SREI

Sistema de Registro Eletrônico Imobiliário

Parte 4 – Auditoria Operacional de TIC

B - Requisitos para o Ambiente Operacional de TI

Título	SREI Parte 4 B - Requisitos para o ambiente operacional de TIC
Versão	Versão 1.3 release 2
Data da liberação	30/05/2012
Classificação	Restrito
Autores	Matteo Nava, Volnys Bernal
Propriedade	CNJ
Restrições de acesso	LSI-TEC, CNJ e ARISP

Sumário

1 Introdução

Este documento descreve os **requisitos operacionais** que devem ser atendidos pelos Cartórios de Registro de Imóveis relacionados à infraestrutura física, tecnologia da informação e comunicação e gestão da segurança da informação para o Sistema de Registro Eletrônico Imobiliário (SREI)

Os requisitos descrevem os controles de segurança aplicados aos ambientes operacionais de tecnologia da informação e comunicação (TIC) para minimizar riscos em relação à integridade dos registros eletrônicos, à integridade do sistema, à disponibilidade dos dados e propiciar a continuidade das atividades, mesmo em situações catastróficas.

Os requisitos foram desenvolvidos utilizando como referencia as principais normas e padrões de segurança da informação, como a ISO 20.000 , ISO/IEC 27.000 [www.abnt.org.br], ITIL [http://www.itil-officialsite.com] e PCI [pt.pcisecuritystandards.org].

2 Visão geral da organização dos requisitos operacionais

Esta seção apresenta uma visão geral da forma de organização dos requisitos operacionais, abordando os seguintes tópicos:

- Entidades envolvidas na operação do SREI;
- Classificação dos requisitos;
- Obrigatoriedade do atendimento dos requisitos;
- Escopo de abrangência da auditoria operacional.

2.1 Entidades envolvidas na operação do SREI

A Figura 1 e a Figura 2 representam as formas de organização do ambiente operacional de um cartório.

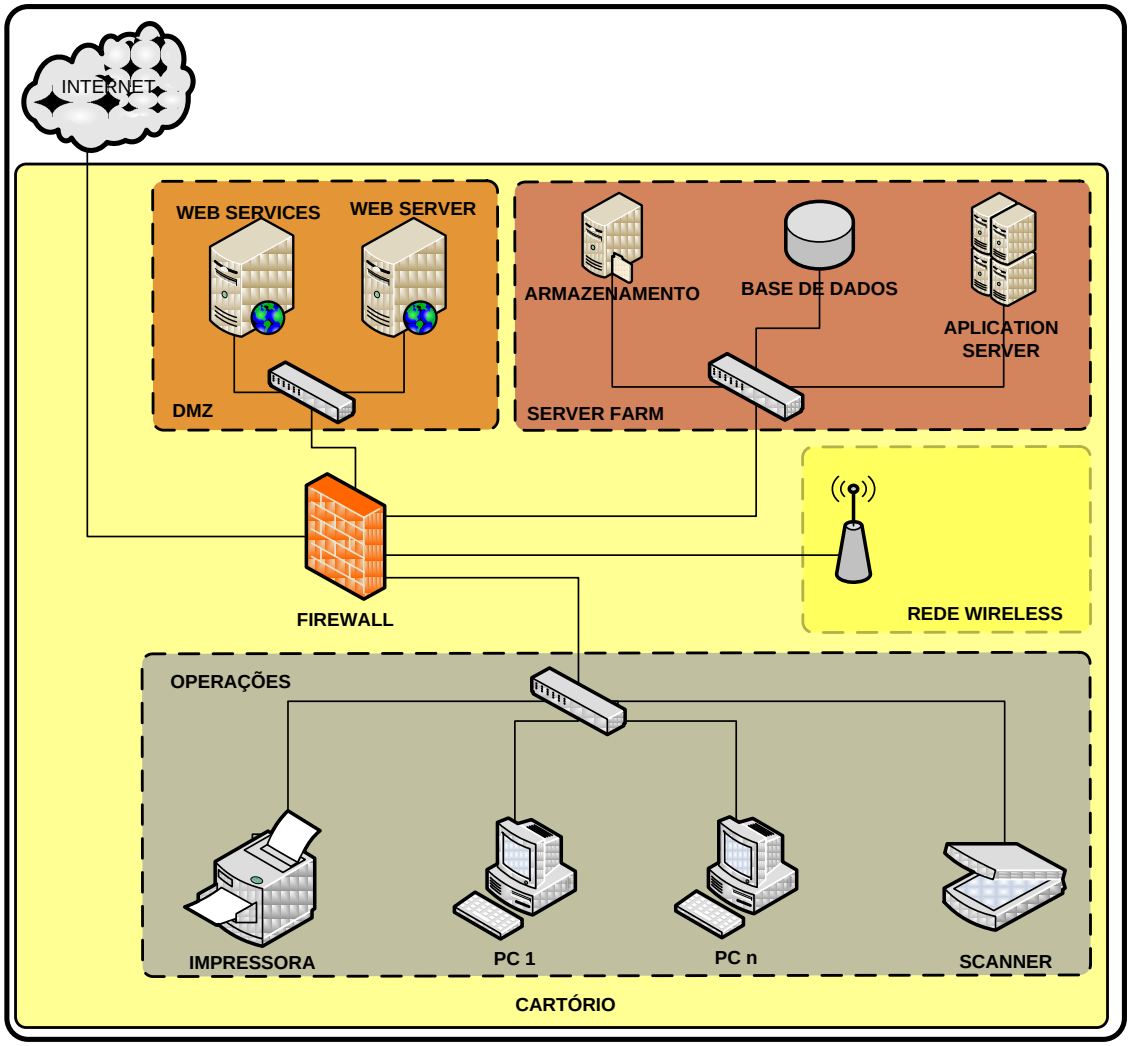

Figura 1 - Cenário com cartório hospedando todas as operações.

