Política de Interconexão de Recursos de TI

Dezembro 2006

Índice

1. Objetivo

A Política de Interconexão de Recursos de TI orienta quanto às exigências do Governo do Estado do Ceará, especificadas pelo **Decreto Governamental nº XXXXXXX** para a interconexão e compartilhamento de informações entre órgãos, entidades governamentais estaduais e federais, fornecedores e colaboradores, através da Rede Governamental. As orientações aqui relacionadas são obrigatórias e complementam padrões existentes, orientações e procedimentos a serem utilizados pelos órgãos/entidades estaduais para interconexão de redes.

Este documento serve como guia para planejamento, estabelecimento, manutenção e término de interconexões de sistemas de informação operados por diferentes órgãos/entidades estaduais, incluindo organizações de uma mesma Secretaria de Governo.

2. Abrangência

Aqui são apresentadas orientações gerais para interconexão de redes de informação, através da utilização da infra-estrutura da Rede Governamental. As solicitações de interconexão incluem a utilização da Rede Governamental como meio de acesso à Internet, a comunicação entre os órgãos/entidades estaduais, a comunicação entre órgãos/entidades estaduais e outras entidades não pertencentes ao governo do Estado do ceará.

As orientações aqui contidas destinam-se a administradores de sistemas, administradores de redes, administradores de segurança das setoriais, ao administrador de segurança de TI estadual e qualquer pessoa que seja responsável por planejar, aprovar, estabelecer, manter ou terminar interconexões de sistemas que utilizem a estrutura da Rede Governamental.

Nenhuma recomendação específica de tecnologia é referenciada aqui.

3. Vigência

Esta política passa a vigorar a partir da data de sua aprovação pelo Comitê Gestor de Segurança, e será revisada anualmente. O processo de revisão será antecipado em face da necessidade de reestruturação dos processos administrativos ou operacionais da Rede Governamental.

4. Documentação Complementar

4.1. Documentação complementar a esta Política:

- Guia de Análise de Riscos.

4.2. Outras políticas e documentos referenciados nesta política:

- Modelo de Política local de Usuários
- Modelo de Política de Administradores e Gestores de TI.

5. Política

5.1. Considerações Gerais

A interconexão de redes é definida como a conexão direta de dois ou mais sistemas de informação para o compartilhamento de dados e outros recursos computacionais. As organizações podem obter vários benefícios pela interconexão de seus sistemas de informação, tais como, a redução de custos operacionais, aumento de funcionalidade, eficiência, e acesso centralizado a informações.

As Organizações podem interconectar seus sistemas de informação por várias razões, como por exemplo:

- Trocar informações entre usuários selecionados
- Fornecer acesso em diversos níveis a bancos de dados proprietários
- Colaborar em projetos conjuntos
- Fornecer treinamento on-line
- Fornecer armazenamento seguro de informações críticas e arquivos de *backup*.

A interconexão de redes tem três componentes básicos: dois sistemas de informação (A e B) e o mecanismo através dos quais eles são interligados (o "meio" através do qual as informações são disponibilizadas, trocadas ou apenas trafegadas). Estes componentes estão mostrados na figura 1. Neste documento, assume-se que o Sistema A e o Sistema B operam sob diferente gerenciamento e são de propriedade de diferentes entidades.

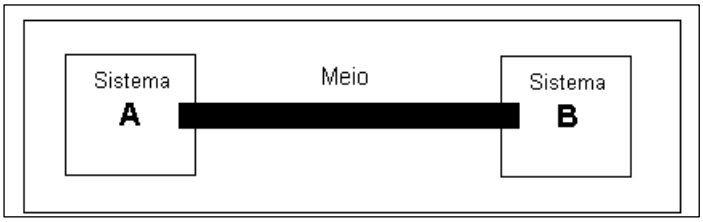

Figura 1. Interconexão

Os órgãos/entidades que compõem o Governo do Estado do Ceará utilizam a infra-estrutura da Rede Governamental para interconexão. A Rede Governamental é o "meio" que conecta os sistemas de informação dos diversos órgãos/entidades.

A Rede Governamental é uma estrutura complexa, que permite a interconexão de qualquer órgão/entidade estadual a uma rede controlada, de uso exclusivo do Governo ou de organizações por ele autorizadas. Apesar de restrita, ela não garante confidencialidade entre os órgãos/entidades que a utilizam.

Uma alternativa para órgãos/entidades estaduais que necessitem de confidencialidade é conectar seus sistemas através de uma rede privada virtual (VPN - *Virtual Private Network*) sob a estrutura da Rede Governamental. Uma VPN permite que duas ou mais partes comuniquem-se seguramente criando uma conexão privada, ou túnel, entre elas.

Informações transmitidas através desta podem ser interceptadas por pessoas não autorizadas, portanto, é necessário que os dados sensíveis sejam criptografados para garantir confidencialidade e integridade.

Existem vários níveis de interconexão de redes. De que forma se dará o acesso, e quais os recursos de informação serão acessados dependerão das atividades da organização e de suas necessidades de segurança. Em alguns casos, uma organização poderá decidir em estabelecer uma interconexão limitada, onde os usuários estarão restritos a uma única aplicação ou pasta de arquivos.

Alternativamente, um órgão/entidade governamental pode estabelecer uma conexão mais abrangente, permitindo que usuários acessem múltiplas aplicações e/ou bancos de dados. Finalmente, algumas organizações podem permitir total transparência e acesso a suas respectivas redes através da interconexão.

Apesar das vantagens, a interconexão de redes de informação pode expor os participantes a riscos. Se a interconexão não é apropriadamente projetada, falhas de segurança podem ocorrer e resultar em comprometimento de todos os sistemas conectados e das informações que eles armazenam, processam ou transmitem.

De maneira similar, se um dos sistemas conectados é comprometido, a interconexão pode ser utilizada para alcançar e comprometer o outro sistema e suas informações. O potencial para comprometer é ressaltado pelo fato de que, na maioria dos casos, os órgãos/entidades estaduais participantes têm pouco ou nenhum controle sobre as operações e gerenciamento do sistema da outra parte.

É obrigatório, então, que as partes interessadas discutam sobre os riscos envolvidos durante o planejamento da futura ou atual conexão e dos controles de segurança que podem ser implementados para diminuir estes riscos. É imprescindível que seja estabelecido um acordo entre as partes com respeito ao gerenciamento, operação e uso da interconexão, formalmente documentado.

Para interconexões seguras, é necessário que os órgãos/entidades estaduais troquem autorizações escritas através da equipe de planejamento conjunta antes de conectar seus sistemas de informação a outros sistemas, para que possa ser definido um nível de risco aceitável. A autorização escrita deverá definir as regras de comportamento e controles que devem ser mantidos para interconexão de redes, e que deverão ser incluídos no plano de segurança do órgão ou entidade estadual.

5.2. Exigências de Segurança para Interconexão de Redes através da Rede Governamental

As exigências de segurança aplicam-se a todas as interconexões que forem estabelecidas sob a responsabilidade direta ou indireta do Governo do Estado, incluindo aquelas que

são operadas pelos órgãos/entidades da administração pública estadual e por empresas terceirizadas.

Quando duas ou mais entidades planejarem o estabelecimento de uma interconexão, deverão prevalecer as exigências de segurança da entidade com maior nível de segurança estabelecido do grupo.

5.3. Planejamento da interconexão

O processo de comunicar dois ou mais sistemas, serviços e redes dentro da Rede Governamental deverá começar com a fase de planejamento, na qual os órgãos/entidades estaduais envolvidos, sob coordenação da Administração de Segurança de TI Estadual (ver item 5.3.1.4 deste documento), executam atividades preliminares e examinam todos os pontos relevantes quanto aos aspectos técnicos de segurança e administrativos. A fase de planejamento garante que a interconexão irá operar tão eficientemente e seguramente quanto possível. Esta seção discute os passos recomendados para planejar uma interconexão de redes.

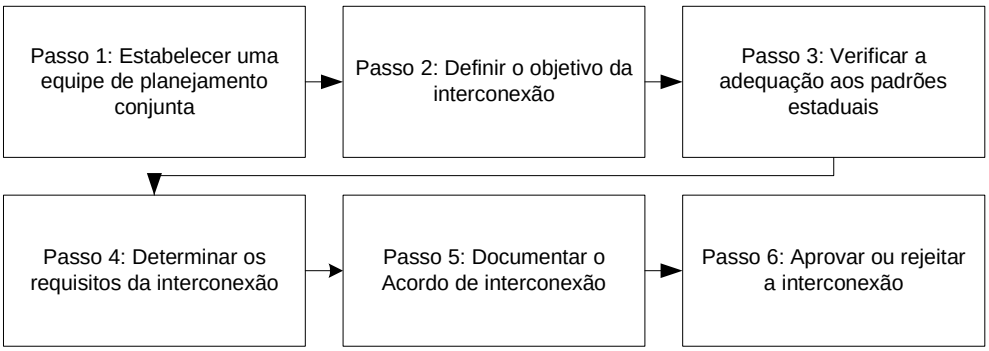

Figura 2. Planejamento da interconexão

5.3.1. Estabelecer uma equipe de planejamento conjunta

5.3.1.1. Os órgãos/entidades estaduais são responsáveis por garantir a segurança de seus respectivos sistemas e informações.

5.3.1.2. Os órgãos/entidades devem estabelecer uma equipe conjunta de planejamento composta pelo Administrador de Segurança de TI da setorial de cada entidade envolvida, ou equivalente, e possivelmente pelo administrador de sistemas e/ou serviços que estarão envolvidos na conexão. No caso de fornecedores ou empresas terceirizadas, estes deverão indicar os profissionais apropriados para atuar no planejamento.

5.3.1.3. Independente de como é formada, a equipe deverá estar comprometida com a segurança durante todo ciclo

de vida da comunicação.

