PROJETO SREI

Sistema de Registro Eletrônico Imobiliário

Parte 4 – Auditoria Operacional de TIC

C - Roteiro para auditoria operacional de TIC

Título	SREI Parte 4 C - Roteiro para auditoria operacional de TIC
Versão	Versão 1.1 release 2
Data da liberação	30/05/2012
Classificação	Restrito
Autores	Matteo Nava
Propriedade	CNJ
Restrições de acesso	LSI-TEC, CNJ e ARISP

Sumário

1 Introdução

Este documento descreve os procedimentos para a auditoria dos requisitos do Ambiente operacional de T.I. O auditor deve utilizar os procedimentos descritos neste documento para a análise dos ambientes que necessitam atender os requisitos descritos no documento citado anteriormente para a certificação SREI.

O processo de auditoria contempla duas etapas, sendo a primeira de análise de documentações, consiste na avaliação dos requisitos que se apoiam nas documentações para a sua implementação. Sucessivamente é realizada a segunda fase da auditoria que demanda a presença do auditor para avaliar localmente a conformidade dos requisitos.

2 Escopo

Este documento deve ser utilizado pelo auditor para a avaliação dos requisitos operacionais de TI dos sistemas do SREI. Os procedimentos são diferenciados de acordo com um dos quatros tipos de ambiente contemplados na arquitetura do SREI, conforme descrito a seguir:

Tipo ambiente	**Descrição**
Cartório	Cartório de Registro de Imóveis
Cartório com restrições	Cartório de Registro de Imóveis com restrições de recursos operacionais e de recursos financeiros
Provedor de serviço	Provedor de serviço contratado que abriga parte das operações do cartório.
SAEC	Serviço de Atendimento Eletrônico Compartilhado

3 Fase 1 - Analise de documentações

Consiste no levantamento e na sucessiva análise das documentações dos ambientes e dos processos de T.I. utilizados pelo SREI. São assim verificados as políticas, os procedimentos operacionais e a configuração dos sistemas de T.I. para verificar a conformidade com os requisitos operacional do SREI. Esta fase é realizada antes da visita local por parte dos auditores e que poderá em caso de presença de não conformidades graves ser impeditivo para a realização da etapa sucessiva de avaliação presencial.

A seguir são relacionados os principais documentos que devem ser fornecidos para o auditor. É importante evidenciar que na relação a seguir existem documentos que são obrigatórios somente para determinados ambientes, conforme descritos no documento de Requisitos operacionais. Desta forma o auditor deve ajustar a relação de documentos abaixo conforme o ambiente avaliado.

Documento
Política de segurança da informação
Laudo de vistoria (Geradores)
Registro de manutenção (Geradores)
Documentação da rede de comunicação de dados
Arquivos de configuração dos nós de rede
Arquivos de configuração dos equipamentos de proteção de perímetro (Firewalls)
Documentação de configuração segura (Hardening)
Registros de eventos de sistemas críticos
Relatório da última análise interna de vulnerabilidades
Relatório da última análise externa de vulnerabilidades
Política ou Procedimento de gerenciamento de usuários
Procedimento de cópias de segurança
Últimos 3(Três) registros de cópias de segurança
Termo ou Acordo de confidencialidade

Termo ou Acordo de utilização
Política de classificação da informação
Política de uso da internet.
Formulário de atribuição de acesso
Documentos e formulários utilizados para a requisição, aprovação e documentação de mudanças
Procedimento de gestão de incidentes
Resultados e relatórios da última avaliação de riscos
Contratos com parceiros críticos para a prestação de serviços (e.g. Datacenters, fornecedores de sofware, enlaces dedicados, etc)
Plano de continuidade de negócios
Relatórios e resultados da gestão de capacidade
Plano de ação para a gestão de capacidade

Eventualmente, pode ser necessária a solicitação de outras documentações, além destas citadas conforme a necessidade do auditor.

Após o recebimento de todos os documentos, a auditoria deve analisá-los em um prazo máximo de 5 dias uteis. Terminada esta análise e a conclusão do resultado parcial a auditoria, caso o numero de não conformidades seja elevado ao ponto de recomendar o adiamento da continuidade do processo de auditoria, é possível para a fase 2 de auditoria presencial.