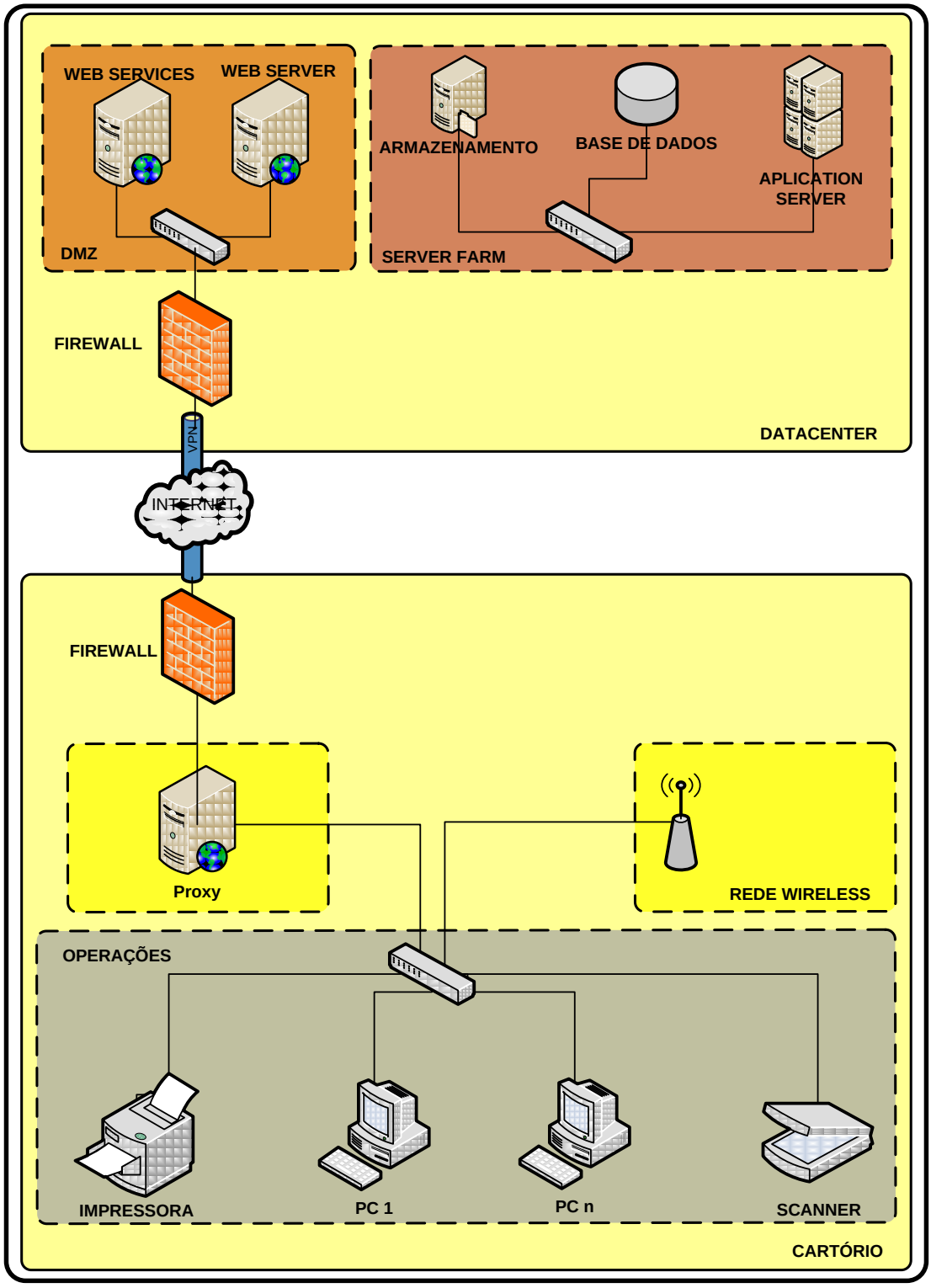

Figura 2 – Cenário com cartório fazendo uso de um provedor de serviço (datacenter) para hospedar parte das operações.

A obrigatoriedade do atendimento aos requisitos operacionais depende do tipo de entidade. As entidades relacionadas estão apresentadas no Quadro 1.

Quadro 1 – Classificação das entidades.

Código	Nome	Descrição
C	Cartório	Cartório de Registro de Imóveis
CR	Cartório com restrições	Cartório de Registro de Imóveis com restrições de recursos operacionais e de recursos financeiros
P	Provedor de serviço	Provedor de serviço contratado que abriga parte das operações do cartório.
S	SAEC	Serviço de Atendimento Eletrônico Compartilhado

2.2 Classificação dos requisitos

Os requisitos foram organizados em áreas e grupos de requisitos a fim de facilitar seu entendimento. O Quadro 2 apresenta esta organização.

Quadro 2 – Áreas e grupos de requisitos.

Área de requisitos	Grupo de requisitos
Infraestrutura física	Segurança física; Suprimento de energia elétrica; Monitoração por câmeras; Alarme contra intrusão; Prevenção contra incêndio; Ventilação e climatização; Cofre para mídias de backup; Outros controles de segurança de infraestrutura.
Segurança de TIC	Redes de comunicação de dados; Configuração segura de sistemas; Rastreabilidade de eventos; Atualizações de segurança dos sistemas;

	Software de antivírus; Avaliação de vulnerabilidades; Controles computacionais; Disponibilidade do serviço; Armazenamento e salvaguarda dos dados; Privacidade; Treinamento e conscientização.
Gestão das operações	Manual e política de segurança da informação; Definição e segregação de funções; Gestão de ativos de TI; Gestão de usuários do sistema; Gestão de mudanças; Gestão de incidentes. Gestão de riscos; Gestão de contratos com fornecedores; Continuidade dos negócios; Gerenciamento da capacidade.

2.3 Obrigatoriedade do atendimento dos requisitos

O Quadro 3 apresenta a classificação para indicar o nível de obrigatoriedade do atendimento de um determinado requisito operacional pela entidade.

Quadro 3 – Classificação da obrigatoriedade do atendimento dos requisitos.

	Obrigatoriedade do atendimento do requisito	**Descrição**
O	Obrigatório	O requisito deve atendido de forma integral
OC	Obrigatório condicional	O atendimento integral ao requisito é obrigatório somente quando for satisfeita uma determinada condição.
R	Recomendado	O atendimento integral ao requisito é facultativo, opcional, porém sendo fortemente recomendada sua adoção.
F	Facultativo	O atendimento ao requisito é opcional.
NA	Não se aplica	O requisito não se aplica a esta entidade.

2.4 Escopo de abrangência da auditoria operacional

O escopo de aplicabilidade dos requisitos de auditoria operacional é definido pelos **componentes do sistema** e pelo **ambiente de dados do cartório** conforme os seguintes critérios:

- Devem ser considerados como **componentes de sistema** qualquer componente de rede, servidor ou aplicação que esteja incluso ou conectado ao ambiente que opera com dados de cartório. Também estão incluídos componentes virtualizados como máquinas, roteadores, switchs, appliances, aplicações e estações virtuais.
- O **ambiente de dados do cartório** é composto por pessoas, processos e tecnologias que armazenam, processam e transmitem dados de cartório ou dados sensíveis.
- Os limites do **ambiente de dados de cartório** são definidos por meio de segmentação de rede ou isolamento. Sem a segmentação do ambiente de dados de cartório, toda a rede deve ser contemplada no escopo para o processo de auditoria operacional.
- Caso haja uma entidade de terceira parte envolvida no armazenamento, processamento ou transmissão de dados de cartório os requisitos definidos no presente documento se estendem também a esta entidade.

3 Requisitos operacionais

Esta seção apresenta a relação de requisitos operacionais que devem ser implementados pelas entidades envolvidas no Sistema de Registro Eletrônico Imobiliário (SREI).

Os requisitos operacionais foram divididos nas seguintes áreas:

- Infraestrutura;
- Segurança de TIC;
- Gestão das operações.

3.1 Infraestrutura

Os requisitos definidos a seguir se aplicam a todas as instalações prediais utilizadas no processamento e armazenamento de informações do SREI. Os requisitos estão organizados nos seguintes tópicos:

- Segurança física;
- Suprimento de energia elétrica;
- Monitoração por câmeras;
- Alarme contra intrusão;
- Prevenção contra incêndio;
- Ventilação e climatização;
- Cofre para mídias de backup;
- Outros controles de segurança de infraestrutura.

3.1.1 Segurança física

Os controles de segurança física têm como objetivo minimizar ou mitigar por completo os riscos inerentes ao ambiente físico. Por ambiente físico, para o escopo destes controles, deve-se considerar todo o imóvel de propriedade do cartório ou terceiro, delimitado às áreas que operem com danos do cartório ou tenha influencia direta ou indireta em sua operação, cujos riscos de danos por causas naturais ou de natureza humana possa oferecer riscos à segurança da informação.

Ref	Requisito	Descrição	C	CR	P	S
1.1.1	Níveis de segurança física	O ambiente físico do cartório DEVE ser dividido em áreas físicas claramente delimitadas e associadas a níveis de segurança física. Os níveis de segurança física DEVEM possuir suas áreas aninhadas. Exceto para o nível 1, o acesso de um indivíduo a um determinado nível (“N”) DEVE ser precedido do acesso ao nível anterior (“N-1”). O ambiente deve possuir, no mínimo, três níveis de segurança física: • Nível 1 - Atendimento: área de circulação de clientes e de atendimento aos clientes dos cartórios; • Nível 2: - Operação: área na qual são realizadas as atividades operacionais do cartório; • Nível 3 – Sensível: área crítica (ex. CPD) que abriga os equipamentos sensíveis do SREI e os sistemas de segurança (CFTV, sistema de controle de acesso e central de alarmes); Estes perímetros devem ser delimitados por barreiras físicas (ex: paredes, divisórias, grades, catracas, portas, etc). A definição destes perímetros deve ser documentada e constar na política de segurança da informação.	O	O	O	O

1.1.2	Área de segurança física nível 2	A área de segurança física nível 2 (operação) do cartório DEVE atender, no mínimo, aos seguintes requisitos de segurança física: a) O acesso de pessoas ao nível 2 DEVE ser restrito por uma porta com tranca; b) O acesso DEVE ser restrito aos colaboradores do cartório; c) O acesso de visitantes DEVE ser precedido de autorização de acesso concedida por um colaborador com direito de acesso; d) A conexão de equipamentos de terceiros (computadores, notebooks, smartfones, tokens, discos, etc) na rede ou nos sistemas de TIC do cartório DEVE ser precedida de autorização e inspeção e o seu uso DEVE ser supervisionado.	O	R	O	O
1.1.3	Área de segurança física nível 3	A área de segurança física nível 3 (sensível) do cartório DEVE atender, no mínimo, aos seguintes requisitos de segurança física: a) O nível 3 DEVE abrigar áreas sensíveis de operação do cartório como, por exemplo, o Centro de Processamento de Dados (CPD); b) A segregação física da área de nível 3 DEVE ser realizada por paredes de alvenaria ou material de igual ou maior resistência e portas e janelas com tranca. O uso de rack com portas com tranca é admitido como área de nível 3; c) O controle de acesso à área de nível 3 DEVE ser realizado através de porta com tranca. A tranca DEVE ser de acionamento manual (tipo chave) ou de acionamento eletrônico (cartão de acesso, biometria, etc); d) Somente os colaboradores com necessidade específica de acesso ao nível 3 DEVEM ter autorização de acesso à área. Pessoas que não possuam permissão de acesso (serviços de manutenção, limpeza, etc) PODEM permanecer somente quando estiverem acompanhadas por colaborador autorizado; e) Equipamentos de gravação, fotografia, vídeo, som ou similares, computadores portáteis e mídias de armazenamento removíveis DEVEM possuir sua entrada controlada e somente DEVEM ser utilizados mediante autorização, supervisão e inspeção.	O	O	O	O
1.1.4	Segregação dos equipamentos de	Os equipamentos de TIC DEVEM ser segregados dos equipamentos de segurança (controle	R	R	O	O

	segurança	de acesso, alarme, CFTV, etc) em áreas distintas de nível 3 de segurança.				