5.3.1.4. A Administração de Segurança de TI Estadual deverá ser informada do início de qualquer atividade de planejamento visando a interconexão entre órgãos/entidades com outros órgãos/entidades ou fornecedores.

5.3.2. Definição do processo

5.3.2.1. Os órgãos/entidades estaduais devem trabalhar em conjunto para determinar o objetivo da interconexão, determinar como serão alcançado os respectivos objetivos, e identificar potenciais riscos e custos adicionais.

5.3.2.2. A definição do processo estabelecerá a base da interconexão e facilitará o planejamento. Fatores que devem ser considerados incluem recursos da Rede Governamental e possíveis custos comuns (equipe, instalações físicas), expectativas de benefícios (por exemplo, aumento de eficiência, acesso centralizado as informações) e riscos potenciais (por exemplo, técnico, legal e financeiro).

5.3.2.3. Como parte deste processo, as organizações envolvidas deverão examinar assuntos relacionados à privacidade das informações que irão ser trocadas ou trafegarão através da interconexão, e determinar se tal uso respeita as políticas de segurança de TI estadual. A equipe de planejamento deverá consultar as exigências mínimas requeridas para poder estabelecer o nível de segurança da sua interconexão, devendo ser respeitadas as exigências de segurança das entidades com o maior nível de segurança. Permissões para troca ou transferência de informações devem ser documentadas, junto com um compromisso para proteger tais informações.

5.3.3. Certificação e Reconhecimento

Antes de interconectar seus sistemas de informação, cada organização deverá garantir que seus respectivos sistemas estejam adequadamente certificados de acordo com os Padrões Mínimos para Conexão à Rede Governamental, contidos no documento Recomendações de Soluções de Segurança baseadas em *Software* Livre com licenças GNU.

5.3.4 Determinação dos Requisitos para Interconexão

A equipe de planejamento conjunta deve identificar e examinar todas as questões técnicas, de segurança e administrativas relevantes relacionadas à interconexão. Estas informações serão usadas para desenvolver o Acordo de Segurança de Interconexão (ASI) e um Memorando de Entendimento (ME). Estas informações serão utilizadas para desenvolver um plano de implementação para estabelecer a interconexão programada.

A equipe de planejamento conjunta deverá obedecer aos seguintes procedimentos, levantando as informações descritas a seguir:

5.3.4.1 Grau e Método de interconexão: Define o grau da interconectividade que irá ser estabelecida entre os sistemas de informação, variando desde conectividade limitada (troca de informações limitada) à conectividade no nível de órgão ou entidade (compartilhamento ativo de informações e aplicações). Em adição, descreve o método utilizado para conectar os sistemas (Rede Governamental ou VPN sob Rede Governamental).

5.3.4.2 Impacto na Infra-estrutura e Procedimentos Operacionais Existentes:

Determinar se a infra-estrutura de rede de computadores em uso pelos órgãos/entidades é suficiente para suportar a interconexão, ou se componentes adicionais serão necessários (por exemplo, roteadores, *switches*, servidores e *software*). Se componentes adicionais forem necessários, determinar o impacto potencial, ao instalar e utilizar, que estes componentes adicionais acarretarão na infra-estrutura existente. Adicionalmente, determinar o impacto potencial que a interconexão terá sobre as operações atuais, incluindo novas demandas de administração de sistemas, aumento de tráfego e novos requisitos de treinamento.

5.3.4.3 Requisitos de *Hardware*: Identificar o *hardware* que será necessário para suportar a interconexão, incluindo linhas de comunicação, roteadores, *firewalls*, *hubs*, *switches*, servidores e estações de trabalho. Determinar se o *hardware* existente é suficiente, ou se componentes adicionais serão necessários. Se novo *hardware* for necessário, produtos apropriados deverão ser selecionados para garantir a interoperabilidade.

5.3.4.4 Requisitos de *Software*: Identificar os *softwares* que serão necessários para garantir a interconexão, incluindo *software* para *firewalls*, *appliances*, servidores e estações de trabalho. Determinar se o *software* já existente é suficiente, ou se *software* adicional será necessário. Se novos *softwares* forem necessários, produtos adequados deverão ser selecionados para garantir a interoperabilidade.

5.3.4.5 Sensibilidade das informações: Identificar o grau de sensibilidade das informações que serão utilizadas, disponibilizadas, trocadas ou

trafegadas através da interconexão. Identificar a sensibilidade das informações é um procedimento crítico para determinar os controles de segurança que deverão ser utilizados para proteger sistemas conectados e informações. Exemplos de informações sensíveis incluem informações financeiras, informações pessoais e informações confidenciais dos órgãos/entidades estaduais.

5.3.4.6 Comunidade de Usuários: Define se todos ou um grupo limitado de usuários terão acesso, trocarão ou receberão informações através da interconexão. No caso de usuários limitados, devem ser desenvolvidas abordagens para compilar e gerenciar os perfis de todos os usuários que irão ter acesso à interconexão, incluindo identificação de usuários, endereços de estações, tipos de estações, sistemas operacionais, e qualquer outra informação relevante.

5.3.4.7 Serviços e Aplicações: Identificar os serviços e sistemas corporativos que serão fornecidos sobre a Interconexão para cada organização,e as aplicações associadas com esses serviços, se apropriado. Exemplos de serviços incluem *e-mail*, *file transfer protocol* (FTP), RADIUS, Kerberos, *database query*, *file query*, serviços Netbios (137, 138 e 139), CIFS e outros serviços computacionais.

5.3.4.8 Controles de Segurança: Identificar os controles de segurança que serão implementados para proteger a confidencialidade, integridade, disponibilidade e não repúdio de informações e sistemas que passem pela interconexão. Controles podem ser selecionados dos exemplos fornecidos neste documento e em outras fontes. Controles devem ser apropriados para os sistemas que irão ser conectados através do ambiente de interconexão que irá operar.

5.3.4.9 Segregação de responsabilidades: Determinar qual a responsabilidade das entidades sobre a interconexão estabelecida. A segregação de responsabilidades reduz o risco de que um único indivíduo cause danos aos sistemas interconectados e às informações, seja acidentalmente ou deliberadamente.

5.3.4.10 Relato e Resposta a Incidentes: Estabelecer procedimentos para relatar e responder a atividades anômalas e suspeitas que são detectadas através de tecnologia ou pessoal de suporte. Determinar quando e como notificar outros órgãos/entidades envolvidos no processo de interconexão sobre incidentes de segurança, incluindo a causa do incidente, informações e programas afetados, e o atual e potencial impacto. Adicionalmente, identificar os tipos de incidentes que requerem uma resposta coordenada, e determinar como coordenar atividades de resposta. Cada entidade deve desenvolver um plano de resposta a incidentes para este propósito.

5.3.4.11 Cópias de Segurança: Determinar se as *informações* que são trafegadas através da interconexão devem ser copiadas e/ou

armazenadas para segurança. Se cópias de segurança são necessárias, devem ser identificados os tipos e informações que *deverão* ser copiadas e com qual freqüência (diária, semanal ou mensal), e se os *backups* serão realizados por todas as organizações envolvidas ou apenas por um participante. Como referência, pode ser utilizado o modelo de Política de Cópias de Segurança, incluso no modelo Política de Administradores e Gestores de TI (modelo) publicado pela CGETI.

5.3.4.12 Planejamento de Contingência: Cada órgão/entidade da administração pública estadual deverá ter um Plano de Contingência para responder e recuperar-se de desastres e de outras contingências que causem disfunção nas operações, variando desde a falha de componentes do sistema até a perda de instalações computacionais. Deve ser definido como notificar cada um dos outros participantes da interconexão, para determinar em que medida as organizações assistirão umas as outras, e os termos em que essa assistência se dará. O plano deve determinar se devem ser incorporados mecanismos de redundância entre os componentes que provêem a interconexão, incluindo pontos de interconexão, e como recuperar cópias de segurança. Deve também coordenar treinamento de respostas a desastres, testes e exercícios. Caso a necessidade de planejamento de contingência seja identificada, devem ser definidos os recursos necessários para que sejam formalmente solicitados à administração dos órgãos/entidades.

5.3.4.13 Termo de Reconhecimento: Os usuários devem assinar um termo de reconhecimento indicando que eles compreendem as regras. Se aplicações compartilhadas são utilizadas, deve haver garantia que os usuários conhecem como utilizá-las corretamente. Se a interconexão é utilizada para troca ou transferência de informações sensíveis, os usuários devem compreender os cuidados especiais para utilizar estas informações.

5.3.4.14 Funções e responsabilidades: Inclui o pessoal que será responsável por estabelecer, manter ou gerenciar a interconexão, incluindo administradores de rede, de sistema, supervisores de segurança de TI, administradores de segurança de TI setoriais. Deve ser escolhido pessoal que tenha especialidade no assunto em questão. Se contratados estão envolvidos, as organizações devem solicitar um acordo de confidencialidade para resguardar a confidencialidade e integridade das informações trocadas.

5.3.4.15 Agendamento: Um agendamento preliminar para todas as atividades deve ser desenvolvido, envolvendo o planejamento, estabelecimento e manutenção da interconexão. Devem ser determinadas também as condições para terminar ou reautorizar a interconexão. Por exemplo, as partes devem concordar em rever o acordo de interconexão para determinar se haverá reautorização e continuidade operacional em uma

periodicidade pré-estabelecida.

5.3.4.16 Custos e orçamento: Deve ser especificada a expectativa de custos necessários para planejar, estabelecer e manter a interconexão. Todos os custos associados, incluindo mão-de-obra, *hardware, software,* linhas de comunicação, instalações, segurança física, treinamento e testes devem estar incluídos. Um orçamento deve ser desenvolvido e determinado como os custos serão distribuídos entre as partes.