4 Fase 2 - Auditoria presencial

A primeira fase da auditoria presencial consiste na averiguação das informações presentes nos documentos analisados, ou seja, é necessário constatar se os processos executados no cartório efetivamente refletem o que está documentado.

Para os demais requisitos que não dependem de documentação, devem ser utilizados os procedimentos relacionados abaixo.

4.1 Segurança física

Descrição
a) Verificar a presença da descrição das características dos níveis de segurança na política de segurança da informação. A política de segurança da informação deve conter: • Ilustração simbólica representando os 3(três) níveis de segurança exigidos; • O nível que apresenta maior criticidade deve estar contido no nível de menor criticidade, sendo assim, o nível 3(três) deve estar contido no nível (dois) e ambos os níveis contidos no nível 1(um). Ilustrando, deste modo, a presença de controles de acesso cumulativos entre os níveis; • Descrição das medidas para o controle de acesso às áreas críticas. b) Inspecionar fisicamente o ambiente auditado para verificar a presença das barreiras físicas entre níveis exigidas. c) Verificar se há componentes oriundos dos níveis 2(dois) e 3(três) instalados fisicamente no nível 1(um).
a) Verificar a presença de barreira física entre os níveis 2(dois) e 3(três). A forma de acesso entre estes níveis deve utilizar: • Porta com tranca através de chave, cartão de acesso ou biometria. b) Verificar a utilização de alguma forma de controle de acesso de visitantes às áreas de nível 2(dois). Esta medida deve possibilitar a identificação do visitante e constar a permissão do colaborador. c) Verificar os métodos de controle de conexão de equipamentos de terceiros (visitantes, fornecedores, manutenção, etc).
a) As áreas de nível 3(três) não devem conter nenhum tipo de sistema oriundos dos níveis 1(um) e dois(dois). b) Verificar os acessos concedidos a estas áreas. Nenhum individuo, fora aqueles necessários ao funcionamento do sistema como, por exemplo, a área de suporte, deve possuir acesso às áreas de nível 3(três). c) O controle de acesso a esta área deve ser: • Através de porta com tranca manual ou eletrônica; ou • Delimitado por *racks* com tranca.

a) Verificar se há a presença de equipamentos que contenham ou gerenciam sistemas de segurança predial na mesma delimitação física das áreas críticas de nível 3(três). Caso sejam utilizados *racks* com tranca, deve ser verificada a presença destes equipamentos num mesmo *rack.*

4.2 Suprimento de energia elétrica

Descrição
a) Verificar a presença de no-breaks e se estes alimentam os seguintes itens: • Servidores críticos; e • Componentes de rede que viabilizam a disponibilidade do serviço. b) Outros equipamentos como, por exemplo, sistemas de segurança devem estar conectados em estabilizadores de energia.
a) Verificar a presença de geradores. Os seguintes cuidados devem ser observados: • Os geradores devem estar instalados em locais afastados da operação e das áreas críticas. • Possuir laudo de vistoria do corpo de bombeiros. • Possuir registros de manutenção em dia.
a) Verificar se o sistema de CFTV permite: • Permitir a gravação mesmo em ambientes sem iluminação; • Habilitar a gravação quando detectado movimento; • Permitir monitoramento e gerenciamento centralizado de todo o conjunto de câmeras instalado.
a) Verificar a presença de imagens gravadas no servidor de CFTV com período mínimo de criação de 90 dias anteriores à auditoria.
a) Verificar, através do estudo das imagens geradas ou monitoramento em tempo real, se as câmeras contemplam: • Visualização geral do ambiente de nível 1(um); • Os acessos aos ambientes de níveis 2(dois) e 3(três) possibilitando, sobretudo, a identificação facial de quem acessa; e • Visualização geral do ambiente de nível 3(três).