3.1.2 Suprimento de energia elétrica

O suprimento contínuo e constante de energia elétrica deve ser garantido para os ambientes que operam com dados do cartório. O principal objetivo deste controle é, sobretudo, a garantia da disponibilidade e integridade dos serviços e dos componentes relacionados.

Ref	Requisito	Descrição	C	CR	P	S
1.2.1	Proteção contra variações no fornecimento de energia elétrica	Os equipamentos críticos (servidores e equipamentos de rede) situados no ambiente nível 3 DEVEM ser protegidos contra falta ou instabilidade do fornecimento de energia elétrica por meio da utilização de equipamento com a característica de *no-break*. Demais equipamentos DEVEM ser protegidos por estabilizadores de energia.	O	R	O	O
1.2.2	Disponbilidade de suprimento de energia elétrica	DEVE ser garantido o fornecimento de energia elétrica para o ambiente operacional ou parte dele por meio do uso de geradores: a) DEVE haver gerador para o suprimento auxiliar de energia elétrica para os equipamentos críticos quando da ocorrência de interrupções no seu fornecimento; b) O gerador DEVE suportar tais equipamentos com um nível de carga inferior a 50%; c) Manutenção e testes DEVEM ocorrer periodicamente.Relatórios de conformidade devem ser gerados a cada período de manutenção e teste; d) O sistema gerador e o combustível utilizado DEVEM ser mantidos em local seguro e externo ao ambiente do cartório.	F	F	R	O

3.1.3 Monitoração por câmeras

A monitoração por câmeras deve permitir, acima de tudo, a visualização e possível identificação de indivíduos presentes ou, sob qualquer forma, envolvidos quando da ocorrência de eventos de segurança da informação.

Ref	Requisito	Descrição	C	CR	P	S
1.3.1	Monitoração por câmeras (CFTV)	O ambiente DEVE ser monitorado por Circuito Fechado de Televisão (CFTV). O sistema de CFTV DEVE: • 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.	O	R	O	O
1.3.2	Preservação das imagens	As imagens geradas pelas câmeras DEVEM ser preservadas por, no mínimo, 90 dias.	O	R	O	O
1.3.3	Posicionamento das câmeras	O posicionamento das câmeras DEVE incluir, no mínimo: • O ambiente de nível 1; • Os pontos de acesso à área de nível 2 e à área de nível 3, de forma a possibilitar o reconhecimento facial dos indivíduos que realizam o acesso; • O ambiente de nível 3.	O	R	O	O

3.1.4 Alarme contra intrusão

Os alarmes contra intrusão atuam como complemento às barreiras físicas e ao monitoramento pessoal dos ambientes que operam com dados de cartório. Porém, este controle age impreterivelmente quando da ausência de colaboradores no ambiente, tornando possível, adicionalmente à monitoração por câmeras, a vigilância local durante os períodos de ausência de colaboradores.

Ref	Requisito	Descrição	C	CR	P	S
1.4.1	Alarme contra intrusão	Sistemas de alarmes contra intrusão DEVEM ser utilizados a fim de alertar o rompimento de barreiras do perímetro de segurança.	O	R	O	O
1.4.2	Ativação de alarme contra intrusão	Alarmes de detecção de presença de pessoas DEVEM ser ativados quando a área não estiver ocupada.	O	R	O	O

3.1.5 Prevenção contra incêndio

Devem ser adotadas medidas de prevenção e controle de incêndios para garantir a disponibilidade e integridade dos sistemas e componentes que os viabilizam. Deve ser considerada a segurança contra incêndio dos componentes de sistemas como, por exemplo, software, hardware (estações de trabalho, servidores diversos, etc), dispositivos de armazenamento (CDs, DVDs, fitas de cópias de segurança e similares), documentos impressos e, principalmente, recurso humano.

Ref	Requisito	Descrição	C	CR	P	S
1.5.1	Combate a incêndio	O ambiente DEVE possuir sistema de combate a incêndio adequado às suas instalações físicas.	O	O	O	O
1.5.2	Detector de	O ambiente DEVE possuir detector de fumaça em suas instalações.	R	F	O	O

	fumaça					
1.5.3	Alarme de incêndio	O ambiente DEVE possuir alarme de incêndio em suas instalações físicas.	R	F	O	O

3.1.6 Ventilação e climatização

Medidas para a renovação, circulação e climatização de ar devem ser implementadas para garantir a operacionalização correta das atividades.

Ref	Requisito	Descrição	C	CR	P	S
1.6.1	Ventilação	O local de operação DEVE possuir ventilação adequada às atividades desempenhadas.	O	R	O	O
1.6.2	Climatização	A área de nível 3 DEVE possuir sistema de ar-condicionado redundante, dimensionado de forma a manter a temperatura adequada mesmo na ocorrência de falha em um dos equipamentos.	R	F	O	O

3.1.7 Cofre para mídias de backup

As mídias de cópias de segurança são o objeto principal para a continuidade dos negócios de um cartório. Portanto, a sua integridade deve ser garantida por tempo indeterminado contra eventos de origem humana ou naturais como, por exemplo, intrusão, incêndios, inudanções, danos estruturais do ambiente, etc.

1.7.1	Cofre para mídias de backup	DEVE existir um cofre para possibilitar o armazenamento das mídias de backup. O cofre DEVE atender 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	O	O	O	O

		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. Caso algum destes requisitos não seja atendido: • O cofre para mídias de backup DEVE ser estanque contra agua; • DEVEM existir controles preventivos ou compensatórios adequados para o risco de inundação.				

3.1.8 Outros controles de segurança de infraestrutura

Outros controles, além daqueles dispostos anteriormente, devem ser considerados para a segurança da estrutura predial e dos componentes de infraestrutura e comunicação de dados.

Ref	Requisito	Descrição	C	CR	P	S
1.7.2	Resistência contra inundação	O local que abriga os servidores e sistemas de armazenamento do SREI DEVE estar localizado a, no mínimo, • 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 agua da chuva.	O	O	O	O
1.7.3	Segurança dos armários de	Todos os armários existentes nas instalações físicas do cartório que abrigam componentes do sistema de comunicação de dados e telefonia DEVEM ser protegidos contra acesso não	R	F	O	O

	comunicação	autorizado.				
1.7.4	Proteção contra raios	A infraestrutura predial que abriga o cartório DEVE possuir sistema de proteção contra raios que seja homologado.	R	F	O	O

3.2 Segurança de tecnologia de informação e comunicação (TIC)

Os requisitos de segurança de tecnologia de informação e comunicação (TIC) estão organizados nos seguintes tópicos:

- Redes de comunicação de dados;
- Configuração segura de sistemas;
- Rastreabilidade de eventos;
- Atualizações de segurança dos sistemas;
- Software de antivírus;
- Avaliação de vulnerabilidades;
- Controles computacionais;
- Disponibilidade do serviço;
- Armazenamento e salvaguarda dos dados;
- Privacidade;
- Treinamento e conscientização.

3.2.1 Redes de comunicação de dados

Os requisitos têm como objetivo principal garantir que a infraestrutura de rede do SREI seja claramente definida e controlada a fim de permitir a plena disponibilidade e segurança dos serviços e dos dados que utilizam esta infraestrutura.

A Figura 2 representa de forma esquemática uma topologia genérica de rede para as entidades, representando os principais sistemas de processamento, de proteção e, também, evidenciando as segregações mínimas que devem existir.

