IEC 62443-3-3:2013 Requisitos de segurança de sistemas para a automação industrial

Sete requisitos fundamentais, 51 requisitos de sistema

100 requisitos. Esta norma é certificável por um organismo acreditado. Versão de 07/2026.

A IEC 62443-3-3 permite certificação, e o que é certificado é um sistema, não uma organização nem uma pessoa. As vias são o ISASecure SSA e o IECEE CB Scheme. Quem quiser certificar a organização precisa da 62443-2-1 ou da 2-4, quem se referir ao componente precisa da 62443-4-2. Esta lista contém os 51 requisitos de sistema e as 49 melhorias de requisito. Quais deles se aplicam depende do nível de segurança pretendido: 38 a partir do SL 1, 60 a partir do SL 2, 90 a partir do SL 3, todos os 100 no SL 4. Nenhuma melhoria já se aplica no SL 1. Esta lista é um auxiliar de trabalho para autoavaliação, não uma prova.

Empresa	Data	Elaborado por

5 FR 1: Quem ou o que pede acesso, e se é realmente quem afirma ser 24

SR 1.1 **Os utilizadores humanos são identificados e a sua identidade é verificada antes de obterem acesso, em todos os pontos onde possam operar ou configurar o sistema de automação. Isto inclui painéis de operador na máquina, acessos de engenharia e serviços de rede.**

Como se comprova: Inventário de todos os pontos de início de sessão do sistema, ou seja, HMI, sala de controlo, acesso de programação do PLC, switch, VPN e cliente de manutenção remota, cada um com o mecanismo de autenticação aí utilizado. Acrescentar um extrato de configuração ou uma captura de ecrã do ecrã de início de sessão para cada classe de dispositivo. Uma operação pequena começa com uma tabela por dispositivo, colunas: dispositivo, interface, autenticação presente sim ou não, justificação em caso de não. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.1 RE 1 **Cada utilizador humano trabalha com um identificador individual atribuído exclusivamente a essa pessoa. As contas partilhadas e de turno estão desativadas, as restantes exceções são justificadas caso a caso e apoiadas por medidas adicionais.**

Como se comprova: Exportação de contas por sistema que associe o identificador à pessoa, lista de exceções com justificação e medida compensatória, por exemplo uma câmara ou um registo de presenças no posto do operador. Esta linha é uma melhoria de requisito e por isso nunca é obrigatória no SL 1, sendo exigida a partir do SL 2.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.1 RE 2 **Quem inicia sessão a partir de uma rede não fiável, por exemplo a partir da internet ou através de uma ligação de manutenção remota, comprova a sua identidade utilizando pelo menos dois fatores independentes.**

Como se comprova: Configuração do acesso remoto com o segundo fator ativado, um registo de exemplo de início de sessão que mostre ambos os fatores, e a lista de emissão de tokens ou registos de aplicações. Uma operação pequena utiliza o segundo fator da gateway VPN existente ou uma aplicação de autenticação, o que não custa nada além do tempo de configuração. Melhoria de requisito, exigida a partir do SL 3, não no SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.1 RE 3 **A comprovação por dois fatores independentes aplica-se não só ao acesso a partir do exterior, mas a todo o início de sessão de um utilizador humano, incluindo os inícios de sessão dentro da rede classificada como fiável.**

Como se comprova: Extrato da política do serviço central de autenticação que mostre que o segundo fator é aplicado sem qualquer isenção de rede, mais registos de exemplo de início de sessão da sala de controlo e do painel de operador. Melhoria de requisito, exigida apenas a partir do SL 4.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.2 **Não só as pessoas, mas também os processos de software e os dispositivos se autenticam junto do sistema antes de lhes ser permitido trocar dados ou utilizar serviços. Isto inclui os acoplamentos entre controladores, as ligações de dados a sistemas de nível superior e as ferramentas de diagnóstico.**

Como se comprova: Lista das ligações máquina a máquina com origem, destino, protocolo e a credencial utilizada em cada caso, por exemplo certificado, conta de serviço ou chave pré-partilhada. Acrescentar um extrato de configuração de um acoplamento que torne a autenticação visível. Exigido a partir do SL 2, não exigido no SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 1.2 RE 1 **Cada processo de software e cada dispositivo apresenta o seu próprio identificador único. Não são permitidas contas de serviço partilhadas nem uma única chave utilizada em todo o sistema por vários dispositivos.** Documento