4.3 Alarme contra intrusão

Descrição
a) Verificar a presença de alarmes de intrusão implementados. O sistema de alarme deve contemplar: • Todos os pontos de acesso e, principalmente, todos os pontos de acesso aos ambientes de nível 2(dois) e 3(três); b) O sistema deve possuir as seguintes características:

• Em ambientes internos o sensor pode ser passivo, micro-ondas ou disc; e • Em ambientes externos devem ser implementados sensores infravermelho capaz de suportar intempéries e de diferenciar movimentos humanos de chuva, vegetação, pássaros e outros animais. • Possuir modulo de comunicação alternativa por *Radio Frequency(* RF), *General Packet Radio Service* (GPRS) ou *Transmission Control Protocol/Internet Protocol* (TCP/IP) em caso de falha no sistema comum transmitido via telefonia fixa.
a) Verificar se os sistemas de alarme estão configurados para ativar fora do período de funcionamento do ambiente. b) Verificar se os sistemas de alarme estão configurados para enviar avisos aos responsáveis pelo perímetro e para o responsável pela segurança predial.

4.4 Prevenção contra incêndio

Descrição
a) Os sistemas de combate a incêndio podem ser divididos em duas categorias de acordo com o cenário de aplicação: • Para pequenos cartórios com baixa disponibilidade de recursos, devem ser utilizados extintores adequados e de fácil acesso na ocorrência de incêndio. Para esta categoria, deve ser considerado: i. Extintores adequados ao tipo de material combustível armazenado na sala. Extintores de água pressurizada para incêndio de classe A (papel, madeira, etc); extintores de Co2 para incêndios de classe C (equipamento elétrico energizado) ou extintores para incêndios de classe B (líquidos inflamáveis) que também podem ser utilizados para incêndios de classes A e C; ii. Verificar o prazo de validade dos extintores; iii. Verificar se não há obstrução para a utilização dos extintores (mesas, *racks,* armários, etc); • Para grandes cartórios, datacenter e outras entidades de grande porte deve ser utilizado sistema de supressão por agente limpo (NFPA-2001) acionados por sistemas eletrônicos de detecção de incêndios. Adicionalmente, a entidade deve disponibilizar extintores obedecendo às mesmas regras citadas acima.
a) Todos os ambientes passíveis de incêndio devem ser verificados para identificar a presença de sensores de fumaça. Estes alarmes podem atender os seguintes tipos: • Fotoelétrico; • Térmico; • Ultravioleta; • Iônico; • Óptico; • Termovelocimétrico;

• Para CPDs podem ser utilizado sensores de temperatura Programável. b) Os seguintes itens devem ser verificados: • Área de abrangência do sensor versus a área total do ambiente; • Funcionamento da sirene (embutida no sensor ou alto falantes separados); • Sensibilidade dos sensores. Estes testes podem ser realizados através de acionamento da função de testes do sensor, caso exista, ou através da simulação de incêndio por fumaça ou chama.
a) Verificar se o volume sonoro das sirenes é audível em todos os ambientes. b) Verificar se o sistema de alarmes possui função remota de aviso.

4.5 Ventilação e climatização

Descrição
a) Verificar se o ambiente de operações possui sistema de condicionamento de ar capaz de executar a renovação do ar ambiente; b) Caso não haja sistema de condicionamento de ar, verificar se o ambiente possui janelas adequadas ao número de colaboradores e dimensões do perímetro;
a) Verificar se os ambientes possuem sistema de climatização de ar. As seguintes características devem ser verificadas: • Para as operações, a temperatura ideal deve variar entre 21°C a 26°C. • Para CPDs, a temperatura ideal deve ser analisada por empresa especializada em contrapartida com as indicações do fabricante e quantidade de equipamentos quando da instalação do sistema (verificar laudo, nota ou relatório disponibilizado pela empresa de sistema de condicionamento de ar);