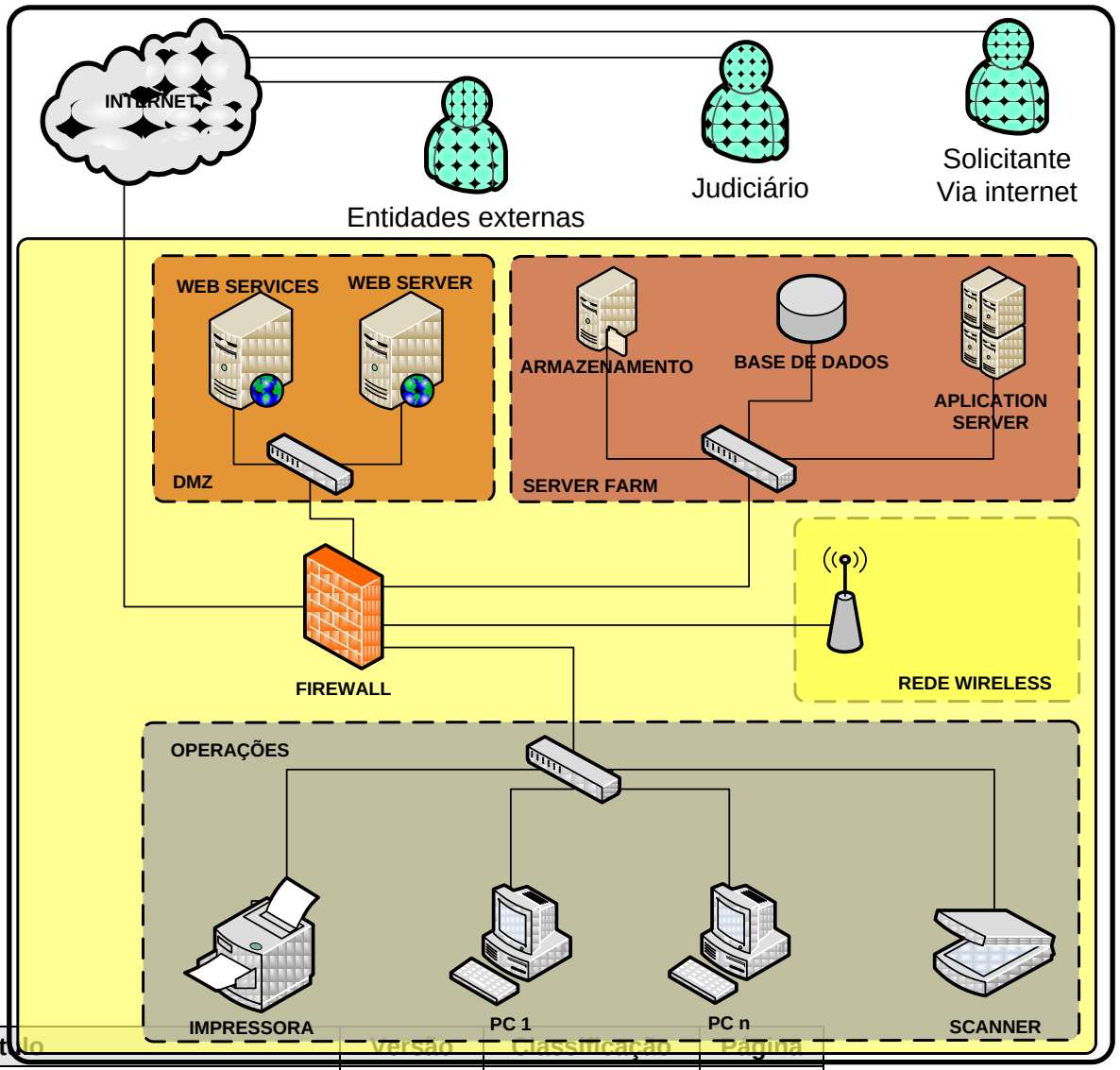
INTERNET
Entidades externas
Judiciário
Solicitante
Via internet
WEB SERVICES
WEB SERVER
DMZ
ARMAZENAMENTO
BASE DE DADOS
APLICATION SERVER
SERVER FARM
FIREWALL
REDE WIRELESS
OPERAÇÕES
IMPRESSORA
PC 1
PC n
SCANNER

Figura 3 – Exemplo de topologia de rede para a Entidade.

A seguir são relacionados os requisitos operacionais relacionados à rede de dados que devem ser atendidos pelas entidades.

Ref	Requisito	Descrição	C	CR	P	S
2.1.1	Documentação da rede	O cartório DEVE manter documentação sobre a infraestrutura de rede de comunicação de dados. A documentação DEVE incluir: a) Topologia física da rede e equipamentos de comunicação (roteador, *switch, firewall, modens, access point* de redes *wireless*, etc); b) Topologia lógica da rede, informando as subredes e as tabelas de roteamento; c) A relação de equipamentos (servidor, desktop, roteador, switch, etc) e suas configurações de rede; d) A relação dos sistemas em cada servidor.	O	R	O	O
2.1.2	Identificação dos equipamentos e dispositivos	Cada equipamento e dispositivo DEVE possuir uma identificação única com o objetivo de possibilitar a gestão do ambiente computacional (atualizações, notificação e correção de falhas, notificação de incidentes, etc.) e, também, a geração das trilhas de auditoria.	R	F	O	O
2.1.3	Segregação das redes	A topologia de rede DEVE, no mínimo, segregar as seguintes redes: • Rede DMZ: servidores que fornecem serviços à entidades externas via Internet, como servidor WEB, servidor SMTP, servidor DNS, proxy HTML, etc. (obrigatório); • Rede de servidores: servidores internos críticos do SREI (obrigatório); • Rede de operação: desktops de operação (obrigatório); • Rede para clientes: desktops disponibilizados aos usuários (caso exista); • Rede sem fio: pontos de acesso disponibilizado aos usuários (caso exista); As segregações de rede PODEM ser de ordem física, utilizando equipamentos de rede dedicados ou de ordem lógica por meio de configuração de VLANs nos equipamentos de	O	O	O	O

		rede. NÃO DEVE haver armazenamento de dados do SREI em computadores presentes nas redes expostas, como a DMZ e a rede para clientes.				
2.1.4	Proteção de perímetro das redes	Roteadores ou firewalls DEVEM ser utilizados bloquear acessos não autorizados. DEVE ser habilitado acesso somente a protocolos e serviços conhecidos e, quando possível, para entidades confiáveis. Cada regra de firewall e roteador DEVE ser claramente documentada, justificando o motivo de cada liberação de acesso. As regras de firewalls e roteadores DEVEM ser revisadas criticamente a cada ano.	O	O	O	O
2.1.5	Alterações da configuração	As alterações realizadas nas configurações de rede DEVEM ser documentadas. Todo o processo de alteração de configuração DEVE ser gerenciado conforme o requisito sobre gestão de mudanças. Toda alteração de configuração que esteja relacionada a serviços oferecidos a entidades externas ou regras de firewall DEVE passar por um teste de vulnerabilidades e o resultado formalmente documentado.	R	F	O	O
2.1.6	Redes sem fio	Caso presente, a rede sem fio DEVE estar segregada das demais redes. O acesso da rede sem fio às demais redes DEVE ser controlado por sistema de filtragem, com o objetivo de limitar o acesso às redes internas do cartório (rede de servidores e rede de operação); As configurações padrão dos fabricantes de equipamentos de redes sem fio DEVEM ser trocadas, incluindo senhas e chaves criptográficas; Para a criptografia da autenticação e transmissão, DEVEM ser utilizados protocolos robustos como, por exemplo, o protocolo IEEE 802.11i (WPA2) ou integrado com protocolo de autenticação 802.1x. As chaves DEVEM ser de conhecimento somente dos responsáveis e de quem necessita saber por necessidade do negócio. Quando do desligamento de um colaborador que tenha	O	O	O	O

		conhecimento das chaves, estas chaves DEVEM ser trocadas imediatamente.				
2.1.7	Comunicação entre sites	A comunicação de dados entre sites do SREI (sites de redundância, de réplica de dados, etc) DEVE ser realizada através de VPN ou link de comunicação dedicada segura.	O	R	O	O
2.1.8	Ambiente de testes e homologação	DEVE possuir um ambiente segregado para teste e homologação do sistema.	R	F	O	O

3.2.2 Configuração segura de sistemas

A configuração segura de sistemas (também denominada de *hardening*) é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas em sistemas computacionais (sistema operacional, roteador, servidor WEB, etc). O resultado é a aplicação de medidas e ações que visam proteger um determinado sistema contra acesso e uso não autorizado.