Como se comprova: Correspondência entre dispositivo e identificador ou número de série do certificado que demonstre que nenhum identificador aparece duas vezes. Melhoria de requisito, exigida a partir do SL 3 e por isso não faz parte do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 1.3 **As contas são geridas ao longo de todo o seu ciclo de vida: criação, alteração de privilégios, desativação por saída e remoção são regidas por regras e apoiadas pelos sistemas envolvidos. Isto abrange contas de utilizador, contas de serviço e contas de emergência.** Documento

Como se comprova: Registo de contas com tipo, titular, finalidade e estado, mais evidência de admissões e saídas, por exemplo uma entrega assinada ou um ticket que mostre a desativação com a respetiva data. É aconselhável uma revisão periódica das contas, e numa operação pequena basta uma reconciliação anual da lista de contas com a lista de pessoal. Exigido a partir do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 1.3 RE 1 **A gestão de contas está unificada em todos os componentes do sistema, de modo que a desativação de uma conta num local não fique sem efeito em dispositivos individuais.**

Como se comprova: Evidência da integração com o diretório central, por exemplo serviço de diretório ou RADIUS, com uma lista dos componentes ligados e uma lista explícita dos dispositivos que não podem ser ligados, juntamente com o respetivo procedimento alternativo. Registo de teste de uma desativação que produz efeito em todos os sistemas ligados. Melhoria de requisito, exigida a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 1.4 **Os identificadores são emitidos de acordo com regras fixas, atribuídos de forma inequívoca a uma pessoa, um dispositivo ou uma função, retirados quando deixam de ser utilizados e nunca reatribuídos posteriormente a um titular diferente.**

Como se comprova: Regra de nomenclatura dos identificadores, por exemplo apelido mais inicial ou código de fábrica mais número, mais o histórico de identificadores retirados que demonstre que não são reutilizados. Uma operação pequena mantém uma única lista corrida com data de emissão e data de retirada. Exigido a partir do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 1.5 **Os autenticadores, tais como palavras-passe, chaves, certificados e tokens, são emitidos de forma organizada, alterados quando há suspeita de divulgação e revogados quando necessário. As contas predefinidas e as palavras-passe de fábrica tal como fornecidas são alteradas antes da entrada em funcionamento.**

Como se comprova: Lista de emissão de tokens e certificados com destinatário e data, evidência de alterações e revogações, mais uma lista de verificação de entrada em funcionamento por dispositivo com o item palavra-passe de fábrica alterada, assinado. Exigido a partir do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 1.5 RE 1 **As credenciais dos processos de software não são armazenadas como um ficheiro legível no suporte de armazenamento, mas sim num armazenamento apoiado por hardware que impede a leitura da parte secreta.**

Como se comprova: Evidência do tipo do componente de segurança utilizado, por exemplo TPM, elemento seguro ou HSM, com um extrato de configuração que comprove que a chave é armazenada dentro do componente. Um registo de compra ou uma folha de dados é suficiente como evidência de tipo. Melhoria de requisito, exigida a partir do SL 3, não exigida no SL 1 nem no SL 2.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.6 **O acesso sem fios ao sistema, por exemplo WLAN, comandos remotos por rádio ou diagnóstico por Bluetooth, só pode ser utilizado após identificação e autenticação do utilizador e do dispositivo, e é gerido de forma deliberada.**

Como se comprova: Inventário de todas as ligações sem fios com finalidade, alcance e método de encriptação, extrato de configuração do ponto de acesso e a lista de dispositivos finais aprovados. Uma operação pequena documenta ainda quais as interfaces sem fios dos dispositivos que foram deliberadamente desligadas. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.6 RE 1 **Todo o acesso sem fios tem de poder ser atribuído a um utilizador específico ou a um dispositivo específico, uma chave de rede partilhada por todos os participantes não é suficiente.**

Como se comprova: Evidência de um método com credenciais individuais, por exemplo autenticação WLAN empresarial contra um diretório ou certificados por dispositivo, mais um registo de ligação que mostre o identificador individual. Melhoria de requisito, exigida a partir do SL 2 e por isso não no SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.7 **Onde quer que sejam utilizadas palavras-passe, a sua robustez mínima pode ser configurada, por exemplo comprimento mínimo e tipos de caracteres exigidos, e os valores configurados produzem efeito para todas as contas em causa.**