5.3.5 Acordo de Interconexão

A equipe de planejamento conjunta deverá documentar não apenas o acordo que governará a interconexão, mas também os termos sob os quais as organizações irão obedecer ao acordo, baseado na revisão de todos os aspectos técnicos, de segurança e administrativos relevantes. Dois documentos devem ser desenvolvidos: Acordo de Segurança de Interconexão (ASI) e um Memorando de Entendimento (ME). Pelo fato do ASI e ME conterem informações sensíveis, eles devem ser armazenados em local seguro e protegidos contra furto, danos e destruição. Se cópias forem armazenadas eletronicamente, elas devem ser protegidas contra modificação ou exibição não autorizada.

5.3.5.1 Acordo de Segurança de Interconexão (ASI)

O ASI é um documento de segurança que especifica os requisitos técnicos e de segurança para estabelecer, operar e manter uma interconexão através da Rede Governamental. O ASI deve documentar os requisitos para conectar os sistemas de informação, descrever os controles de segurança que serão utilizados para protegê-los, e conter plantas e desenhos das topologias a serem interconectadas, além de possuir um bloco para assinaturas.

5.3.5.2 Memorando de Entendimento (ME)

O Memorando de Entendimento (ME) documenta os termos e condições para o compartilhamento de informações e recursos de informação de uma maneira segura. Especificamente, o ME define o objetivo da interconexão; relaciona as pessoas que farão parte da equipe de planejamento conjunta; identifica os pontos de contato relevantes; especifica as responsabilidades de cada órgão/entidade da administração pública estadual envolvida e define os termos do acordo, incluindo divisão de custos e os prazos para terminar e reautorizar a interconexão. O ME não inclui detalhes técnicos da interconexão, que devem ser estabelecidos no ASI.

5.3.6 Aprovação ou rejeição da interconexão do sistema

A equipe de planejamento conjunta deverá analisar o ASI e o ME. Após a análise, devem emitir um parecer para os respectivos representantes de cada organização. De posse do parecer, os representantes decidem se:

- Aprovam a interconexão

- Aprovam temporariamente ou
- Rejeitam a interconexão

5.3.6.1 Se os representantes de cada organização aceitarem o ASI e o ME, deverão assinar e datar os documentos, aprovando assim a interconexão. Uma cópia assinada de cada documento deve ser enviada para os administradores dos órgãos/entidades envolvidas no planejamento da interconexão. Cópias dos documentos devem ser arquivados pela Administração de Segurança de TI Estadual.

5.3.6.2 Uma ou todas as entidades envolvidas podem decidir por garantir uma aprovação temporária. Aprovação temporária pode ser aceita se a interconexão solicitada não atende a todos os requisitos relacionados no ASI, mas a urgência da missão requer que a interconexão seja estabelecida. Os representantes de cada organização devem enviar um documento assinado a cada respectivo administrador de segurança de TI dos órgãos/entidades envolvidas especificando as tarefas que devem ser completadas antes da aprovação total, incluindo a implementação de controles de segurança adicionais, se necessários. Os representantes devem acordar prazos para execução das tarefas, que devem ser completadas antes da interconexão estar totalmente operacional.

5.3.6.3 Uma ou todas as entidades envolvidas podem rejeitar a interconexão, a equipe de planejamento conjunta deverá retornar ao processo de planejamento. Nesta, os representantes de cada organização devem prover um documento assinado para os respectivos administradores de segurança especificando as razões para a rejeição da interconexão e fornecendo sugestões de soluções. A equipe conjunta de planejamento deverá reunir-se para discutir e aprovar as soluções e prazos para correção das deficiências relacionadas.

5.4 Estabelecendo a interconexão de sistemas

Depois que uma interconexão de redes é planejada e aprovada, ela deve ser implementada. Esta seção fornece recomendações para o estabelecimento de uma interconexão de redes, como mostrado na Figura 3.

Figura 3. Estabelecendo a interconexão

5.4.1 Plano de implementação

Para garantir que os sistemas de informação serão conectados apropriadamente e seguramente, a equipe de planejamento conjunta deverá desenvolver um Plano de Implementação de Interconexão. O objetivo deste plano é centralizar todos os aspectos do esforço de interconexão em um documento para clarificar como os requisitos técnicos especificados pelo ASI irão ser implementados. Um plano de implementação bem desenvolvido aumentará a probabilidade de que a interconexão operará de maneira correta e segura.

No mínimo, o plano de implementação deverá:

5.4.1.1 Descrever os sistemas corporativos e serviços da Rede Governamental que serão conectados;
5.4.1.2 Identificar a sensibilidade ou grau de classificação das informações que serão disponibilizadas, trocadas ou que trafegarão através da interconexão;
5.4.1.3 Identificar pessoal que irá estabelecer e manter a interconexão, e claramente especificar suas responsabilidades;
5.4.1.4 Identificar tarefas e procedimentos de implementação;
5.4.1.5 Identificar e descrever controles de segurança que serão utilizados para proteger a confidencialidade, integridade, disponibilidade e não repúdio dos sistemas interconectados e suas informações;
5.4.1.6 Fornecer critérios de medição e procedimentos de testes que garantam que a interconexão opera de maneira adequada e segura;
5.4.1.7 Especificar requisitos de treinamento para usuários.

5.4.2 Execução do Plano de Implementação

Depois que um plano de implementação é desenvolvido, ele deve ser executado. Uma lista de tarefas recomendadas para o estabelecimento da interconexão é fornecida abaixo. Procedimentos detalhados associados a cada tarefa devem ser fornecidos junto com o Plano de Implementação.

5.4.2.1 Implementação/ Configuração de Controles de Segurança

Se controles de segurança não existem ou estiverem configurados inadequadamente, o processo de estabelecimento da interconexão poderá expor os sistemas corporativos, redes locais e serviços a pessoas não autorizadas.

O primeiro passo é implementar controles de segurança apropriados ou configurar controles já existentes, como especificado no ASI. Controles de segurança devem incluir:

A) ***Firewalls:*** *Firewalls* determinam se pacotes de informações têm permissão de ingressar em uma rede, e restringem o acesso a recursos específicos. *Firewalls* devem ser instalados para proteger redes internas e outros recursos de acesso não autorizado através da interconexão. Se já existirem, devem ser configurados de acordo com os requisitos do ASI. Se a interconexão envolve o uso de

servidores, devem ser posicionados em uma DMZ (Zona Desmilitarizada), que deve ser estabelecida através da instalação de dois *firewalls*: um na linha externa e outro conectado a rede interna. As portas do *firewall* devem estar configuradas corretamente com controles de acesso, políticas e procedimentos definidos. Todas as senhas padrão devem ser alteradas.

B) **Detecção de Intrusão:** Um sistema de detecção de intrusão (IDS) detecta ameaças a segurança pela observação de padrões de atividade que são associados com tentativas de intrusão ou mau uso de usuários internos. Todas as entidades envolvidas devem implementar sistemas IDS (ou configurar um IDS já existente) para detectar atividades maliciosas ou indesejáveis que possam afetar a interconexão ou as informações que passam por ela. Uma combinação de IDS baseado em rede ou em *host* pode ser utilizada, se necessário. Mecanismos de alerta devem ser configurados para notificar administradores de redes, de sistemas ou administradores de segurança de TI quando tentativas de intrusão ou atividades inesperadas são detectadas.

C) **Auditoria:** Mecanismos de auditoria devem ser instalados e configurados para registrar atividades que ocorram através da interconexão, incluindo processos de aplicação e atividades de usuários. Atividades que devem ser registradas incluem tipo do evento, data e hora do evento, identificação do usuário, identificação da estação de trabalho, o sucesso ou falha de tentativas de acesso, ações de segurança tomadas pelos administradores de sistemas, de redes e administradores de segurança de TI. Registros de segurança devem ter acesso apenas de leitura, e apenas pessoal autorizado deverá ter acesso aos logs. Adicionalmente, logs devem ser armazenados em uma localização segura e protegidos contra furto ou destruição.

D) **Identificação e autenticação:** Identificação e autenticação são utilizadas para prevenir pessoas não autorizadas de terem acesso a sistemas de informação. Mecanismos fortes para identificar e autorizar usuários devem ser utilizados para garantir apenas acesso autorizado à interconexão. Estes mecanismos incluem identificação de usuários e senhas, certificados digitais, dispositivos de identificação (*tokens*), biometria e *smart cards*, dependendo do nível de segurança exigido. Se utilizadas, senhas devem ter pelo menos seis caracteres, devem ser uma mistura de caracteres numéricos, alfabéticos e especiais, e devem ser trocadas regulamente. Arquivos que armazenam senhas devem ser criptografados e protegidos seguramente contra acesso não autorizado. Como referência, o modelo de Políticas Usuários da Rede Local disponibilizado pela CGETI. Dependendo da sensibilidade das informações, organizações podem permitir que usuários acessem a interconexão depois de autenticados em seu domínio local, reduzindo a quantidade de múltiplas senhas ou outros mecanismos. Aplicações operando através da interconexão podem confiar nas informações de autenticação de usuários de um domínio local, utilizando um mecanismo de autenticação via *proxy.*

E) **Controles de Acesso Lógico:** Controles de Acesso Lógico são mecanismos utilizados para designar quem tem acesso a recursos de sistemas e que tipos de transações e funções eles têm permissão para executar.