Ref	Requisito	Descrição	C	CR	P	S
2.2.1	Hardening dos sistemas	As configurações padrão dos sistemas (sistema operacional, equipamentos, servidor WEB, sistema de gerenciamento de banco de dados - SGBD, etc) DEVEM ser alteradas de forma a mitigar os riscos existentes. • 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	O	O	O	O

		exemplo, SSH, VPN, ou SSL/TLS; • Habilitação de controles de senhas seguras e uso de hash para codificação de senhas armazenadas. • Etc.				

3.2.3 Rastreabilidade de eventos

A rastreabilidade dos eventos tem como objetivo permitir a reconstrução dos eventos que ocorreram ambiente operacional.

A rastreabilidade dos eventos que ocorreram no sistema é possível através da geração e retenção de registros adequados de eventos (logs).

Ref	Requisito	Descrição	C	CR	P	S
2.3.1	Geração de registros - rede de dados	Caso algum equipamento de rede realize tradução dinâmica de endereços (NAT – *Network Address Translation*): • O equipamento DEVE gerar registros NAT relativos às conexões TCP e datagramas UDP traduzidas. Apesar da quantidade de registros gerada, principalmente decorrente da geração de registros UDP, tais registros são fundamentais para possibilitar a identificação da origem da sessão de comunicação no caso de eventos anômalos.	OC	RC	OC	OC
2.3.2	Geração de registros - sistemas	A geração dos seguintes eventos DEVE estar habilitada nos sistemas: • 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);	O	R	O	O

		• Ações de cada usuário; • Atividades relevantes dos sistemas.				
2.3.3	Concentrador de registros	DEVE ser mantido um servidor de registros (*logs*) de eventos com a finalidade de minimizar riscos em relação à integridade desta informação e, também, facilitar sua preservação.	R	F	O	O
2.3.4	Preservação dos registros de eventos	Os registros de eventos DEVEM ser preservados por, no mínimo, três anos.	O	R	O	O

3.2.4 Atualizações de segurança dos sistemas

Todos os componentes de sistema, cujo fabricante ou desenvolvedor disponibilize pacotes de atualização de segurança ou correções pontuais, devem ser atualizados de acordo com os controles abaixo descritos.

Ref	Requisito	Descrição	C	CR	P	S
2.4.1	Atualização de segurança das estações de trabalho	As atualizações de segurança das estações de trabalho DEVEM ser realizadas de forma automática com todas as atualizações publicadas pelos fabricantes.	O	O	O	O
2.4.2	Atualização de segurança dos servidores	As atualizações de segurança dos servidores e demais equipamentos DEVEM ser realizadas de forma manual. A atualização DEVE ser realizada por técnico qualificado. A atualização DEVE ser realizada em ambiente de teste. Caso não ocorra problemas, DEVE ser aplicada no ambiente de produção.	O	R	O	O

		Caso a entidade não possua um ambiente de teste, a aplicação da atualização DEVE ser realizada no ambiente de produção de tal forma que possa ser recuperado o estado anterior caso ocorram problemas decorrentes da atualização (*rollback)*.				
2.4.3	Periodicidade da atualização de segurança nos servidores	A verificação de existência de atualizações de segurança DEVE ser realizada, no máximo, a cada sete dias.	R	R	O	O

3.2.5 Software de antivírus

Os servidores e estações de trabalho devem possuir software antivírus instalado e atualizado para evitar infecções por códigos maliciosos. Determinados códigos maliciosos podem, sobretudo, causar danos à integridade dos dados de cartório e, em determinadas situações, facilitar intrusão por pessoas não autorizadas ou causar danos maiores a todo o sistema.

Ref	Requisito	Descrição	C	CR	P	S
2.5.1	Instalação de antivírus	Todos os servidores e estações de trabalho DEVEM possuir software antivírus instalado.	O	O	O	O
2.5.2	Proteção contra modificação das configurações do antivírus	O acesso e modificação das configurações do software antivírus DEVE ser limitado aos administradores responsáveis em todas as estações e servidores. Usuários NÃO DEVEM possuir privilégio de modificação das configurações do software de antivírus.	O	R	O	O
2.5.3	Atualização da base de dados do	A atualização da base de infecções deve ser atualizada de forma automática por um servidor central.	R	F	O	O

	antivírus	Este servidor deve atualizar com o repositório central do fabricante assim que as atualizações forem disponibilizadas.				
2.5.4						

3.2.6 Avaliação de vulnerabilidades

Vulnerabilidades podem estar presentes em componentes de sistemas, sendo estas inerentes às versões utilizadas ou criadas a partir de modificações nos sistemas agravando riscos de intrusões, falhas ou infecções por códigos maliciosos. Estes riscos devem ser mitigados ou, caso inviável, reduzidos perante análise interna e externa de vulnerabilidades.

Ref	Requisito	Descrição	C	CR	P	S
2.6.1	Avaliação de vulnerabilidades pela própria entidade.	Avaliações de vulnerabilidades para os sistemas expostos a Internet DEVEM ser realizadas periodicamente pela entidade, no mínimo, a cada seis meses.	R	F	O	O
2.6.2	Avaliação de vulnerabilidades por entidade externa	Avaliações de vulnerabilidades para os sistemas expostos a Internet DEVEM ser realizadas anualmente por uma entidade externa independente. As avaliações de vulnerabilidades DEVEM contemplar, no mínimo, os seguintes tópicos: • 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;	O	R	O	O

		• Tratamento de erros inapropriado; • Cross-site scripting (XSS); • Controle de acesso inapropriado.				

3.2.7 Controles computacionais

Os controles computacionais consistem em medidas para a redução ou mitigação de riscos referentes à utilização inadequada dos componentes de sistemas.

Ref	Requisito	Descrição	C	CR	P	S
2.7.1	Qualidade das senhas	O cartório DEVE definir uma política de qualidade de senhas. As senhas utilizadas pelos colaboradores DEVEM ser de difícil adivinhação e não devem fazer nenhuma referência aos dados pessoais dos colaboradores, como datas de nascimento ou nomes. Quando possível, DEVEM ser utilizadas facilidades do sistema para forçar a utilização das diretrizes de qualidades de senhas por parte dos usuários.	O	O	O	O
2.7.2	Base única de usuários e senhas	Sempre que possível, DEVE ser utilizada uma mesma base de usuários e senhas para os diversos sistemas do cartório.	R	F	O	O
2.7.3	Troca das senhas	A troca de senhas DEVE ser forçada a cada 180 dias de forma automatizada, não podendo repetir, no mínimo, as três senhas anteriores.	O	O	O	O
2.7.4	Redefinição da senha	O responsável pela redefinição (*reset*) da senha de um usuário (devido ao bloqueio da senha ou de seu esquecimento) DEVE ser realizar o processo de *reset*somente após identificação precisa do usuário, impedindo que a redefinição da senha seja requisita por terceiros.	O	O	O	O

2.7.5	Bloqueio de usuário por inatividade	Usuários inativos a mais de 60 dias DEVEM ter seu identificador de usuário bloqueado.	O	O	O	O
2.7.6	Bloqueio de usuário por erro da senha	Usuários que errarem a senha por 6 vezes DEVEM ser bloqueados.	O	O	O	O
2.7.7	Bloqueio de tela	Os usuários DEVEM ser conscientizados a bloquear a tela quando se ausentarem do computador.	O	O	O	O
2.7.8	Bloqueio automático de tela	Após o período de 5 minutos de inatividade as telas das estações de trabalho e servidores DEVEM ser bloqueadas com desbloqueio dependente de senha.	O	O	O	O
2.7.9	Sincronização do relógio	Os relógios dos sistemas DEVEM estar sincronizados através de um protocolo de sincronização de tempo (como, por exemplo, NTP ou SNTP). O sistema de referência para tempo DEVE ser um servidor confiável de tempo, tal como o serviço fornecido pelo ntp.br.	O	O	O	O
2.7.10						

3.2.8 Disponibilidade do serviço

Os controles para a disponibilidade dos serviços consistem na implementação de medidas para a redução do risco de indisponibilidade, ou seja, da paralisação parcial ou completa da prestação de serviços e da comunicação entre sites.