4.6 Cofre para mídias de backup

Descrição
a) Verificar se existe cofre para o armazenamento de mídias de cópias de segurança. Verificar, através do manual disponibilizado pelo fabricante ou através de etiquetas e adesivos indicadores no chassi no cofre, o atendimento aos seguintes requisitos: • Ser de aço ou material de resistência equivalente e resistente ao fogo; • Oferecer resistência contra fogo por minimamente 60 minutos, classe S 60 DS da norma EN 1047-2 [3] ou equivalente ANSI/UL 263 [4]; • Oferecer resistência contra arrombamento/abertura WG Classe II (segurança 50/80 RU) da norma EN 1143-1 [5]; • Possuir prateleiras ou gavetas internas para acomodação das mídias de backup;

• Possuir tranca com chave manual ou eletrônica. a) Caso o requisito acima não possa ser atendido. As seguintes medidas devem ser verificadas: • Verificar, através de contato com fabricante ou manual de informações, se o cofre utilizado para armazenar mídias é estanque contra água; • Requisitar os controles compensatórios para o risco de inundação. As seguintes medidas devem ser planejadas: i. Retomada das operações; ii. Salvaguarda das informações de proprietário de direito.

4.7 Outros controles de segurança de infraestrutura

Descrição
b) Requisitar aos oficiais ou responsáveis por guiar a auditoria pelo ambiente auditado o cálculo comprovando os seguintes requisitos: • A uma altura 30% superior da amplitude da última cheia do rio mais próximo (Altura = 0,3*AmplitudeCheia + AmplitudeCheia + AlturaNormalRio); e • A uma altura 30% superior da amplitude da última cheia das ruas próximas (Altura = 0,3*AmplitudeCheia + AmplitudeCheia + AlturaNormalVia); e • Em um local sem risco de inundação decorrente de vazamentos de encanamentos; e • Em um local sem risco de inundação por água da chuva.
a) Verificar se os armários utilizados para abrigar equipamentos de telecomunicações sejam protegidos por chave.
a) Verificar se a infraestrutura predial possui proteção contra raios homologada conforme a Norma NBR5419/93.

4.8 Segurança de tecnologia de informação e comunicação

4.8.1 Redes de comunicação de dados

Descrição
a) Requisitar aos responsáveis pelo ambiente auditado a documentação referente à infraestrutura de comunicação de dados. Esta documentação deve incluir: • Topologia física da rede e equipamentos de comunicação (roteador, *switch, firewall, modens, access point* de redes *wireless*, etc); • Topologia lógica da rede, informando as subredes e as tabelas de roteamento; • A relação de equipamentos (servidor, desktop, roteador, switch, etc) e

suas configurações de rede; • A relação dos sistemas em cada servidor.
a) Verificar através do cadastro de ativos e, também, da análise uma amostra significativa dos equipamentos a presença de identificadores repetidos.
a) Requisitar documentação de rede que possibilite verificar a segregação entre as redes. b) Verificar, adicionalmente, os arquivos de configuração dos switchs que validam a documentação fornecida no requisito anterior. c) Os seguintes requisitos devem ser validados: **a)** Existência de DMZ contemplando todos os servidores com acesso via internet; **b)** Todos os servidores; **c)** Rede de operação (Estações de trabalho), caso necessário, devido a quantidade de equipamentos, a rede de operação pode ser simplificada; **d)** Estações disponibilizadas para clientes; **e)** Todo ponto de acesso de rede sem fio. d) Todas estas redes devem, impreterivelmente, serem segregadas. e) NÃO DEVE haver dados do SREI armazenados em servidores contemplados pela DMZ.
a) Requisitar a configuração dos sistemas de proteção de perímetro utilizados pelo ambiente. Os seguintes requisitos devem ser verificados: • As regras definidas nos equipamentos devem seguir o princípio de '*deny all*', ou seja, todo acesso deve ser negado a princípio e somente acessos conhecidos liberados; • Todos os protocolos liberados devem ser conhecidos e, quando possível, liberados somente para as entidades que necessitam; • Toda regra de firewall deve estar formalmente documentada; • A necessidade de análise críticas das regras de firewall devem estar formalmente declaradas na política de segurança da informação ou documento de igual valor.
a) Levantar e verificar os registros dos procedimentos de gestão de mudança aplicados em alterações do ambiente realizadas anteriormente.
a) Verificar, através das configurações de switchs, roteadores ou sistemas de proteção de perímetro a efetividade do isolamento da rede sem fio. b) Identificar qual o sistema de autenticação utilizado. Conforme o método de implementação utilizado, as seguintes características devem ser verificadas: • 802.11i (WPA2): A senha padrão, fornecida com o equipamento, deve ser trocada antes da sua implementação no ambiente de produção. • Integrado com 802.1x: Verificar se, somente as pessoas autorizadas tenham acesso. c) Nenhum protocolo, além daqueles referidos nesta seção, devem ser utilizados para o controle de acesso às redes sem fio.
a) Buscar as configurações de roteadores, switchs e sistemas de perímetro pela implementação de um canal criptografado entre sites.
a) Constatar a presença de softwares e configurações de teste no ambiente