F) **Lista de Controle de Acesso (Access Control Lists - ACL)** e regras de acesso especificam os privilégios de acesso de pessoal autorizado, incluindo o nível de acesso e tipos de transações e funções que são permitidas (por exemplo, ler, escrever, executar, apagar, criar e procurar). *hardware* e software podem ter ACLs configuradas diretamente, ou as ACLs podem ser administradas *offline* e depois distribuídas para roteadores e outros dispositivos. Regras de acesso devem garantir privilégios adequados de acesso à pessoal autorizado, baseadas em suas atribuições e funções de trabalho. Apenas administradores de sistema devem ter acesso aos controles. Adicionalmente, mensagens (*banners*) de advertência devem notificar a usuários não autorizados que eles estão acessando sistemas pertencentes ao Governo Estadual e que podem ser punidos conforme as leis vigentes. A mensagem deve ainda advertir que os sistemas são monitorados.

G) **Varredura de Códigos Maliciosos:** Informações que passam de um sistema de informações para outro devem ser varridas por *software* de controle contra *software* malicioso na tentativa de detectar código malicioso, incluindo vírus, vermes (*worms*), *spywares*, *malwares*, *adwares*, Cavalos de Tróia, etc. Todos os servidores e estações devem ter sistemas de controle contra *software* malicioso, instalados e gerenciados centralmente. Deve haver atualização automática das definições de assinaturas. Procedimentos devem ser desenvolvidos para atribuir responsabilidades quanto à resposta e recuperação de ataques baseados em código malicioso.

H) **Criptografia:** Criptografia é utilizada para garantir que informações não possam ser lidas ou modificadas por usuários não autorizados. Quando utilizada adequadamente, a criptografia protegerá a confidencialidade e integridade das informações durante transmissão e armazenamento, e poderá ser utilizada para autenticação e não repúdio. A criptografia pode ser implementada em dispositivos como roteadores, *switches*, *firewalls*, servidores e estações de trabalho. Os dispositivos devem implementar o nível de criptografia necessário para informações que irão trafegar na interconexão. Se necessário, mecanismos de criptografia (assinaturas digitais ou certificados pessoais, por exemplo) para autenticar usuários durante a interconexão e compartilhamento de aplicações, e também para prover não repúdio devem ser implementados.

I) **Segurança física e ambiental:** A segurança física objetiva a proteção física de recursos de TI. *hardware* e *software* que suportarão a interconexão, incluindo pontos de interconexão, deverão ser instalados em locais seguros e protegidos contra acesso não autorizado, interferência e danificação. Controles ambientais deverão ser instalados para proteger os ativos contra fogo, água, calor e/ou umidade excessiva. Adicionalmente, estações de trabalho deverão estar em áreas seguras contra danos, perda, furto ou acesso físico não autorizado. Deverá ser considerada a utilização de crachás, cartões eletrônicos de acesso ou dispositivos biométricos para controlar o acesso a essas áreas.

J) **Instalação ou configuração de *Hardware* e *Software*:** Depois da instalação ou configuração de controles de segurança, ainda pode ser necessário instalar *hardware* e *software* para estabelecer a interconexão, ou configurar *hardware* e

softwares já existentes com este objetivo.

K) **VPN:** *Virtual Private Network* – Podem ser implementadas de diversas maneiras, através de recursos de *software* e *hardware*. Garantem a confidencialidade durante transmissões através de redes públicas.

L) **Roteadores e *Switches*:** Estão sob responsabilidade da contratada vencedora da licitação da Rede Governamental.

M) **Integração de aplicações:** Integração de aplicações através de serviços fornecidos através da interconexão. Exemplos incluem aplicações de banco de dados, correio eletrônico, web *browsers*, servidores de aplicação, servidores de autenticação, controladores de domínio, ferramentas de desenvolvimento e programas de comunicação, entre outros.

N) **Testes de operacionalidade e de segurança:** Testes devem ser conduzidos para garantir que os equipamentos funcionarão adequadamente e que os recursos de segurança serão efetivos. Devem ser realizados testes de interoperabilidade entre as aplicações e o tráfego devendo ser simulado de forma que os testes de segurança sejam realizados em um ambiente próximo ao de produção. Todos os testes devem ser documentados e comparados com as expectativas dos participantes da interconexão. Neste momento, erros devem ser corrigidos e todas as ações tomadas devem ser documentadas.

O) **Levantamento de riscos** Um levantamento de riscos deve ser realizado para identificar vulnerabilidades e ameaças quanto à interconexão e para determinar o nível de risco correspondente. O levantamento deve ser realizado por terceiros, devidamente credenciados para isso. Os controles de segurança devem ser ajustados para diminuir os riscos identificados, e se necessário, controles adicionais devem ser implementados. Todas as ações corretivas devem ser documentadas.

P) **Treinamento e conscientização sobre segurança:** Treinamento e conscientização sobre segurança devem ser fornecidos a todo pessoal envolvido no gerenciamento, uso e operação da interconexão. Regras de comportamento devem ser distribuídas para todos os usuários que irão utilizar a interconexão, juntamente com um termo de reconhecimento que deve ser devolvido assinado. Usuários devem ser instruídos de como proceder para relatar atividades suspeitas ou proibidas, e de como solicitar assistência ou suporte se encontrarem problemas.

5.4.3 Ativação da interconexão: A ativação da interconexão deverá ocorrer assim que todas as partes envolvidas cumprirem com as recomendações deste documento e com o disposto no ASI.

6. Manutenção da Interconexão

Depois do estabelecimento de uma interconexão, a manutenção deve ser constante para garantir operação correta e segura. Esta seção descreve as atividades recomendadas para manter uma interconexão.

6.1 Comunicação

É de grande importância que os órgãos/entidades envolvidos mantenham procedimentos claros de comunicação e que colaborem regularmente. Linhas de comunicação bem definidas garantem que a interconexão é devidamente mantida e que os controles de segurança permanecerão efetivos.

Procedimentos claros também facilitam mudanças nas atividades de gerenciamento, tornando mais fácil para os órgãos/entidades envolvidos notificar quando ocorrerem mudanças planejadas nos sistemas que podem afetar a interconexão. Permite também que os órgãos/unidades envolvidos notifiquem-se mutuamente quando da ocorrência de incidentes de segurança e problemas estruturais, permitindo a condução de respostas coordenadas, se necessário. Comunicações devem ser conduzidas entre pessoal designado utilizando procedimentos aprovados, como especificado no ASI. As informações que devem ser compartilhadas incluem as seguintes:

6.1.1 Acordos iniciais e mudanças nos acordos
6.1.2 Alterações na gerência e pessoal técnico
6.1.3 Atividades relacionadas para estabelecer e manter a interconexão
6.1.4 Alterar as atividades de gerenciamento que podem afetar a interconexão
6.1.5 Incidentes de segurança que podem afetar os sistemas conectados e também os dados
6.1.6 Desastres e outras contingências que podem afetar os sistemas interconectados
6.1.7 Encerramento da interconexão
6.1.8 Restabelecimento planejado da interconexão

As informações podem ser trocadas verbalmente ou em forma escrita, dependendo de sua natureza. Atividades que alterem, modifiquem ou ajustem qualquer sistema dos órgãos/entidades envolvidos devem ser comunicadas obrigatoriamente de forma escrita.

6.2 Manutenção de equipamentos

Os órgãos/entidades devem acordar sobre quem irá manter os equipamentos utilizados para operar a interconexão, para garantir sua contínua integridade e disponibilidade. Os equipamentos devem ser mantidos em intervalos regulares e de acordo com as especificações do fabricante. Apenas pessoal autorizado deve ter autorização para realizar operações de manutenção e reparo. Todas as atividades de manutenção e ações corretivas devem ser documentadas, e os registros devem ser armazenados em local seguro. Os órgãos/entidades devem notificar-se mutuamente antes de realizar atividades de manutenção, incluindo

paradas programadas.

6.3 Gerenciamento de usuários

Os órgãos/entidades envolvidos na interconexão devem gerenciar ativamente os usuários dos serviços. Se um usuário é promovido ou sofre mudanças de responsabilidades, a organização responsável deverá atualizar o perfil do usuário para evitar acesso a dados ou informações que não são mais apropriadas. Procedimentos devem ser estabelecidos para investigar, desabilitar e terminar o acesso para usuários que não acessarem a interconexão ativamente por um determinado período de tempo. Privilégios para usuários que não acessem a interconexão depois de um período de tempo predeterminado devem ser suspensos. Estas medidas auxiliam no processo de prevenção contra intrusos que tentem explorar contas inativas.

6.4 Revisões de segurança

Uma ou todos os órgãos/entidades envolvidos na interconexão devem rever os controles de segurança envolvidos ao menos uma vez por ano ou quando uma mudança significativa ocorrer, garantindo a operação adequada e mantendo níveis apropriados de proteção. Uma grande variedade de ferramentas de segurança estão disponíveis comercialmente, devendo ser utilizados *firewalls* e outros controles para identificar riscos administrativos e vulnerabilidades de configuração e outros riscos de segurança. Testes de invasão também devem ser conduzidos.

Revisões de segurança devem ser conduzidas por profissionais designados pela Administração de Segurança de TI Estadual, ou por uma organização independente indicada por uma das partes. Os órgãos/entidades envolvidos devem acordar com o rigor e freqüência destas revisões e também quanto aos relatórios. Por exemplo, todos os envolvidos devem examinar os resultados das revisões de segurança para identificar áreas que requeiram atenção. Riscos à segurança devem ser minimizados o mais rápido possível. Ações corretivas devem ser documentadas, e os registros armazenados em local seguro.

6.5 Análise de registros (logs) de auditoria

Os órgãos/entidades envolvidos na interconexão devem analisar logs de auditoria em intervalos predeterminados para detectar e acompanhar atividades suspeitas e/ou fora dos padrões, podendo indicar intrusões ou má utilização interna. Dado o grande volume de informação contida em logs de auditoria, deve-se mantê-los em um tamanho adequado para gerenciamento. Ferramentas automáticas devem ser utilizadas para procurar anomalias, padrões desconhecidos, assinaturas de ataques conhecidos, alertando administradores de sistema se uma ameaça for detectada. Adicionalmente, um administrador de sistemas com experiência (ou mais de um, se a segregação de tarefas for aplicada) deverá periodicamente revisar os logs para tentar detectar atividades suspeitas que ferramentas automatizadas podem não reconhecer. Logs de auditoria devem ser mantidos por período aprovados por todas as partes envolvidas na conexão.