Ref	Requisito	Descrição	C	CR	P	S
2.8.1						

2.8.2	Servidor redundante	A entidade DEVE manter redundância dos sistemas para assegurar a disponibilidade do serviço no caso de falha de componentes.	R	F	R	O
2.8.3	Sistema redundante em instalação predial distinta	A redundância dos sistemas DEVE ocorrer em uma instalação predial distinta (site backup), externa e distante.	R	F	R	O
2.8.4	Enlaces redundantes	A entidade DEVE manter redundância dos enlaces de comunicação para assegurar a disponibilidade do serviço no caso de falha de componentes.	R	F	O	O

3.2.9 Armazenamento e salvaguarda dos dados

Estes controles contemplam a segurança do armazenamento e o mantenimento das formas utilizadas para as cópias de segurança, visando a integridade e disponibilidade destes dados.

Ref	Requisito	Descrição	C	CR	P	S
2.9.1	Armazenamento com discos redundantes	O armazenamento dos dados críticos, que incluem os registros eletrônicos, DEVE ser realizada em sistemas de discos redundantes (por exemplo, RAID 1 ou RAID 5).	O	O	O	O
2.9.2	Procedimento de backup	A entidade DEVE possuir um procedimento de backup. O procedimento de backup DEVE incluir, no mínimo: • 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;	O	O	O	O

		• Periodicidade de teste de recuperação do conteúdo do backup.				
2.9.3	Backup de dados	A entidade DEVE realizar backup de dados críticos diariamente. O resultado do backup DEVE ser testado no momento da realização do backup.	O	O	O	O
2.9.4	Armazenamento local das mídias de backup	A entidade DEVE armazenar as mídias de backup localmente em cofre apropriado para este fim.	O	O	O	O
2.9.5	Armazenamento externo das mídias de backup	A entidade DEVE armazenar as mídia de backup em local externo, em cofre apropriado para este fim.	O	O	O	O
2.9.6	Teste das mídias de backup	Periodicamente DEVEM ser realizados testes nas mídias de backup.	O	O	O	O
2.9.7	Teste do procedimento de recuperação dos dados	Periodicamente DEVE ser testado o procedimento de recuperação dos dados	O	O	O	O
2.9.8	Controle de acesso ao backup dos dados.	O acesso às mídias de backup DEVE ser restrito às pessoas autorizadas. DEVEM existir controles adequados que permitam que somente as pessoas autorizadas tenham acesso ao backup dos dados.	O	O	O	O
2.9.9	Controle sobre o backup de dados	A entidade DEVE manter registros que possibilite identificar os dados presentes no backup.	O	O	O	O
2.9.10	Cópias de segurança realizadas remotamente	Quando cópias de segurança forem realizadas ou trafegar pela Internet, deve ser garantido que toda a comunicação seja criptografada e que somente os colaboradores e parceiros autorizados tenham conhecimento da chave criptográfica.	O	O	O	O

2.9.11	Segurança das cópias de segurança	• A integridade das cópias de segurança deve ser garantida através da implementação de ferramentas de monitoramento de integridade ou de detecção de modificações para alertar os colaboradores responsáveis quando da tentativa de qualquer modificação ou cópia não autorizada. • A confidencialidade das informações deve ser garantida por meio de criptografia dos dados armazenados.				

3.2.10 Privacidade

Os dados do SREI possuem informações críticas relacionadas à privacidade das pessoas, como, por exemplo, endereço, estado civil, bens de direito que possui e valores destes bens de direito. Apesar da obrigatoriedade de acesso público destas informações, este acesso deve ser controlado a fim de garantir a privacidade dos dados das pessoas.

Os dados dos colaboradores também são informações que devem ser tratadas de forma a garantir a privacidade das informações.

Ref	Requisito	Descrição	C	CR	P	S
2.10.1	Privacidade dos dados do SREI	A entidade DEVE possuir controles de forma a controlar o acesso e divulgação de dados sensíveis que envolvam a privacidade das pessoas. Os controles DEVEM abranger os processos, procedimentos e tecnologia utilizada. DEVE abranger os sistemas computacionais, os dados armazenados e os dados de backup.	O	O	O	O

3.2.11 Treinamento e conscientização

Para o desenvolvimento seguro das atividades do cartório em conformidade com os requisitos dispostos neste documento é necessário que todos os colaboradores que necessitem operar sistemas ou qualquer um de seus componentes relacionados às atividades do cartório sejam adequadamente conscientizados e treinados para tal.

Ref	Requisito	Descrição	C	CR	P	S
2.11.1	Treinamento e conscientização	O colaborador que necessita utilizar os recursos do ambiente computacional e, principalmente, sistemas críticos de negócio, DEVEM ser treinados e conscientizados sobre: • As políticas de segurança da informação; • Os procedimentos operacionais adotados pelo cartório; • O uso dos sistemas computacionais.	O	R	O	O
2.11.2	Treinamento na mudança de função	O colaborador, quando da mudança de função ou cargo, DEVE ser novamente treinado e conscientizado sobre suas novas atividades.	O	R	O	O
2.11.3	Novos sistemas	O colaborador DEVE ser conscientizado quando às mudanças e novas aquisições de sistemas e recursos de processamento da informação.	O	R	O	O

3.3 Gestão das operações

Os requisitos de gestão das operações estão organizados nos seguintes tópicos:

- Manual e política de segurança da informação;

- Definição e segregação de funções;
- Gestão de ativos de TI;
- Gestão de usuários do sistema;
- Gestão de mudanças;
- Gestão de incidentes;
- Gestão de riscos;
- Gestão de contratos com fornecedores;
- Continuidade dos negócios;
- Gerenciamento da capacidade.

3.3.1 Manual e política de segurança da informação

As políticas de segurança da informação contemplam as boas práticas que devem ser seguidas dentro do ambiente que opera com os dados do cartório e durante o desempenho de quaisquer atividades relacionadas. Estas políticas devem ser de conhecimento dos colaboradores e de qualquer prestador de serviço ou terceiro que necessite acessar ou manipular os dados de cartório ou, também, preste serviço que possa influenciar diretamente o ambiente de dados de cartório. As políticas devem ser atualizadas a intervalos regulares e refletir o ambiente atual.

Ref	Requisito	Descrição	C	CR	P	S
3.1.1	Política de segurança da	O cartório DEVE possuir uma política de segurança da informação formalmente estabelecida que contemple todos os requisitos aplicáveis especificados na normal NBR ISO 27001. Os	R	F	O	O

	informação	requisitos não aplicáveis devem ser claramente justificados e documentados				
3.1.2	Requisitos obrigatórios do SREI	A política de segurança DEVE, também, contemplar tópicos associados aos requisitos que a entidade deve atender de forma obrigatória, relacionados neste documento.	R	F	O	O
3.1.3	Política de classificação da informação	A política de classificação da informação deve declarar os critérios e rótulos para a definição da criticidade das informações processadas e armazenadas. A política de classificação da informação deve contemplar no mínimo os seguintes requisitos: A política de classificação da informação deve contemplar, no mínimo, as seguintes classes: ○ **Informações sensíveis**: Informações de detentores de direito, dados proprietários e pessoais de clientes ou colaboradores; ○ **Informações internas**: Documentações de sistema, políticas, procedimentos e qualquer outro documento relacionado aos recursos de processamento da informação ou ao negócio; ○ **Informações públicas**: informações que não necessitam de requisitos de confidencialidade e podem ser divulgadas ao público. Para cada uma das classes, DEVEM ser definidas as condições de acesso, armazenamento, manipulação (incluindo cópia e transmissão), salvaguarda e descarte.	O	O	O	O
3.1.4	Política de uso da Internet	O acesso a Internet DEVE ser controlado a fim de minimizar o risco de vazamento ou comprometimento de informações sensíveis ou comprometimento dos sistemas internos. DEVE haver uma política de uso da Internet que contemple, no mínimo, controles para os seguintes requisitos: • Download e execução de executáveis; • Uso pessoal da Internet;	O	R	O	O

		• Acesso a sites perigosos ou de conteúdo impróprio; • Monitoração de acessos; • Uso do e-mail da organização.				

3.3.2 Definição e segregação de funções

As atividades nas organizações precisam ser conduzidas tendo claras quais são as funções e responsabilidades de cada pessoa na organização.