operacional.

4.8.2 Configuração segura de sistemas

Descrição
a) Requisitar os documentos de configuração segura (*hardening)* referentes a todos os sistemas e componentes de sistemas críticos. Os seguintes itens devem ser verificados: • Exclusão de usuários e senhas padrão, quando possível; • Utilização de parâmetros de operação seguros; • Habilitação somente dos serviços, portas, processos e protocolos necessários para o funcionamento correto do servidor, em função da sua finalidade; • Utilização de tecnologias e protocolos seguros como SSH, SSL, SFTP, entre outros, ao invés de outros inseguros como NetBIOS, FTP, Telnet, etc. • Utilização de protocolos de segurança no acesso com privilégio administrativo, que não seja realizado através do console, utilizando protocolos seguros como, por exemplo, SSH, VPN, ou SSL/TLS; • Habilitação de controles de senhas seguras e uso de hash para codificação de senhas armazenadas. b) Adicionalmente, devem utilizados documentos de configuração segurança desenvolvidos por entidades confiáveis, respeitando as especificidades de cada aplicação. Caso este tipo de documento seja utilizado, requisitar os documentos ao responsável pela entidade e confirmar sua validade.

4.8.3 Rastreabilidade de eventos

Descrição
a) Levantar os logs de NAT e verificar se constam os endereços IPs dos sistemas da rede interna.
a) Requisitar uma amostra dos registros de eventos dos sistemas críticos. b) Verificar se todos os pontos requisitados são atendidos. São eles: • Seção de comunicação com a identificação do endereço IP de origem; • Tentativas de acesso e de *login* (sucesso e falha); • Tentativas de acesso aos serviços (WEB, correio eletrônico, etc); • Ações de cada usuário; • Atividades relevantes dos sistemas.; e c) Verificar se todos os sistemas críticos estão contemplados.
a) Verificar se é utilizado um servidor de centralização dos registros de auditoria gerados pelos sistemas. b) Constatar se todos os sistemas críticos direcionam seus registros a este servidor.
a) Verificar a data de criação e, adicionalmente, as datas inclusas nos registros. O registro mais antigo, para cada sistema, deve constar, no mínimo, 3(três) anos anteriores a data da auditoria atual, aplicável somente a servidores que estejam em operação há, no mínimo, 3 anos.

4.8.4 Atualizações de segurança dos sistemas

Descrição
a) Verificar, através de amostra significativa das estações de trabalho, se estas estão configuradas para realizar atualizações automaticamente através do repositório do fabricante.
a) Verificar através da versão de sistema o estado de atualização de servidores. Adicionalmente, certificar de que nenhum servidor esteja configurado para atualizações automáticas.
a) Verificar, através das informações disponibilizadas pelo fabricante e o estado de atualização dos equipamentos se há novas atualizações com mais de 7 (sete) dias de publicação pelo próprio fabricante.

4.8.5 Software de antivírus

Descrição
a) Constatar para estações, através de amostra significativa do ambiente, e para servidores, todos, se possuem software antivírus instalado e configurado.
a) Verificar se existe bloqueio para a modificação de configurações do software antivírus através da tentativa de acesso com usuário atribuído com um perfil sem direitos administrativos.
a) Verificar, através da configuração do software antivírus, se está configurado para atualizar a base de infecções de forma automática e imediata à liberação pelo fabricante.