6.6 Resposta a incidentes de segurança

Todos os órgãos/entidades envolvidos devem notificar-se mutuamente em caso de intrusão, ataques ou mau uso interno, garantindo que as partes possam determinar se seus sistemas foram comprometidos. Os órgãos/entidades devem tomar as medidas necessárias para isolar e responder a tais incidentes, de acordo com seus respectivos procedimentos de resposta à incidentes.

As ações que podem ser tomadas incluem desligar computadores, desabilitar contas, reconfigurar roteadores e *firewalls*, ou desligar um sistema. Se o incidente envolve pessoal de todas as organizações envolvidas na interconexão, ações disciplinares são indispensáveis. Em alguns casos, representantes dos órgãos/entidades envolvidos deverão coordenar as atividades de resposta à incidentes, especialmente se danos maiores a segurança ocorrerem.

Se o incidente for um ataque ou um tentativa de intrusão, as autoridades apropriadas devem ser notificadas, e todas as tentativas devem ser feitas para preservar as evidências. Todos os incidentes de segurança, juntamente com os relatórios e as medidas de reposta tomadas, devem ser documentados.

6.7 Plano de contingência

Os órgãos/entidades envolvidos devem coordenar treinamentos de planejamento de contingência, testar e exercitar para minimizar o impacto de desastres e outras contingências que podem danificar sistemas conectados ou comprometer a confidencialidade e integridade de dados compartilhados. Atenção especial deverá ser dada para notificação e alerta de emergência, avaliação de danos e resposta e recuperação, incluindo recuperação de dados.

Os órgãos/entidades devem desenvolver procedimentos conjuntos baseados em planos de contingência já existentes. As organizações devem notificar-se mutuamente sobre alterações, baseando-se no esquema de primário e alternativo, incluindo alterações de coordenação, endereços, telefones, fax e endereços de *e-mail.*

6.8 Gerenciamento de mudanças

O gerenciamento de mudanças é fundamental para garantir que a interconexão está funcionando adequadamente e seguramente. Cada órgão/entidade envolvida deverá estabelecer uma equipe de controle de mudanças, ou algo de função similar, para revisar e aprovar mudanças planejadas para seus respectivos sistemas, tais como atualização de *software* ou adição de serviços.

A decisão para atualizar ou modificar um sistema deverá ser baseada nos requerimentos de segurança especificados no ASI e na determinação de que a alteração não irá afetar prejudicialmente a interconexão. Sempre que possível, mudanças planejadas deverão ser testadas em um ambiente isolado, fora de produção, para evitar que afetem os sistemas de TI em funcionamento.

Depois de aprovar uma mudança, a ECM ou similar, deverá ser responsável por gerenciar e acompanhar as mudanças para garantir que não haverá danos para interconexão, seja por corromper serviços ou por introduzir vulnerabilidades.

Na maioria dos casos, tais mudanças são projetadas para melhorar a operação e a segurança da interconexão, com a adição de novas funções, aperfeiçoamento de interfaces de usuários, redução ou eliminação de vulnerabilidades conhecidas. Não obstante, é crítico que os órgãos/entidades envolvidos na interconexão revejam cuidadosamente as alterações antes de implementá-las, além de gerenciar e acompanhar as mudanças depois de realizadas. Quaisquer vulnerabilidades ou problemas devem ser corrigidos o mais rápido possível.

6.9 Manutenção de Planos de Segurança de Sistemas

Os órgãos/entidades/fornecedores envolvidos na interconexão deverão atualizar seus planos de segurança de sistemas e outras documentações relevantes, pelo menos uma vez por mês ou sempre que uma mudança significativa ocorrer em seus sistemas de TI ou na interconexão.

7. Término da Interconexão

Esta seção descreve o processo para finalizar uma interconexão de sistemas. Se possível, a interconexão deverá ser finalizada causando a menor disfunção possível entre as partes envolvidas.

7.1 Desconexão planejada

A decisão para finalizar a interconexão deverá ser tomada pelo proprietário do sistema com o assessoramento de sua equipe técnica e gerencial. Antes de finalizar a interconexão, a parte que tomou a iniciativa deverá notificar a todos os envolvidos por escrito, e deverá aguardar o recebimento do reconhecimento por escrito. A notificação deverá descrever as razões para desconexão, a janela de tempo, além de identificar a equipe técnica e gerencial que irá conduzi-la.

Os órgãos/entidades envolvidos na interconexão podem finalizá-la por uma variedade de razões, incluindo:

A) Mudanças das necessidades de comunicação;
B) Falha nas auditorias de segurança, incluindo aumento nos riscos que cheguem a níveis inaceitáveis;
C) Impossibilidade de atender as especificações técnicas do ASI;
D) Impossibilidade de atender aos termos e condições do ME;
E) Considerações que envolvam custos, incluindo os custos de manter a interconexão;
F) Mudanças de configuração de sistemas ou de localização física de equipamentos e recursos.

O agendamento para finalização da interconexão deverá permitir um adequado

período de planejamento para que todos os envolvidos possam realizar os ~~as~~ preparativos apropriados, incluindo notificação de usuários afetados e identificação de recursos alternativos para manter serviços necessários. Adicionalmente, as equipes técnicas e de gerenciamento de todos os envolvidos deverão coordenar a logística da desconexão e a disposição dos dados compartilhados, incluindo a destruição ou sobrescrita de dados sensíveis.

A desconexão deverá ser conduzida quando o impacto para os usuários for mínimo, baseando-se em padrões de atividade conhecidos. Após a desconexão, cada órgão/entidade/fornecedor envolvido deverá atualizar seus sistemas, planos e documentos relacionados, para que reflitam o ambiente e o grau de segurança em que os respectivos sistemas operam.

7.2 Desconexão de emergência

Se os órgãos/entidades/fornecedores detectarem um ataque, tentativa de intrusão, ou outra contingência que explore uma vulnerabilidade ou coloque em situação de perigo sistemas e dados, pode ser necessário abruptamente finalizar a interconexão sem fornecer notificação escrita às outras partes. Esta medida extraordinária deverá ser utilizada apenas em circunstâncias extremas e após consulta à equipe técnica e com autorização da gerência de TI. A decisão de realizar uma desconexão de emergência deverá ser realizada pelo proprietário do sistema e implementada por sua equipe técnica. Se o proprietário do sistema não estiver acessível, um membro da equipe técnica pode autorizar a desconexão, de acordo com critérios escritos que estipulem as condições para o exercício desta autoridade.

7.3 Restabelecimento da Interconexão

Os órgãos/entidades/fornecedores podem optar por restabelecer a interconexão após o término. A decisão de restabelecer a interconexão deverá ser baseada na causa e duração da desconexão. Por exemplo, se a interconexão foi terminada por causa de um ataque, intrusão ou outra contingência, as partes envolvidas deverão implementar medidas para prevenir a ocorrência de novos incidentes. Devem também modificar o ASI e o ME para endereçar pontos que mereçam atenção. Alternativamente, se a interconexão foi terminada a mais de 90 dias, cada participante deverá realizar um levantamento de riscos em seus respectivos sistemas, reexaminando todos os pontos relevantes, incluindo o desenvolvimento de um novo ASI e de um novo ME.

8. Propriedade

Este material é de propriedade do Governo do Estado do Ceará, e mantido pela CGETI.

ANEXO A

ACORDO DE SEGURANÇA DA INTERCONEXÃO

Os órgãos/entidades estaduais e terceiros que operarão a interconexão de seus sistemas de informação deverão estabelecer um ASI - Acordo de Segurança da Interconexão para documentar os requisitos técnicos do processo. Um ASI é complementar ao ME - Memorando de Entendimento, que também será estabelecido entre os participantes da interconexão. Neste anexo encontra-se um guia para o desenvolvimento do ASI, e no final deste, um exemplo de ASI.

A.1 Objetivo

O objetivo do ASI é documentar e formalizar o processo de interconexão entre dois ou mais órgãos/entidades estaduais e terceiros e também para especificar os detalhes que serão necessários para prover salvaguardas de segurança aos sistemas que serão interconectados. Um guia genérico de elaboração de um ASI é fornecido neste documento, mas os termos do acordo podem ser ajustados em consenso entre os órgãos/entidades estaduais e terceiros envolvidos no processo.

Sistemas de informação de propriedade de órgãos/entidades estaduais, de outros governos, instituições civis e militares, e de empresas comerciais só deverão ser utilizados para transações envolvendo informações em uma interconexão depois que um ASI seja aprovado e devidamente assinado pelos representantes de cada organização envolvida.

Sistemas aprovados através deste ASI para interconexão entre duas ou mais organizações deverão alcançar ou superar os requisitos de segurança implementados pelo órgão/entidade com maior nível de exigência de segurança e seguir as recomendações contidas neste documento.

A.2 Referências

Como referência, deve ser utilizado a Política de Interconexão de Recursos de TI.

A.3 Abrangência

Estes procedimentos são efetivos nas seguintes fases do Ciclo de Vida de Desenvolvimento de Sistemas (CVDS):

Conceituação		Implantação	**X**
Projeto		Operação	**X**
Desenvolvimento	**X**	Desativação	**X**

A.4 Procedimentos

O ASI é utilizado para complementar o ME no estabelecimento dos requisitos para interconexão de redes e/ou sistemas entre duas ou mais organizações. O ME é utilizado para documentar os requisitos do ponto de vista administrativo e/ou de negócios entre as organizações. O ME não deverá incluir detalhes técnicos sobre como a interconexão será estabelecida, que é função do ASI. O ASI é um documento que delineia a solução técnica e os requisitos de segurança para interconexão. Ele não substitui um ME. Se um ME é atualizado, o ASI deve ser verificado para que reflita os novos requisitos.

