Manual de Procedimentos da Operação

Módulo 5 - Submódulo 5.13

Rotina Operacional
Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético

Código	Revisão	Item	Vigência
RO-CB.BR.01	**00**	**4.1.11.**	**09/07/2021**

MOTIVO DA REVISÃO

- Emissão da RO-CB.BR.01 intitulada “Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético”.

LISTA DE DISTRIBUIÇÃO

CNOS	COSR-SE	COSR-NE	COSR-NCO	COSR-S
Agentes de Operação	-	-	-	-

Instrução de Operação	Código	Revisão	Item	Vigência
Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético	**RO-CB.BR.01**	**00**	**4.1.11.**	**09/07/2021**

ÍNDICE

Instrução de Operação	Código	Revisão	Item	Vigência
Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético	**RO-CB.BR.01**	**00**	**4.1.11.**	**09/07/2021**

1. OBJETIVO

Estabelecer os controles mínimos de segurança cibernética a serem implementados pelos agentes e pelo ONS no Ambiente Regulado Cibernético (ARCiber).

2. REFERÊNCIAS

Módulo 2.16 dos Procedimentos de Rede – Requisitos operacionais para centros de operação e instalações da rede de operação.

3. CONCEITOS

3.1. ARCiber – Ambiente Regulado Cibernético é o conjunto de redes e equipamentos que estão considerados no escopo desta Rotina Operacional. O ARCiber é composto por:

a) Centros de operação dos agentes;

b) Equipamentos que participam da infraestrutura de envio ou recebimento de dados e voz para ambientes operativos do ONS ou para centros de operação de outros agentes;

c) Ambiente operativo do ONS.

3.2. *Patch* – Atualização de *software* fornecida pelo fabricante que corrige falhas e vulnerabilidades.

3.3. MFA – Múltiplos Fatores de Autenticação. Técnica de autenticação que garante mais confiabilidade ao exigir que os usuários apresentem mais de uma confirmação. Fatores comumente usados incluem *tokens* OTP e dispositivos biométricos.

3.4. OTP – *One Time Password*. Método de autenticação de múltiplos fatores que se constitui de uma senha de uso único, que é válida somente para uma sessão de login ou transação.

3.5. VPN – *Virtual Private Network*. Conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados.

3.6. *Antimalware* – Ferramenta de *software* cujo objetivo é proteger o dispositivo contra infecções por vírus e outros *softwares* maliciosos.

3.7. *Ambiente Operativo do ONS* - Toda a infraestrutura computacional e de telecomunicações de Tempo Real e histórico, que atende à sala de controle e outras áreas interessadas do ONS, e que está protegida pelos Firewalls operativos.

3.8. *Incidente de Segurança Cibernética* - é composto por um ou mais eventos de segurança cibernética indesejados ou inesperados, que podem levar ao comprometimento dos ativos do ARCiber ou prejudicar as operações do ONS ou do agente.

Instrução de Operação	Código	Revisão	Item	Vigência
Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético	**RO-CB.BR.01**	**00**	**4.1.11.**	**09/07/2021**

4. CONSIDERAÇÕES GERAIS

4.1. ARQUITETURA TECNOLÓGICA PARA O AMBIENTE

4.1.1. As redes devem ser segregadas em zonas de segurança, de acordo com a sua função. O agente deve definir uma arquitetura que segmente as redes minimamente em:

a) Zona de Supervisão (nível 2 da norma ISA-95 e Purdue Reference Model);

b) Zona DMZ Operativa (nível 3 da norma ISA-95 e Purdue Reference Model);

c) Zona Corporativa (nível 4 da norma ISA-95 e Purdue Reference Model).

4.1.2. O ARCiber não deve ser diretamente acessível através da internet mesmo que protegido por um ou mais *firewalls*, bem como seus ativos:

a) Não devem ser visíveis nem ser acessíveis a partir da internet, exceto nos casos previstos em 4.1.3.

b) Não devem ser capazes de se conectar com a internet.

4.1.3. O acesso ao ARCiber a partir de redes externas à organização (como, por exemplo, a internet) somente deve ser permitido para o desempenho de atividades autorizadas. Este acesso deve ser realizado por meio de Rede Privada Virtual (VPN), ou tecnologia similar, através de um gateway ou serviço que ofereça controles de segurança.