Ref	Requisito	Descrição	C	CR	P	S
3.2.1	Definição das funções	A entidade DEVE manter a relação das funções associadas às atividades da Entidade. A entidade DEVE manter, para cada colaborador, as funções que pode exercer. A entidade DEVE manter, para cada colaborador, suas responsabilidades.	O	R	O	O
3.2.2	Segregação de funções	A entidade DEVE, quando possível, garantir a separação entre as funções de autorização, aprovação, execução, controle e contabilização das operações.	O	R	O	O
3.2.3	Privilégio mínimo	A entidade DEVE atender à teoria de segurança do privilégio mínimo, ou seja, o conceito de que os usuários devem ter o menor privilégio possível necessário para executar as tarefas atribuídas.	O	R	O	O

3.3.3 Gestão de ativos de TI

A gestão de ativos compreende os processos para o mantenimento seguro e organizado dos ativos. Os ativos que devem ser considerados, dentro do escopo determinado por este documento, são:

Ativos da informação e TI: Software, hardware (estações de trabalho, servidores, scanners e similares), mídias de cópias de segurança, dados, documentações, etc;

Ref	Requisito	Descrição	C	CR	P	S
3.3.1	Inventário dos ativos de TI	A entidade DEVE manter um inventário com todos os ativos relacionados à TIC.	R	F	O	O
3.3.2	Registro de entrada e saída de ativo de TI	A entidade DEVE manter controle e registros da entrada e saída de equipamentos, dispositivos e mídias das dependências da entidade.	R	F	O	O
3.3.3						

3.3.4 Gestão de usuários do sistema

A utilização de usuários no ambiente computacional deve ser controlada a fim de reduzir, sobretudo, o risco de acessos não autorizados e possibilitar a rastreabilidade na ocorrência de eventos de segurança da informação envolvendo o acesso, a modificação e a cópia não autorizada dos dados de cartório.

Ref	Requisito	Descrição	C	CR	P	S
3.4.1	Cadastro de usuário para acesso ao ambiente computacional	O cadastro de usuário para acesso ao ambiente computacional deve ser realizado utilizando procedimento documentado obedecendo aos seguintes requisitos: • O procedimento DEVE definir claramente quem são os responsáveis pela autorização de inclusão, remoção e alteração de perfil de usuários no sistema; • O cadastro de usuários DEVE ser realizado a partir de formulário específico, descrevendo quais são os sistemas e serviços que o usuário deve possuir acesso.	O	F	O	O
3.4.2	Termo de utilização do ambiente computacional	Cada usuário do sistema DEVE assinar um Termo de utilização do ambiente computacional. Neste termo, os usuários se declaram cientes a respeito da forma de uso correta do ambiente computacional, descrita na política de segurança, incluindo a ciência de que o identificador de usuário recebido é exclusivo para viabilizar o exercício de suas atividades profissionais.	O	R	O	O
3.4.3	Identificadores do usuário	Uma mesma pessoa DEVE, sempre que possível, possuir identificadores de usuários iguais nos diversos sistemas, a fim de facilitar a gestão de usuários e a rastreabilidade dos eventos do sistema.	O	R	O	O
3.4.4	Compartilhamento de identificadores de usuários	O compartilhamento de identificadores de usuários NÃO DEVE ocorrer, pois impossibilita a identificação precisa da pessoa no caso de eventos. Além disso, impõe o compartilhamento da senha. As únicas exceções admissíveis são: Limitação técnica do sistema: Quando o sistema não permite a criação de identificadores distintos de usuários, sejam eles usuários comuns ou usuários com privilégio administrativos; Usuários de conexão de aplicativos: Quando o identificador de usuário for para uso em uma aplicação (usuários de conexão a banco de dados, etc.).	O	R	O	O
3.4.5	Usuário com privilégio administrativo	São considerados usuários com privilégio administrativo os administradores, os operadores e os gestores do sistema, pois realizam atividades críticas relacionadas à configuração do sistema e criação/alteração de privilégios de outros usuários.	O	R	O	O

		Para os usuários com privilégio administrativo, nos sistemas nos quais não é possível ao usuário, antes de um acesso, escolher qual perfil de acesso quer utilizar (perfil de usuário normal ou perfil administrativo), DEVEM ser criados dois identificadores para o usuário, um para uso do sistema com privilégio normal e outro para uso do sistema com privilégio administrativo. O identificador de usuário com privilegio administrativo não DEVE ser utilizado, pelo usuário, para atividades que não exigem privilégio administrativo.				
3.4.6	Recuperação de senhas administrativas críticas	A entidade DEVE possuir procedimentos para guarda e recuperação de senhas dos usuários com privilégio administrativo considerados críticos, a fim de possibilitar a recuperação segura e auditada da senha em caso de indisponibilidade da pessoa (ex: falta, demissão, falecimento, etc)	O	R	O	O
3.4.7	Desligamento de colaborador	Quando do desligamento de um colaborador, a entidade DEVE: Bloquear o uso do identificador do usuário, evitando remover o identificador para possibilitar o rastreamento dos eventos; Revogar todos os direitos de acesso atribuídos a este colaborador.	O	R	O	O
3.4.8	Desligamento de colaborador com funções administrativas	Quando do desligamento de um colaborador com funções administrativas, todas as senhas de identificadores de usuários compartilhados de conhecimento do colaborador DEVEM ser trocadas.	O	R	O	O
3.4.9	Atribuição de privilégios de acesso	A atribuição de privilégios DEVE ser realizada com base ao papel e função do usuário e deve adotar o principio do privilégio mínimo necessário para a execução de suas atividades. Os privilégios atribuídos DEVEM ser documentados, constando as seguintes informações: Relação dos privilégios atribuídos; Relação de todos os sistemas e aplicações ao qual tenha acesso; Declaração de responsabilidade do usuário sobre os privilégios a ele concedidos.	O	R	O	O

		Os privilégios devem ser revisados após mudança de função ou de área, garantindo que os privilégios atribuídos anteriormente sejam revogados e que sejam atribuídos novos privilégios.				
3.4.10	Revisão dos direitos de acesso	Os direitos de acesso devem ser revisados anualmente considerando: • Colaboradores ou parceiros que mudaram de cargo ou função; • Colaboradores ou parceiros que não tenham mais relação com a organização; • Eliminação de usuários genéricos, compartilhados ou de grupo.	O	R	O	O

3.3.5 Gestão de mudanças

A gestão de mudanças reduz significativamente o risco de ocorrência de eventos problemáticos que afetem os princípios de segurança da informação após a implementação de uma mudança, fornecendo condições para prevenção e, quando da ocorrência destes eventos, mitigação e redução eficaz das consequências.

Ref	Requisito	Descrição	C	CR	P	S
3.5.1	Aprovação de mudanças críticas	Todas as mudanças críticas DEVEM ser avaliadas, programada e aprovadas antes de sua implementação. São consideradas como mudanças críticas: Inclusão, remoção ou substituição de equipamentos de rede e servidores; Alterações significativas de sistema operacional em servidores; Alterações significativas no software SREI.	R	F	O	O
3.5.2	Documentação de	Toda mudança crítica deve ser documentada contemplando no mínimo as seguintes	R	F	O	O

	mudança crítica	informações: Descrição da mudança; Levantamento dos possíveis impactos; Resultados da avaliação de risco; Data programada da mudança; Aprovação dos responsáveis; Plano de retorno em caso de problemas (*rollback*); Após a mudança, o registro do resultado da mudança.				

3.3.6 Gestão de incidentes

As entidades que operam com o sistema SREI devem estar preparadas para tratar incidentes de forma eficaz através de planos e medidas contingenciais. Quando da ocorrência de um evento de segurança, as entidades devem agir de forma organizada reduzindo as perdas e paradas nos sistemas.