Um ASI deverá ser assinado pelos representantes dos órgãos/entidades e/ou terceiros envolvidos, cujos nomes e cargos aparecem na Seção 4 do acordo (ver documento exemplo a seguir). O documento deverá ser formalmente assinado antes da interconexão ser declarada operacional.

A.5 Conteúdo de Acordo de Segurança da Interconexão (ASI)

Um ASI deverá possuir uma capa seguida de um documento com quatro seções numeradas. A informação disposta nessas quatro seções abrange as necessidades para interconexão e os controles de segurança necessários para proteger e garantir a confidencialidade, integridade e disponibilidade de sistemas e informações. A quantidade de informação deverá ser suficiente para que as equipes envolvidas possam tomar decisões prudentes sobre a aprovação da interconexão dos sistemas. As quatro seções são as seguintes:

- Seção 1: Requisitos de Interconexão
- Seção 2: Considerações sobre segurança de sistemas
- Seção 3: Diagrama topológico
- Seção 4: Assinaturas

Torna-se difícil definir as considerações de segurança que devem ser documentadas sem que haja um detalhado conhecimento de cada sistema que será conectado. Os itens da seção 2 deverão ser incluídos através de mútuo consenso entre as equipes envolvidas.
Um sistema pode ter vários requisitos de segurança que devem ser documentados e que podem não se aplicar ao outro sistema. Os representantes técnicos de cada organização devem discutir e formalizar estes requisitos no ASI.

A.6 Seção 1: Requisitos de Interconexão

Utilize esta seção para documentar o requerimento formal para interconectar os dois sistemas. Explique a razão da interconexão, justificando-a em no máximo dois parágrafos. Inclua as seguintes informações:

- Os benefícios que serão alcançados;
- Os nomes dos sistemas que serão interconectados;
- O órgão/entidade que iniciou o processo. Se o requerimento for

originado em um órgão/entidade de nível hierárquico maior, indique o nome da organização e, se for apropriado, o nome do responsável que requisitou a interconexão.

A.7 Seção 2: Considerações sobre segurança de sistemas

Utilize esta seção para documentar os recursos de segurança que serão utilizados para proteger a confidencialidade, integridade e disponibilidade dos dados e sistemas que serão interconectados. O representante técnico de cada organização deverá discutir o conteúdo desta seção para chegar a um acordo mútuo sobre os itens a serem incluídos. Os órgãos/entidades deverão responder a cada item, mesmo se apenas uma das partes é afetada pelo item em questão. Note que alguns itens são recomendados, outros são opcionais. Itens opcionais que afetem apenas um sistema devem ser respondidos e incluídos.

Itens Sugeridos: (Não inclua este título “Itens Sugeridos” no ASI) Os seguintes itens devem ser abordados no ASI:

- *Informações gerais / Descrição dos dados*: Descreve as informações e os dados que serão disponibilizados, trocados ou transferidos através da interconexão de dois ou mais sistemas.

- *Serviços oferecidos*: Descreve a natureza dos serviços de informação (por exemplo, correio eletrônico [*e-mail*], protocolo de transferência de arquivos [FTP], consulta de banco de dados [*database query*], consulta de arquivos [file *query* / *browser*], outros serviços computacionais diversos) oferecidos através da interconexão para cada órgão/entidade e/ou terceiro envolvido.

- *Sensibilidade dos dados*: Determine o nível de sensibilidade da informação que será manipulada através da interconexão, incluindo o maior nível de sensibilidade envolvido e as medidas de proteção mais restritivas necessárias.

- *Comunidade de Usuários*: Descreva a “comunidade de usuários” que serão servidos pela interconexão, incluindo seus níveis de acesso aprovados e o menor nível de aprovação para quem irá acessar a interconexão. Também devem ser estipulados requisitos de investigação de antecedentes, se for apropriado.

- *Informação sobre troca de dados*: Descreva todos os serviços técnicos de segurança pertinentes a troca segura de dados entre os sistemas interconectados.

- *Regras de comportamento*: Relacione as expectativas de comportamento para os usuários que irão ter acesso através da interconexão. Cada participante deverá proteger informações que pertençam aos outros participantes, através da implementação de controles de segurança que protejam contra intrusão, forjamento, vírus, entre outros. Não insira aqui indicações relativas a leis e políticas. Estas indicações são normalmente realizadas no ME.

- *Política de segurança formal*: Especifique, se houverem, as políticas de segurança que governam cada sistema. Por exemplo: “Política de Controles Contra Software Malicioso” para “SEAD”.

- *Relato de Incidentes*: Descreva aqui os acordos que regem a comunicação e as respostas para incidentes de segurança da informação para as organizações envolvidas. Por exemplo, “cada órgão/entidade deverá comunicar incidentes de acordo com seus procedimentos internos.”. Se a comunicação de incidentes não for acordada, indique aqui.

- Responsabilidades por trilhas de auditoria: Descreva como a responsabilidade por auditar trilhas de auditoria (logs) será dividida entre os envolvidos e quais eventos cada organização será responsável por registrar. Especifique a quantidade de tempo de retenção dos registros. Se nenhum tipo de registro for realizado, indique aqui.

Outros itens: (Não inclua o título “Outros itens” no ASI) Se os representantes técnicos determinarem que algum dos itens abaixo é “não aplicável”, uma referência deve ser feita no ASI em lugar de eliminar o item. Por exemplo, se não houver conectividade discada (*dialup*), o item apropriado será “Capacidade de conexão via linha discada não será utilizada por nenhum dos sistemas interconectados”.

- *Parâmetros de segurança*: Especifique os parâmetros de segurança trocados entre sistemas para autenticar que o sistema requisitador é legítimo e que os serviços requisitados são permitidos pelo ASI. Por exemplo, ao nível de sistemas, se um novo serviço como *e-mail* é requisitado sem coordenação anterior, deverá se detectado, recusado e documentado como possível tentativa de intrusão até que o serviço de interconexão seja autorizado. Também, parâmetros adicionais de segurança podem ser requisitados (por exemplo, monitoramento de usuários) para permitir que um sistema determine se outro sistema requisitador está autorizado a receber informações e/ou serviços e se todos os detalhes da transação atendem ao escopo de serviços autorizados no ASI.

- *Modo de segurança operacional*: Se as partes envolvidas utilizam o conceito de Níveis de Proteção ou de Níveis de Interesse para Confidencialidade, Integridade e Disponibilidade, baseados em critérios comuns de implementação, forneça aqui os valores documentados para os sistemas. Opcionalmente, o modo de segurança das operações deve ser documentado para todos os sistemas envolvidos.

- *Treinamento e conscientização*: Descreva os detalhes de qualquer treinamento de segurança novo ou adicional que sejam necessários, e a designação de responsabilidades pela condução do treinamento e conscientização durante o ciclo de vida da interconexão.

- *Restrições de equipamentos específicos*: Descreva qualquer restrição nova ou revisada a ser colocada em terminais, incluindo o seu uso, localização e acesso

físico.

- *Conectividade através de linha discada ou banda-larga*: Descreva qualquer consideração especial para conexões discadas ou de banda larga para qualquer sistema na interconexão proposta, incluindo riscos de segurança e salvaguardas utilizadas para reduzir esses riscos.

- *Documentação de segurança*: Descreva o título e detalhes gerais de cada plano de segurança de sistema das organizações envolvidas na interconexão, incluindo a designação de responsabilidades pelo desenvolvimento e aceitação do plano, assim como qualquer outro documento relevante.

Seção 3: Diagramas topológicos

O ASI deverá incluir diagramas topológicos ilustrando a interconectividade de um sistema para outro. O diagrama deverá incluir:

- O título "SEÇÃO 3: DIAGRAMA TOPOLÓGICO"

- Todos os recursos de comunicação, circuitos e outros componentes utilizados para interconexão, entre as organizações envolvidas.

- O diagrama deverá representar a localização lógica de todos os componentes (por exemplos, *firewalls*, roteadores, *switches, hubs, servers*, dispositivos de criptografia, estações de trabalho, e outros dispositivos de segurança, como IDSs).

- Se necessário, sinalize no cabeçalho e rodapé de cada página com os requisitos de manipulação apropriados, como "APENAS PARA USO OFICIAL" ou "APENAS PARA USO INTERNO".

Seção 4: Assinaturas

O ASI deverá incluir linhas para assinatura. Opcionalmente, esta seção deverá incluir qualquer procedimento que os representantes das organizações considerem necessários para finalizar o ASI. Esta seção pode incluir os seguintes itens:

- A data de expiração do acordo;
- Requisitos de revisões periódicas, especificando a data da próxima revisão;
- Outros procedimentos requeridos pelas organizações envolvidas;
- As assinaturas dos representantes de cada organização, e a data dessas assinaturas.

APENAS PARA USO OFICIAL

ACORDO DE SEGURANÇA DE INTERCONEXÃO

Entre “Organização A e Organização B”

[Selos, logos ou brasões das organizações aqui]

EXEMPLO

[data]

[Organização “A” Organização “B”]

APENAS PARA USO OFICIAL

Figura A1. Capa exemplo de um ASI

APENAS PARA USO OFICIAL

ACORDO DE SEGURANÇA DE INTERCONEXÃO

SEÇÃO 1: REQUISITOS DE INTERCONEXÃO

Os requisitos para interconexão entre “Organização A” e “Organização B” são para o propósito de troca de dados entre o “Sistema A”, de propriedade da “Organização A”, e o “Sistema B”, de propriedade da “Organização B”. Organização B requisita a utilização da base de dados XYZ da Organização A, e a Organização A requisita a utilização da base de dados ABC da Organização B, como aprovado pelos respectivos coordenadores através do convênio, respectivamente. O benefício que se espera alcançar é a viabilização do “Projeto X”.