4.1.4. Soluções *Antimalware* devem ser implementadas no ARCiber e mantidas atualizadas.

a) Soluções de *application whitelisting* podem ser implementadas como alternativa ou complemento às soluções *Antimalware*.

4.2. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

4.2.1. Deve ser nomeado pelo menos um gestor e um suplente, responsáveis pela segurança cibernética do ARCiber e atuar como ponto de contato externo.

4.2.2. Deve ser estabelecida política que defina papéis e responsabilidades em relação à segurança cibernética do ARCiber.

4.3. INVENTÁRIO DE ATIVOS

4.3.1. Todos os ativos, *softwares* e *hardwares*, conectados ao ARCiber devem ser inventariados minimamente a cada 24 meses e considerar minimamente:

a) Tipo de dispositivo;

b) Fabricante do equipamento;

c) Função;

d) Endereço IP ou *MAC Address*;

e) Protocolo de aplicação e/ou porta de serviço;

f) Versão do firmware e/ou sistema operacional quando aplicável.

4.3.2. O inventário dos ativos deve ser armazenado de forma segura, com políticas de armazenamento bem definidas, com acesso restrito às pessoas que necessitem das informações para o exercício de suas funções.

4.3.3. Padrões de configuração segura (*hardening*) devem ser criados conforme política de segurança do agente para os sistemas operacionais, *firmwares*, banco de dados e demais versões de *softwares* existentes no ARCiber:

a) Mecanismos de monitoramento da conformidade destes padrões no ARCiber produtivo, automatizados ou manuais, devem ser implementados.

4.4. GESTÃO DE VULNERABILIDADES

4.4.1. A política de segurança da organização deverá contemplar a gestão de pacotes de correção de segurança (patches) para todas as tecnologias conectadas ao ARCiber, contemplando no mínimo:

a) Cronograma de implementação das correções;

b) Mapeamento dos ativos inventariados para as atualizações disponibilizadas pelos fabricantes.

4.4.2. Novos ativos somente deverão ser conectados ao ARCiber após a aplicação de todos os pacotes de correção de segurança disponíveis.

a) Caso o novo equipamento esteja substituindo um equipamento existente que tenha apresentado defeito, a aplicação dos pacotes de correção de segurança poderá ser postergada, mas com prazo pré-definido.

4.5. GESTÃO DE ACESSOS

4.5.1. Deve existir uma política de gestão de acessos e identidades, que contemple minimamente os requisitos descritos a seguir.

4.5.1.1. Credenciais de acesso devem ser individuais e aprovadas pela alçada competente. Para os casos em que não seja possível implementar credenciais individuais, deve-se:

a) Gerar e manter uma lista das pessoas autorizadas a usar as contas compartilhadas.

b) Implementar os controles previstos em 4.5.1.6.

4.5.1.2. Política de senhas que contemple: tamanho mínimo, complexidade, necessidade de ser diferente da senha padrão do fabricante, ações a serem tomadas caso um número máximo de tentativas de acesso malsucedidas seja atingido, e critérios para a gestão de mudanças (prazo, ocorrência de incidentes, etc).

a) A política de senhas pode ser implementada por controles tecnológicos ou por procedimento. Caso as características de senha previstas na política não possam ser implementadas em

determinados ativos devido à restrição tecnológica, deve-se implementar o nível máximo suportado pelo ativo.

4.5.1.3. Na construção dos perfis de acesso deve-se seguir o princípio de minimização (somente deve-se conceder o acesso mínimo necessário).

4.5.1.4. Prazo máximo para cancelamento/remoção de credenciais de usuários desligados e de credenciais sem uso após um determinado tempo.

4.5.1.5. Credenciais de acesso privilegiadas devem estar sujeitas a controles específicos, incluindo:

a) Nível de aprovação adequado, com revisão periódica pelo gestor do ARCiber;

b) Uso exclusivo durante a execução de tarefas administrativas;

c) Monitoramento através de trilhas de auditoria;

d) Utilização de múltiplos fatores de autenticação como, por exemplo, tokens OTP (one time password) ou reconhecimento biométrico.

