições Gerais

Casos omissos ou excepcionais serão submetidos à aprovação da Diretoria Executiva.

A não observância aos dispositivos dessa Norma pode acarretar, nos termos da legislação aplicável, sanções administrativas, civis e/ou penais.

Este Instrumento Normativo entra em vigor em 19/01/2015, conforme decisão da Diretoria Executiva da EPE.

7. Anexos

Não se aplica.