SEÇÃO 2: CONSIDERAÇÕES SOBRE SEGURANÇA DOS SISTEMAS

2.1 Informações gerais / Descrição dos dados

A interconexão entre o Sistema A, de propriedade da Organização A, e o Sistema B, de propriedade da Organização B, é bidirecional. O objetivo da interconexão é permitir que a base de dados XYZ seja acessada pelo Departamento de Análise de Dados da Organização B, e para permitir o acesso à base de dados ABC pelo Departamento de Pesquisas da Organização A.

2.2 Serviços oferecidos

Não serão oferecidos serviços a usuários. Esta interconexão apenas permite a troca de dados entre o sistema da Organização A e o sistema da Organização B, através da Rede Governamental.

2.3 Sensibilidade dos dados

A sensibilidade dos dados trocados entre a Organização A e a Organização B é “não classificada”, por tratarem-se de dados públicos.

2.4 Comunidade de usuários

Todos os usuários da Organização A que acessarão os dados recebidos da Organização B são cidadãos brasileiros, com credenciais válidas e investigadas pela Organização A.

Todos os usuários da Organização B que acessarão os dados recebidos da Organização A são cidadãos brasileiros, com credenciais válidas e investigadas pela Organização B.

2.5 Segurança para troca de informações

A segurança da informação trafegada através desta interconexão é protegida por mecanismos de criptografia. Os pontos finais de cada lado estão posicionados em locais com acesso controlado, guarnecidos 24 horas por dia. Usuários individuais não tem acesso aos dados exceto através de seus sistemas de segurança, inerentes ao sistema operacional e as aplicações. Todo acesso é controlado por métodos de autenticação para validar usuários aprovados.

2.6 Expectativas de Comportamento

Espera-se que usuários e sistemas da Organização A protejam a base de dados ABC da Organização B, e que usuários e sistemas da Organização B protejam a base de dados XYZ da Organização A, de acordo com os decretos estaduais XXXX e XXXX que regulamentam o acesso não autorizado no âmbito da Rede Governamental.

2.7 Política de segurança formal

As políticas de segurança que governam a proteção dos dados trocados são a “Política XXX” da Organização A, e a “Política YYY” da Organização B.

2.8 Relato de Incidentes

A parte da interconexão que detectar um incidente de segurança deverá relatá-lo as outras partes envolvidas de acordo com seus procedimentos de relato de incidentes. No caso da Organização B, qualquer incidente de segurança será relatado para a Equipe de Resposta a Incidentes de Segurança Computacional . A política que governa o relato e tratamento de incidentes é a “Política de Resposta a Incidentes de Segurança Computacional”.

2.10 Responsabilidades por trilhas de auditoria

Ambas as partes são responsáveis por auditar processos de aplicação e atividades de usuários envolvendo a interconexão. As atividades que serão registradas incluem tipo do evento, data e hora do evento, identificação do usuário, identificação da estação de trabalho, sucesso e falha de tentativas de acesso, ações de segurança tomadas por administradores de sistema ou gerentes/analistas de segurança. Registros de auditoria serão mantidos por 3 (três) meses.

SEÇÃO 3: DIAGRAMA TOPOLÓGICO

[INSERIR DIAGRAMA AQUI]

SEÇÃO 4: ASSINATURAS

Este ASI é válido por 1 (um) ano após a última data de assinatura abaixo. Ao completar um ano, deverá ser atualizado, revisado e reautorizado. Qualquer uma das partes pode finalizar este acordo, por escrito, notificando com antecedência mínima de 30 (trinta) dias. Admite-se a falta de aviso prévio no caso de ocorrência de um incidente de segurança que necessite de uma resposta imediata.

(Representante autorizado da Org. A)	(Representante autorizado da Org. B)
---	---
(Assinatura / Data)	(Assinatura / Data)

ANEXO B

Memorando de Entendimento

Os órgãos/entidades que operam sistemas interconectados devem estabelecer um Memorando de Entendimento - ME que defina as responsabilidades de todas as partes envolvidas no estabelecimento, operação e segurança da interconexão. Este documento de gerenciamento não deverá conter detalhes técnicos da interconexão planejada. Estes detalhes deverão estar documentados separadamente no ASI - Acordo de Segurança para Interconexão (ver apêndice A). Um guia para o desenvolvimento de ME é fornecido a seguir, podendo ser modificado de acordo com as necessidades dos órgãos/entidades envolvidos.

B.1 Superação

Identificar qualquer acordo prévio que este memorando supere, incluindo títulos dos documentos e datas. Se o memorando não supera nenhum acordo anterior, seguir para o próximo item.

B.2 Introdução

Utilize esta seção para descrever o objetivo do memorando. Um exemplo é fornecido em anexo. Identifique os órgãos/entidades que estão envolvidos na interconexão.

B.3 Autoridades

Identifique qualquer referência a leis, regulamentos, agências ou políticas nas quais o ME é baseado ou referendado.

B.4 Cenário

Utilize esta seção para descrever os sistemas de TI que serão conectados; os dados que serão compartilhados, trocados ou trafegados através da interconexão; e os objetivos e benefícios esperados. A descrição dos sistemas deverá ser breve e não técnica. O objetivo é identificar os sistemas e seus limites. O memorando não deverá conter especificações dos sistemas. Esta seção deverá incluir o nome formal de cada sistema e uma breve descrição de suas funções, identificando suas localizações físicas, sua sensibilidade ou nível de classificação; e identificando os tipos de dados que são armazenados, processados e transmitidos.

B.5 Comunicações

Discute as comunicações que serão trocadas entre as partes durante a interconexão. Identifica eventos específicos em que as partes deverão trocar

notificações formais, e discute a natureza das comunicações.

B.6 Acordo de Segurança para Interconexão - ASI

Notifica que as partes deverão desenvolver em conjunto e firmar um ASI antes dos sistemas serem interconectados. Adicionalmente, descreve o propósito de um ASI.

B.7 Segurança

Notifica que as partes devem concordar em seguir as soluções de segurança especificadas no ASI. Adicionalmente, notifica que as partes devem certificar que seus respectivos sistemas estão de acordo, são operados e foram projetados em conformidade com leis federais, estaduais, regulamentos e respectivas políticas de segurança.

B.8 Custos

Esta seção fornece detalhes financeiros do acordo. Especifica quem deverá arcar com os custos específicos da interconexão e em que condições os dispêndios financeiros devem ser realizados. Normalmente, cada organização é responsável pelos equipamentos e outros recursos necessários para interconectar seu sistema local.

B.9 Prazos

Identifica a data de expiração do memorando e os procedimentos para sua reautorização. Adicionalmente, estipula que o memorando pode ser terminado com a notificação por escrito de uma das partes. O ME e o ASI devem ter a mesma data de expiração.

B.10 Assinaturas

O memorando deverá incluir campos para assinaturas de cada representante oficial designado para sua aprovação. Um campo data deve ser incluído para cada campo de assinatura.

APENAS PARA USO OFICIAL

MEMORANDO DE ENTEDIMENTO - ME

Entre “Organização A e Organização B”

[Selos, logos ou brasões das organizações aqui]

EXEMPLO

[data]

[Organização “A” Organização “B”]

APENAS PARA USO OFICIAL

Figura B1. Capa exemplo de um ASI

APENAS PARA USO OFICIAL

MEMORANDO DE ENTENDIMENTO - ME

Documentos superados: (Nome dos documentos e datas)

Introdução

O objetivo deste memorando é estabelecer um acordo entre a “Organização A” e a “Organização B” envolvendo o gerenciamento, operação e segurança de uma interconexão entre o “Sistema A”, de propriedade da Organização A, e o “Sistema B”, de propriedade da Organização B. Este acordo governará as relações entre a Organização A e a Organização B, incluindo as equipes designadas para serviços técnicos e gerenciais, abstendo-se de gerenciamento centralizado.

Autoridade

Este acordo é baseado no convênio xxxx-xx, que obedece às políticas estabelecidas que regulamentam a interconexão de sistemas no âmbito da rede governamental, datado de xx/xx/xx.

Cenário

A intenção das partes para firmar este acordo é a interconexão dos respectivos sistemas de TI para troca de dados entre as bases de dados ABC e XYZ. A Organização A requer a utilização da base de dados ABC, pertencente a Organização B, e a Organização B requer a utilização da base de dados XYZ, pertencente a Organização A, como aprovado pelos seus respectivos secretários. O benefício esperado após a interconexão é o de possibilitar o processamento dos dados necessários para viabilizar o “Projeto R”, dentro dos prazos especificados.

Os sistemas de TI envolvidos estão descritos a seguir:

Sistema A

- Nome
- Função
- Localização
- Descrição dos dados, incluindo sensibilidade ou nível de classificação

Sistema B

- Nome
- Função
- Localização
- Descrição dos dados, incluindo sensibilidade ou nível de classificação

Comunicações

Comunicações formais e freqüentes são essenciais para garantir o sucesso do gerenciamento e operação da interconexão. As partes concordam em manter linhas abertas de comunicação entre as respectivas equipes designadas tanto de nível técnico quanto gerencial.

Todas as comunicações descritas aqui devem ser conduzidas por escrito, a menos que especificado em contrário.