4.5.1.6. As características especiais das credenciais de acesso padrão embarcadas (locais) nos sistemas operacionais e softwares devem ser consideradas na política de gestão de acessos e identidades:

a) O acesso à senha de contas embarcadas deve ser restrito a um número limitado de pessoas;

b) Cada ativo que possua credencial embarcada deve possuir uma senha distinta. Uma mesma senha não deve ser atribuída a mais de um ativo.

4.6. MONITORAMENTO E RESPOSTA A INCIDENTES

4.6.1. Os ativos do ARCiber devem estar configurados para gerar logs de segurança apropriados para suportar investigações e a reconstrução de possíveis incidentes de segurança. Esses logs devem ser armazenados por prazo definido nas políticas de segurança cibernética da organização.

4.6.2. Os dispositivos de segurança como *Firewalls*, IDS/IPS, *Antimalware* e subsistemas de autenticação devem estar configurados para gerar alertas caso identifiquem atividades suspeitas:

a) As regras para geração de alertas devem ser revisadas periodicamente;

b) Todos os alertas devem ser reportados imediatamente à equipe responsável definida na política de segurança do agente;

c) Os alertas gerados devem ser analisados e respondidos no prazo definido pela política de segurança do agente.

4.6.3. Devem ser estabelecidos mecanismos para identificação e resposta a incidentes cibernéticos tempestivamente.

4.6.4. Deve ser implementado um plano de resposta a incidentes cibernéticos, contemplando minimamente os seguintes requisitos:

Instrução de Operação	Código	Revisão	Item	Vigência
Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético	**RO-CB.BR.01**	**00**	**4.1.11.**	**09/07/2021**

a) Identificação dos cenários de risco cibernéticos aplicáveis ao ARCiber e estratégias de tratamento para cada cenário;

b) Classificação do impacto;

c) Equipes envolvidas, com os seus respectivos papéis e responsabilidades antes, durante e depois da crise;

d) Critérios para ativação do plano de resposta a incidentes cibernéticos.

4.6.5. Testes de ativação dos planos de resposta a incidentes cibernéticos devem ser realizados periodicamente, em ciclos definidos na política de segurança cibernética da organização, cobrindo minimamente as listas de ativação (*call tree*) e revisão dos procedimentos descritos. Os exercícios deverão gerar documentos de lições aprendidas e as respectivas ações corretivas e de melhorias.

4.6.6. Incidentes cibernéticos que afetem ativos do ARCiber devem ser informados ao ONS.

5. ORIENTAÇÕES TÉCNICAS COMPLEMENTARES

5.1. TRATAMENTO DE EXCEÇÕES

5.1.1. Os casos em que requisitos não possam ser implementados devem ser tratados com uma exceção. Cada exceção gerada deve ser criada:

a) Documentada detalhadamente, incluindo a data em que ela foi identificada, o motivo pelo qual ela precisa ser tratada como exceção, os itens desta RO que deixarão de ser atendidos e os impactos esperados;

b) Aprovada pelo gestor responsável pela segurança cibernética do ARCiber;

5.2. ADOÇÃO DE CONTROLES COMPLEMENTARES

Cabe a cada organização adotar controles:

a) complementares nos ativos que integram o ARCiber, conforme suas próprias políticas, diretrizes e avaliações de risco.

b) de segurança cibernética nos ativos que não integram o ARCiber, conforme suas próprias políticas, diretrizes e avaliações de risco.

Instrução de Operação	Código	Revisão	Item	Vigência
Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético	**RO-CB.BR.01**	**00**	**4.1.11.**	**09/07/2021**

6. ANEXOS

ANEXO 1 – DISPOSIÇÕES TRANSITÓRIAS

PRAZO PARA IMPLANTAÇÃO	ITENS DA ROTINA
Até 18 (dezoito) meses após a entrada em vigor do presente documento	4.1.2 4.1.3 4.2.1 4.2.2 4.3.1 4.3.2 4.3.3 4.6.1
Até 27 (vinte e sete) meses após a entrada em vigor do presente documento	4.1.1 4.1.4 4.4.1 4.4.2 4.5.1 4.6.2 4.6.3 4.6.4 4.6.5 4.6.6

7. REFERÊNCIA BIBLIOGRÁFICA

7.1. ANSI/ISA-95.00.01-2010 (IEC 6224-1 Mod) Enterprise-Control System Integration – Part 1: Models and Terminology. 5.2 Functional Hierarchy;

7.2. Purdue Reference Model for CIM.