Ref	Requisito	Descrição	C	CR	P	S
3.6.1	Responsabilidade dos colaboradores	Os colaboradores DEVEM estar conscientes dos procedimentos para reportar eventos. Principalmente, eventos relacionados a: • Comportamento incomum de sistemas de TI como mal funcionamento/bugs, mensagens de erro, alarmes e alertas, atrasos e resultados imprevistos; • Perda de serviços, equipamentos e recursos de TI incluindo roubo, danos, mal funcionamentos, sobrecargas, acidentes, erros humanos ou outras situações que				

		podem causar interrupções nos serviços; • Situações de alto risco que podem facilmente levar a incidentes sérios de segurança da informação em circunstancias menos afortunadas.				
3.6.2	Registro e informação	Dependendo da severidade do evento de segurança relatado, o Suporte deve iniciar um processo adequado de resposta a incidentes e envolver e informar parceiros relevantes provavelmente inclusos: • Oficiais; • TI e Segurança da Informação; • Quadro de sócios; • Segurança predial; • Entidades governamentais; • Recursos Humanos; • Jurídico; Assim que os incidentes relatados tenham sido resolvidos, o Suporte fecha seus registros informando a aqueles que relataram e, também, aqueles que necessitam dos resultados.				
3.6.3	Escopo do procedimento de resposta a incidentes	Os procedimentos para a resposta a incidentes DEVEM garantir uma resposta rápida, efetiva e organizada para todos os tipos de incidentes de segurança da informação, incluindo: • Falhas de disponibilidade (como, por exemplo, perda de serviços de TI resultantes de falhas de sistema ou rede e negação de serviço); • Falhas de integridade (como, por exemplo, erros resultantes de dados de negocio				

		incompletos ou imprecisos; disfunções de redes ou sistemas causadas por vírus e worms; mal uso de sistemas; fraudes envolvendo sistemas de TI); • Falhas de confidencialidade (como, por exemplo, divulgação não autorizada ou acesso a informações sensíveis); • Quase incidentes (como, por exemplo, interrupções de serviço fora do horário ou pico; serio corrompimento de dados utilizando cópias de segurança; descoberta e direitos de acesso inapropriados).				
3.6.4	Procedimento de resposta a incidentes	Os Procedimentos de resposta a incidentes cobrem: • A análise de eventos e fragilidades de segurança relatados e a monitoração de sistemas, alertas e vulnerabilidades a fim de identificar e priorizar eventos de segurança que aparentam indicar atuais incidentes ou quase incidentes; • Retenção (como, por exemplo, desconectar sistemas afetados da rede para future avaliação); • Analise e identificação da causa dos incidentes; • Planejamento e implementação de controles para prevenir recorrências, se necessário; • Comunicação com aqueles que são afetados ou envolvidos na recuperação dos incidentes, incluindo a gestão e, onde apropriado, autoridades externas;				
3.6.5	Recuperação e correção	Ações para a recuperação de incidentes de segurança e para corrigir falhas de sistemas devem ser controladas, assegurando que: • Somente funcionários autorizados sejam permitidos a ter acesso privilegiado a				

		sistemas e dados para o propósito de diagnóstico e para solucionar incidentes de segurança; • Ações de emergência tomadas devem ser completamente documentadas, reportadas a gerência e revisadas de maneira ordenada; • A integridade de dados, sistemas e controles de segurança de negocio são confirmadas para que a utilização normal possa continuar.				

3.3.7 Gestão de riscos

Os riscos devem ser identificados, avaliados e tratados com o objetivo de minimizar os impactos nas operações e garantir a continuidade dos negócios.

Ref	Requisito	Descrição	C	CR	P	S
3.7.1	Gestão de riscos	A entidade DEVE realizar, periodicamente, a avaliação e tratamento de riscos às operações.	O	F	O	O
3.7.2	Conjunto mínimo de ameaças.	A gestão de riscos DEVE incluir, entre outras, a avaliação das seguintes ameaças: • Inundação das instalações; • Fogo nas instalações; • Desabamento da instalação predial; • Roubo de equipamentos (incluindo o sistema de armazenamento de dados).	O	F	O	O

3.3.8 Gestão de contratos com fornecedores

Toda relação com partes externas deve ser documentada, gerenciada e analisada criticamente a intervalos regulares. Adicionalmente, deve garantir a segurança na operação dos serviços.

Ref	Requisito	Descrição	C	CR	P	S
3.8.1	Contratos com entidades externas	Os contratos firmados entre a organização e entidades externas para a prestação de serviços DEVEM obedecer aos seguintes requisitos: • Possuir cláusulas de confidencialidade; • Declarar todas as responsabilidades do prestador de serviço para garantir a integridade dos dados armazenados e, também, a integridade dos recursos de processamento da informação; • Se aplicável, DEVE ser considerado em clausulas de contrato: O acesso remoto de terceiros aos recursos de processamento da informação do cartório DEVE ser limitado aos mínimos privilégios, evitando acesso a outros recursos. Também, este acesso DEVE ser aprovado e documentado em contrato, declarando claramente as responsabilidades e termos de confidencialidade; • Se aplicável, DEVE especificar o acordo de nível de serviço (SLA – *Service Level Agreement*) que deve ser atendido pelo prestador de serviço; • Atender aos requisitos obrigatórios deste documento, quando pertinente.	O	F	O	O
3.8.2	Revisão dos contratos	Os seguintes tópicos DEVEM ser considerados na renovação ou revisão do contrato: • Revisão dos direitos de acesso de parceiros aos sistemas internos; • Revisão das responsabilidades quanto à segurança da informação; • Revisão do SLA e outros requisitos de disponibilidade; As cláusulas revistas DEVEM ser incluídas na nova versão de contrato ou em um aditivo ao	O	F	O	O

		contrato. Existem fatores que podem iniciar o processo de revisão do contrato: • Mudanças significativas na prestação de serviços pelo parceiro; • Novos requisitos de segurança, regulatórios ou legais a serem atendidos; • Mudanças significativas nos processos de negócio; • Não atendimento às cláusulas do contrato.				

3.3.9 Continuidade dos negócios

Os requisitos de continuidade de negócios tem o objetivo de fornecer diretrizes para a implementação segura dos processos de continuidade no caso de desastres ou eventos de segurança da informação significativos.

Ref	Requisito	Descrição	C	CR	P	S
3.9.1	Plano de continuidade de negócios (PCN)	A entidade DEVE estabelecer um plano para garantir a continuidade dos negócios (PCN) quando da ocorrência de eventos críticos. 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;	R	F	R	O

		• Definir as modalidades para validação do plano, contemplando os testes a serem realizados, sua frequência e os recursos envolvidos;				
3.9.2	Eventos considerados no PCN	O plano de continuidade de negócios DEVE considerar, no mínimo, os seguintes eventos: • 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.	R	F	R	O

3.3.10 Gerenciamento da capacidade

A capacidade atual e histórica dos recursos de processamento da informação deve ser analisada e utilizada, junto aos dados de negócio, para a prospecção futura de capacidade, a fim de garantir a disponibilidade definida.

Devem ser tomadas medidas preventivas para a minimização de gargalos e redução de riscos para os ambientes de TI com base nas prospecções geradas.

Ref	Requisito	Descrição	C	CR	P	S
3.10.1	Coleta de métricas de consumo de recursos	A entidade DEVE realizar a coleta de métricas para subsidiar a análise periódica da capacidade atual dos sistemas. Para os sistemas de suporte ao SREI DEVEM, no mínimo, ser analisados os seguintes recursos: • Uso de CPU; • Uso de memória;	R	F	R	O

		• Uso de espaço de armazenamento persistente; • Uso dos enlaces da comunicação.				
3.10.2	Análise de capacidade	A entidade DEVE, periodicamente, realizar a análise da capacidade do sistema, com base no histórico de utilização dos recursos e dos dados de evolução das atividades.	R	F	R	O
3.10.3	Plano de evolução de capacidade	Como resultado da análise de capacidade, caso haja necessidade de aumento de capacidade futura, DEVE ser estabelecido um plano de ação para evolução de capacidade considerando as seguintes informações: • 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.	R	F	R	O

4 Referências

[1] DEUTSCHES INSTITUT FÜR NORMUNG. **DIN V ENV 1627:** Windows, doors, shutters. Burglar resistance. Requirements and classification. October, 1999.

[2] TELECOMMUNICATIONS INDUSTRY ASSN/ELECTRONIC INDUSTRIES ALLIANCE. **TIA/EIA J-STD-607:** Commercial Building Grounding and Bonding Requirements for Telecommunications. October, 2002.

[3] EUROPEAN COMMITTEE FOR STANDARDIZATION. **EN 1047-2:** Secure storage units. Classification and methods of test for resistance to fire. Data rooms and data container. January, 2010.

[4] AMERICAN NATIONAL STANDARDS INSTITUTE. **ANSI/UL 263:** Fire Resistance Ratings, April, 2006.

[5] EUROPEAN COMMITTEE FOR STANDARDIZATION. **EN 1143-1:** Secure storage units. Requirements, classification and methods of test for resistance to burglary. Safes, strongroom doors and strongrooms. October, 1997.

[6] ISO/IEC ABNT - Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de segurança- Código de prática para gestão da segurança da informação**. Rio de Janeiro. 2007

ISO/IEC 20000-2:2005(E) Information Technology - Service Management Part2

[7] PCI Security Standards Council. **PCI-DSS - Payment Card Industry Data Security Standard** v2.0. 2010