Os gestores do Sistema A e do Sistema B concordam em designar e a fornecer informações de contato para as lideranças técnicas de seus respectivos sistemas, e a facilitar contatos diretos entre lideranças técnicas que suportam o gerenciamento e operação da interconexão. Para salvaguardar a confidencialidade, integridade e disponibilidade dos sistemas conectados e os dados que eles armazenam, processam e transmitem, as partes concordam em fornecer informações sobre eventos específicos nos prazos indicados a seguir:

Incidentes de Segurança: A equipe técnica que detectar um incidente de segurança notificará imediatamente a equipe técnica da outra parte, por telefone ou *e-mail* o mais rápido possível, para que possa determinar se seu sistema foi comprometido e tome as precauções de segurança apropriadas. O gestor do sistema receberá uma notificação formal por escrito em até 5 dias úteis depois da detecção do incidente.

Desastres e outras contingências: Se uma das organizações sofrer algum tipo de desastre ou outra contingência que prejudique a operação normal de um ou de ambos os sistemas conectados, sua equipe técnica deverá imediatamente notificar a equipe técnica da outra parte, por telefone ou *e-mail*.

Alterações materiais na configuração do sistema: Mudanças planejadas que alterem a arquitetura do sistema devem ser comunicadas para a equipe técnica da outra parte antes que sejam implementadas. A parte que tomar a iniciativa deverá conduzir uma análise de riscos baseadas na nova arquitetura do sistema, além de modificar e reaprovar o ASI antes da implementação.

Novas interconexões: A parte que tomar a iniciativa deverá notificar a outra parte pelo menos um (1) mês antes de conectar seu sistema de TI com qualquer outro sistema de TI, incluindo sistemas de propriedade e operados por terceiros.

Alterações de pessoal: As partes concordam em fornecer notificação de saída ou ausência por um grande período de tempo dos seus respectivos gestores de sistemas ou lideranças técnicas. Adicionalmente, ambas as partes devem notificar mudanças no perfil de usuários, incluindo usuários que sofram alterações em suas responsabilidades de trabalho.

ACORDO DE SEGURANÇA PARA INTERCONEXÃO

Os detalhes técnicos da interconexão deverão ser documentados em um ASI - Acordo de Segurança para Interconexão. As partes concordam em trabalhar em conjunto para desenvolver o ASI, que deve ser assinado por ambas as partes antes da interconexão ser ativada. Alterações propostas nos sistemas ou no meio de interconexão deverão ser revisadas e avaliadas para determinar o impacto potencial em relação a interconexão.

SEGURANÇA

Ambas as partes concordam em trabalhar em conjunto para garantir a segurança dos sistemas conectados e dos dados que eles armazenam, processam e transmitem, como especificado no ASI. Cada parte certifica que seu respectivo sistema foi projetado, é gerenciado e operado em acordo com leis federais, regulamentos e políticas de segurança vigentes.

CUSTOS

Ambas as partes concordam em compartilhar os custos necessários para efetivar a interconexão. Qualquer modificação necessária para suportar a interconexão é de responsabilidade dos respectivos proprietários dos sistemas.

PRAZOS

Este acordo permanecerá válido por 1 (um) ano após a última data de assinatura. Depois de 1 (um) ano, este acordo expirará. Se as partes resolverem renovar este acordo, este deverá ser revisado, atualizado e reautorizado. O novo acordo deverá explicitamente superar este acordo, devendo ser referenciado por título e data. Se uma ou ambas as partes resolverem terminar este acordo antes do prazo, a intenção deverá ser comunicada com antecedência mínima de pelo menos 30 dias. Admite-se a falta de aviso prévio no caso de um incidente de segurança que necessite de uma resposta imediata.

(Representante autorizado da Org. A) (Representante autorizado da Org. B)

--- ---

(Assinatura / Data) (Assinatura / Data)

ANEXO C

O Anexo C é um guia para o desenvolvimento de um Plano de Implementação para Interconexão e é baseado no item 5.4.1 desta Política.

C.1 Introdução

Descreve o objetivo e escopo do Plano de Implementação, e identifica os requerimentos de políticas em que a interconexão é baseada. Identifica os sistemas de TI que serão interconectados, as organizações proprietárias e os propósitos para que são utilizados. Discute o propósito para interconectar os sistemas e descreve os serviços que serão oferecidos sob a interconexão. Brevemente descreve cada seção do documento.

C.2 Descrição da Interconexão

Descreve a arquitetura da interconexão, incluindo controles de segurança, *hardware*, *software*, servidores e aplicações. Deve ser incluído um diagrama da interconexão, mostrando todos os componentes relevantes.

C.2.1 Controles de Segurança

Identifica e descreve os controles de segurança ora em funcionamento para os ambientes de TI que serão interconectados. Identifica as ameaças que podem comprometer os ambientes interconectados e descreve como os controles de segurança existentes serão configurados para reduzir as ameaças. Identifica os novos controles que serão implementados, incluindo os controles em nível de rede e aplicação.

C.2.2 *Hardware*

Os equipamentos devem ser identificados, descrevendo como são utilizados nos sistemas que serão interconectados, e também como suportarão a interconexão. Identifique e descreva novos equipamentos que serão instalados como parte da interconexão, incluindo sua função.

C.2.3 *Software*

Software inclui os programas de aplicação, rotinas e sistemas operacionais associados com o ambiente de TI. Identifique e descreva o *software* utilizado atualmente nos sistemas que serão interconectados e descreva como serão utilizado durante a interconexão. Identifique novo software que será instalado como parte da interconexão, incluindo sua função.

C.2.4 Troca de dados/informação

Organizações conectam seus sistemas de TI para compartilhar dados, disponibilizá-los ou trafegá-los de uma organização para outra. Pode ser

necessário instalar uma base de dados que seja dedicada a interconexão. Identifique os tipos de dados que serão trocados entre as organizações, e descreva os métodos de transmissão que serão utilizados. Identifique como os dados serão armazenados e processados. Forneça um diagrama de fluxo de dados.

C.2.5 Aplicações e serviços

Descreva os serviços e aplicações que as organizações participantes irão fornecer sob a interconexão, e também como novos serviços ou aplicações serão desenvolvidos, agora e no futuro. Exemplos incluem *e-mail*, consultas a banco de dados, arquivos, serviços computacionais diversos, servidores de aplicação e autenticação.

C.3 Regras e responsabilidades

Identifique o pessoal quer irá estabelecer e manter a interconexão, e defina suas respectivas regras e responsabilidades. Uma grande variedade de especializações é necessária, incluindo um gerente de projeto, arquiteto de redes, especialista de segurança, administrador de sistema, administrador de rede, administrador de banco de dados, desenvolvedor e *design* gráfico. Equipes de todas as organizações envolvidas devem estar envolvidas. Identifique também as responsabilidades da equipe que será autorizada a utilizar a interconexão depois de estabelecida. As regras de comportamento deverão ser consultadas quando desenvolvendo esta seção.

C.4 Tarefas e procedimentos

Forneça uma abordagem passo-a-passo para estabelecer a interconexão, baseada em tarefas e procedimentos. Uma lista de tarefas são fornecidas a seguir. As organizações devem adaptá-las aos seus próprios requerimentos. Adicionalmente, forneça uma lista de verificação para cada tarefa para garantir sua execução adequada.

C.4.1 Implementação de Controles de Segurança

O processo de interconectar ambientes de TI geralmente abre uma organização para um grande número de vulnerabilidades de segurança. Conseqüentemente, o primeiro passo para os órgãos/entidades e/ou terceiros em processo de interconexão é o de implementar controles de segurança apropriados. Defina procedimentos para configurar os controles existentes, e, se necessário, implementar novos controles. Controles de segurança devem incluir *firewalls*, mecanismos de identificação e autenticação, controles de acesso lógico, dispositivos de criptografia, sistemas de detecção de intrusão e medidas de segurança física.

C.4.2 Instalação de *hardware* e *software*

Forneça procedimentos para configurar ou instalar *hardware* e *software* para estabelecer a interconexão, se necessário.

C.4.3 Integração de aplicações

Forneça procedimentos para conectar aplicações através da interconexão, se necessário. Também forneça procedimentos para desenvolver e implementar novas aplicações, se necessário.

C.4.4 Levantamento de Riscos

Descreva o processo para conduzir um levantamento para identificar riscos relativos a interconexão, ou referencie a metodologia existente na organização para levantamento de riscos. Discuta como os riscos serão abordados. Por exemplo, riscos podem ser reduzidos ajustando-se os controles de segurança ou pela implementação de medidas adicionais.

C.4.5 Condução de testes de operação e segurança

Forneça procedimentos de teste detalhados para verificar se a interconexão opera de maneira eficiente e segura. Descreva também como os resultados dos testes serão medidos, e como as deficiências serão abordadas.

C.4.6 Treinamento de Segurança e Conscientização

Descreva o programa de treinamento e conscientização para todo o pessoal que será autorizado a gerenciar, utilizar e/ou operar a interconexão, incluindo novas aplicações associadas com segurança. O treinamento deverá garantir que o pessoal autorizado conhece as regras de comportamento associadas como a interconexão e como devem requisitar assistência se encontrarem problemas. Adicionalmente, o pessoal que é responsável por manter a interconexão deverá receber treinamento especializado que garanta a proficiência na condução de suas responsabilidades.

C.5 Cronograma e orçamento

Estabeleça um cronograma para o estabelecimento da interconexão, incluindo o tempo estimado para completar cada tarefa. Defina também o orçamento para o projeto e descreva como os custos serão divididos entre os órgãos/entidades e/ou terceiros participantes, se necessário.

C.6 Documentação

Cite ou inclua toda documentação que seja relevante para o estabelecimento da interconexão, incluindo planos de sistemas de segurança, especificações de projeto e procedimentos operacionais padrão, se houverem.

ANEXO D

Fluxograma do processo de Interconexão

Caso 1: Interligação de um órgão a Rede Governamental para acesso à Internet
Caso 2: Interligação entre órgãos
Caso 3: Interligação entre um órgão e um fornecedor