4.8.6 Avaliação de vulnerabilidades

Descrição
a) Requisitar os relatórios oriundos da última análise de vulnerabilidades realizada internamente. b) Verificar se todos os sistemas críticos estão contemplados. c) O último relatório deve ser datado, no máximo, de 6(seis) meses anteriores à auditoria atual.
a) Requisitar os relatórios oriundos da última análise de vulnerabilidades realizada por entidade externa. b) Verificar a credibilidade e independência da entidade externa contrata. c) O último relatório deve ser datado, no máximo, de 1(um) ano anterior à auditoria atual. d) Este relatório deve contemplar, no mínimo: • Uso de senhas impróprias; • Mapeamento de portas abertas e serviços ativos; • Análise de vulnerabilidades dos sistemas ativos; • Falhas de injeção, particularmente SQL injection; • Buffer overflow; • Comunicações inseguras; • Tratamento de erros inapropriado; • Cross-site scripting (XSS); • Controle de acesso inapropriado

4.8.7 Controles computacionais

Descrição
a) Requisitar política que conste a complexidade das senhas. Uma senha deve ser considerada complexa quando: • Possui 7(sete) caracteres ou mais; e • Mescla caracteres alfanuméricos com caracteres especiais; e • Caracteres em caixa alta e caixa baixa.

b) Verificar se estas regras estão implementadas nos sistemas de controle de dominio (*LDAP, Active Directory, etc*).
a) Verificar existem sistemas de controle de domínio implementados (*LDAP, Active Directory, etc*).
a) Verificar as políticas de senha configuradas. Estas devem atender os seguintes requisitos: • Devem ser redefinidas de forma automática a cada 180 dias; e • Não devem ser repetidas as três senhas anteriores.
a) Requisitar procedimento ou política que possua o processo de redefinição de senhas.
a) Requisitar o procedimento ou política de gerenciamento de usuários. Adicionalmente, verificar as políticas configuradas no sistema. A seguinte política deve estar definida: • Usuários inativos por mais de 60(sessenta) devem ser bloqueados;
a) Requisitar o procedimento ou política de gerenciamento de usuários. Adicionalmente, verificar as políticas configuradas no sistema. A seguinte política deve estar definida: • Usuários que digitem suas senhas de forma incorreta por 6 vezes devem ter sua conta bloqueada.
a) Requisitar o procedimento ou política de gerenciamento de usuários. Adicionalmente, verificar as políticas configuradas no sistema.
a) Verificar se os sistemas possuem o serviço ntp instalado e se os servidores corretos estão listados no arquivo de configuração. b) O serviço ntp nativo de servidores Windows a partir da versão 2000 server não deve ser considerada.

4.8.8 Disponibilidade do serviço

Descrição
a) Verificar a existência de redundância para sistemas críticos como, por exemplo, aplicações web e armazenamento.
a) Verificar a existência de site de contingência através de contratos, caso seja terceirizado. b) Caso o site de contingencia seja de propriedade da própria entidade, requisitar as configurações de sistemas e roteadores que permitem a troca de sites na ocorrência de eventos.
a) Constatar, através da configuração dos roteadores ou, também, através dos contratos com operadoras a implementação de enlaces redundantes

4.8.9 Armazenamento e salvaguarda dos dados

Descrição
a) Verificar as características de implementação dos dispositivos de armazenamento utilizados pela entidade.
a) Requisitar procedimento de cópias de segurança. Este procedimento deve incluir: • Passos para realização do backup; • Passos para verificação do backup; • Passos para armazenamento e controle do conteúdo dos backups; • Passos para recuperação do backup; • Periodicidade do backup; b) Periodicidade de teste de recuperação do conteúdo do backup.
a) Requisitar a declaração formal do processo de realização de testes de verificação de integridade. b) Requisitar a documentação das aplicações utilizadas para a verificação de integridade. c) Adicionalmente, verificar, através da restauração dos dados, se todos os atributos são mantidos, incluindo, principalmente, os atributos de permissão de acesso.
a) Requisitar declaração formal do processo de realização de cópias de segurança. b) Requisitar a apresentação do backup referente ao dia anterior.
a) Constatar, fisicamente, a utilização de cofres para as mídias de backup. b) Não devem existir mídias de backup em outros locais senão o cofre.
a) Requisitar declaração formal do processo de verificação das condições físicas das mídias de backup.
a) Requisitar declaração formal da existência de análise crítica do procedimento de restauração de backup.
a) Verificar a efetividade do controle de acesso ao cofre.
a) Requisitar 3(três) registros de cópias de segurança.