Como se comprova: Extrato de configuração da política de palavras-passe por sistema com os valores efetivamente definidos, por exemplo comprimento >= 10 carateres e pelo menos três tipos de carateres, mais uma lista dos sistemas que tecnicamente não conseguem suportar esta definição juntamente com a respetiva medida compensatória. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.7 RE 1 **Para os utilizadores humanos vigoram regras adicionais sobre a geração e a vigência das palavras-passe: impede-se a reutilização de palavras-passe anteriores e a validade é limitada no tempo.**

Como se comprova: Extrato de configuração que mostre o histórico de palavras-passe, por exemplo bloqueio de reutilização das últimas cinco palavras-passe, e a validade máxima configurada. Melhoria de requisito, exigida a partir do SL 3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.7 RE 2 **O limite de vigência da palavra-passe aplica-se não só às pessoas, mas a todas as contas, incluindo as de serviço, manutenção e dispositivo.**

Como se comprova: Plano de rotação para contas técnicas com a data da última e da próxima alteração por conta, mais evidência das alterações, por exemplo um registo de alteração ou um ticket. Melhoria de requisito, exigida apenas a partir do SL 4.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.8 **Onde são utilizados certificados, estes provêm de uma gestão de certificados organizada, com regras definidas para pedido, emissão, período de validade, renovação e revogação.** Documento

Como se comprova: Política de certificados ou uma breve regra escrita que indique a responsabilidade, os períodos de validade e a via de revogação, mais um inventário dos certificados emitidos com as respetivas datas de expiração. Uma operação pequena mantém uma tabela com certificado, dispositivo, data de expiração e data de lembrete, o que evita paragens silenciosas da instalação causadas por certificados expirados. Exigido a partir do SL 2.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.9 **Quando são utilizados pares de chaves para autenticação, o sistema valida o certificado na íntegra: cadeia de confiança, período de validade, estado de revogação e prova de que a contraparte possui efetivamente a chave privada. A ligação entre certificado e conta é inequívoca.**

Como se comprova: Extrato de configuração com a verificação de revogação ativada, por exemplo CRL ou OCSP, registo de teste de um início de sessão rejeitado com um certificado expirado ou revogado, mais a tabela de correspondência entre certificado e conta. Exigido a partir do SL 3, não exigido no SL 1 nem no SL 2.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.9 RE 1 **As chaves privadas residem exclusivamente num armazenamento apoiado por hardware do qual não podem ser extraídas, e são também utilizadas dentro desse armazenamento.**

Como se comprova: Folha de dados ou evidência de certificação do componente de segurança utilizado e um extrato de configuração que mostre que a chave é gerada dentro do componente, de modo que a chave privada nunca o abandona. Melhoria de requisito, exigida apenas a partir do SL 4.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.10 **Durante o início de sessão o sistema não revela nenhuma informação que possa ser explorada. As palavras-passe introduzidas são ocultadas e as mensagens de erro não revelam se foi o identificador ou a palavra-passe que estava incorreto.**

Como se comprova: Captura de ecrã do ecrã de início de sessão com a introdução mascarada e uma captura de ecrã da mensagem de erro após uma tentativa falhada. Para dispositivos que tecnicamente não consigam fazer isto, por exemplo painéis de operador mais antigos, acrescentar uma breve nota sobre a medida compensatória, por exemplo acesso físico restrito ao local da instalação. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.11 **O número de tentativas de início de sessão falhadas consecutivas é limitado e a resposta a estas é configurável, por exemplo um bloqueio temporário. A resposta escolhida não impede a operação da instalação relacionada com a segurança funcional.**

Como se comprova: Extrato de configuração com o limiar, por exemplo bloqueio após <= 5 tentativas falhadas, e a duração do bloqueio, mais uma breve avaliação de por que motivo o bloqueio não impede a operação de emergência nem um encerramento seguro da instalação. Em postos de operador com função de segurança, um bloqueio temporizado é preferível a um bloqueio de conta permanente. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.12 **Pode ser apresentado um aviso de utilização antes do início de sessão, remetendo para as regras de utilização e monitorização do sistema. O texto e a apresentação são configuráveis pelo proprietário do ativo.**

Como se comprova: Captura de ecrã do texto do aviso apresentado e da redação aprovada com a data de aprovação. As operações pequenas acordam a redação de forma breve com a representação dos trabalhadores ou com a direção, sendo suficiente um parágrafo. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.13 **O acesso a partir de redes não fiáveis, por exemplo a manutenção remota por fornecedores, está restrito a vias definidas, é monitorizado e pode ser interrompido a qualquer momento.**