4.8.10 Privacidade

Descrição
a) Requisitar Acordo de confidencialidade utilizado pela entidade. Este termo deve contemplar: • Durabilidade de 5(cinco) anos após desligamento; • Penalidades quando da ocorrência de quebra de acordo.

4.8.11 Treinamento e conscientização

Descrição
a) Para todos os controles desta seção, requisitar a declaração formal acerca do treinamento e conscientização dos colaboradores.

4.9 Gestão das operações

4.9.1 Manual e política de segurança da informação

Descrição
a) Para todos os controles desta seção, requisitar uma cópia das seguintes políticas: • Política de segurança da informação; • Política de classificação da informação; • Política de uso da internet.

4.9.2 Definição e segregação de funções

Descrição
a) Requisitar cópia dos Acordos de utilização ou outro documento corresponde que descreva os papeis e funções dos colaboradores.

4.9.3 Gestão de ativos de TI

Descrição
a) Requisitar o inventário de ativos da informação seja este eletrônico ou em papel.
a) Requisitar registro de entrada e saída de equipamentos, dispositivos e mídias.

4.9.4 Gestão de usuários do sistema

Descrição
a) Requisitar procedimento de gestão de usuários contemplando: • Responsabilidades pela autorização, inclusão, remoção e alteração dos perfis. b) Requisitar formulário utilizado para a atribuição de acesso, contendo: • Sistemas e serviço cujo colaborador tem acesso; • Assinatura do responsável pela atribuição;

• Assinatura do usuário, reconhecendo suas responsabilidades e atribuições.
a) Requisitar termo de utilização.
a) Verificar, no controlador de domínio, se existe identificadores pessoais de usuário com privilégios administrativos.
a) Requisitar procedimentos de definição e redefinição de senhas.
a) Identificar na política de segurança se a entidade possui formalmente declarada a remoção de privilégios e identificadores de usuários de colaboradores quando do desligamento dos mesmos.
a) Identificar na política de segurança da informação se a redefinição de senhas administrativas de usuários compartilhados, equipamentos e sistemas que possibilitam a utilização de somente 1(um) usuário administrativo são trocadas quando do desligamento de um colaborador com privilégios administrativos.
a) Identificar, na política de segurança da informação, a declaração formal do principio do privilegio mínimo necessário. b) Requisitar a relação de privilégios formalmente documentada.
a) Identificar, na política de segurança da informação, a declaração foral da revisão de direitos de acesso de forma anual contemplando os requisitos necessários referidos neste controle.

4.9.5 Gestão de mudanças

Descrição
a) Identificar, na política de segurança ou política ou, também, procedimento para a gestão de mudanças, a declaração formal do processo de requisição, aprovação e documentação das mudanças significativas.
a) Requisitar procedimento para a gestão de mudanças. b) Caso exista, requisitar os templates para formulários que devem ser preenchidos quando do momento da requisição, aprovação e documentação da mudança.

4.9.6 Gestão de incidentes

Descrição
a) Identificar, na política de segurança da informação ou procedimento relacionado a gestão de incidentes, se esta formalmente declarada as responsabilidades para a conscientização dos colaboradores.
a) Requisitar procedimento de gestão de incidentes.

a) Requisitar procedimento de gestão de incidentes.
a) Requisitar procedimento de gestão de incidentes.
a) Requisitar procedimento de gestão de incidentes. b) Requisitar política de segurança da informação.

4.9.7 Gestão de riscos

Descrição
a) Identificar, na política de segurança da informação, se esta formalmente declarada a necessidade de avaliações de riscos periódicas. b) Requisitar o resultado da ultima a avaliação de riscos.
a) Requisitar o documento da política de segurança da informação ou documento equivalente que contenha o escopo das avaliações de riscos a serem realizadas.

4.9.8 Gestão de contratos com fornecedores

Descrição
a) Identificar, na política de segurança da informação, a existência de uma declaração formal acerca das necessidades para a formalização de contratos com terceiros.
a) Identificar, na política de segurança da informação, a existência de uma declaração formal acerca dos requisitos e gatilhos para a revisão de contratos; e b) Adicionalmente, requisitar um contrato recente, firmado com parceiro critico para a prestacao dos servi;os relacionados ao SREI e verificar a conformidade com todos os requisitos declarados neste controle.

4.9.9 Continuidade dos negócios

Descrição
a) Identificar, na política de segurança da informação ou documento com a mesma função, a declaração da necessidade e existência de um plano de continuidade dos negócios (PCN); O plano deve contemplar os seguintes tópicos: • Objetivos e estratégias organizacionais para a gestão da continuidade do negócio; • Definir responsabilidades pela coordenação das atividades de gestão da continuidade do negócio; • Identificar e priorizar os processos e ativos críticos para a continuidade das operações do SREI; • Identificar os recursos - financeiros, organizacionais,

tecnológicos, humanos, ambientais necessários para a gestão da continuidade do negócio; • Detalhar e documentar as atividades e procedimentos que compõem o plano de continuidade do negócio; b) Definir as modalidades para validação do plano, contemplando os testes a serem realizados, sua frequência e os recursos envolvidos;
a) Requisitar o plano de continuidade dos negócios (PCN) e verificar se este atende a todos os requisitos presentes neste controle. • Indisponibilidade da instalação predial, incluindo seus equipamentos e documentos armazenados; • Destruição da instalação predial, incluindo seus equipamentos e documentos armazenados; • Indisponibilidade dos enlaces de comunicação; • Indisponibilidade de pessoal.

4.9.10 Gerenciamento da capacidade

Descrição
a) Identificar, na política de segurança da informação ou documento de mesmo valor, a existência da declaração da necessidade da gestão de capacidade e os recursos analisados. Os recursos analisados devem ser, no mínimo: • Uso de CPU; • Uso de memória; • Uso de espaço de armazenamento persistente; • Uso dos enlaces da comunicação. b) A análise de recursos pode ser variável de acordo com as especificidades da aplicação e do hardware utilizado, portanto, caso seja necessário utilizar outras métricas ou, também, caso não seja necessário utilizar as métricas apresentadas acima, esta decisão deve ser justificada.
a) Requisitar resultados e relatórios para a gestão de capacidade.
a) Requisitar plano de ação para a gestão de capacidade, caso exista. Os seguintes itens devem ser considerados: • Planejamento das ações para melhora da capacidade futura, contendo a previsão (data) para a realização das ações; • Provisionamento de recursos financeiros para a melhora; • Resultados esperados das ações.

5 Coleta e guarda de evidências

O peso de uma evidência depende criticamente de sua integridade para proteger contra desafios jurídicos afirmando que a evidencia pode ter sido modificada ou adulterada do ponto inicial de coleta até o armazenamento e processamento e analise para a apresentação. A análise somente DEVE ser realizada em cópias primárias da evidência, obtida sob a supervisão de pessoal confiável. Detalhes de quando e onde o processo de cópia foi executado, quem executou e quais ferramentas e programas foram utilizados, tudo é registrado. Os requisitos para esta atividade são:

- **Documentos em papel:** o original é mantido seguro com o registro do individuo que encontrou o documento, onde o documento foi achado, quando foi achado e quem testemunhou a descoberta; qualquer análise faz o uso de cópias, mantendo a original armazenada seguramente;
- **Dados computacionais:** Imagens espelhadas ou cópias de qualquer mídia removível, informações em discos rígidos e em memórias coletadas; todas as ações durante o processo de coleta e cópia são registradas e o processo deve ser testemunhado; a mídia original e o registro ou (se isto não é possível), no mínimo, uma cópia de imagem deve ser armazenada seguramente.