Como se comprova: Inventário das vias de acesso remoto com finalidade, parte remota, pessoa de contacto e a via utilizada, mais registos de ligação e evidência da capacidade de desligar, por exemplo um interruptor de chave, uma regra de firewall ou um router de manutenção remota que possa ser desligado. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 1.13 RE 1 **Cada sessão individual a partir de uma rede não fiável é explicitamente aprovada por uma pessoa responsável antes de a ligação ser estabelecida, uma ligação permanentemente aberta não é suficiente.**

Como se comprova: Registos de aprovação por sessão de manutenção remota com hora, motivo, pessoa que aprova e duração, tecnicamente por exemplo através de um interruptor de chave no router de acesso ou de um portal de aprovação. Numa operação pequena basta um livro de registo de manutenção remota no armário de comando, assinado pelo técnico de manutenção em cada sessão. Melhoria de requisito, exigida a partir do SL 2 e por isso nunca no SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

6 FR 2: Controlo de utilização (privilégios, sessões, registos de auditoria) 24

SR 2.1 **O sistema aplica tecnicamente os privilégios que foram concedidos: cada pessoa com sessão iniciada, cada dispositivo e cada processo de software recebe exatamente o acesso que lhe foi atribuído, e qualquer tentativa que vá além disso é rejeitada.**

Como se comprova: Um conceito de privilégios que associe contas a permissões, mais uma captura de ecrã ou um extrato de configuração por sistema de controlo, HMI e posto de engenharia que mostre os privilégios ativos. Além disso, um registo de teste em que uma conta com poucos privilégios tenta uma ação bloqueada e é rejeitada. Exigido a partir do SL 1. Uma operação pequena gere-se com duas ou três funções, por exemplo operar, manter, projetar, e documenta-as numa única página.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 2.1 RE 1 **A aplicação de privilégios não se aplica apenas aos operadores humanos, mas igualmente aos processos de software e dispositivos que acedem ao sistema por conta própria.**

Como se comprova: Uma lista de contas técnicas e de serviço, por exemplo clientes OPC UA, ligações de historian, serviços de cópia de segurança, cada uma com o respetivo conjunto de privilégios atribuído. Um extrato da gestão de privilégios que mostre que estas contas não funcionam com direitos de administrador. Melhoria de requisito, exigida a partir do SL 2, não no SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 2.1 RE 2 **Os privilégios não são concedidos a indivíduos um a um, mas sim através de funções, e a correspondência entre função e ações permitidas fica registada de forma rastreável.** Documento

Como se comprova: Uma matriz de funções e privilégios em forma de tabela: as linhas são as funções, as colunas as ações tais como alterar um valor de referência, descarregar um programa, reconhecer um alarme, criar uma conta. Mais a lista de correspondência entre pessoa e função. Melhoria de requisito, exigida a partir do SL 2. Uma folha de cálculo mantida atualizada, com data de alteração, é totalmente suficiente como evidência.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 2.1 RE 3 **Para casos excecionais estritamente definidos, um supervisor autorizado pode levantar uma restrição de privilégios por um período limitado, e cada uma dessas exceções fica registada no rasto de auditoria.**

Como se comprova: Uma descrição do procedimento de aprovação de exceções que indique quem a pode conceder e durante quanto tempo permanece válida, mais registos de auditoria de exceções já concedidas, retirados do registo do sistema. Melhoria de requisito, exigida a partir do SL 3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 2.1 RE 4 **As intervenções particularmente críticas exigem a aprovação de duas pessoas autorizadas independentes antes de a ação ser executada.**

Como se comprova: Uma lista das ações sujeitas a dupla aprovação, por exemplo alterar parâmetros de segurança ou descarregar um novo programa de controlo, juntamente com evidência de configuração e registos de auditoria que identifiquem ambos os aprovadores. Melhoria de requisito, exigida apenas a partir do SL 4.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.2 **A utilização de ligações sem fios na rede de automação está sujeita a uma autorização explícita, e só os participantes aprovados podem trocar dados ou intervir por via aérea.**

Como se comprova: Um inventário de todas as ligações sem fios, por exemplo pontos de acesso WLAN, emparelhamentos Bluetooth, routers de rede móvel, cada um com a sua finalidade e os seus participantes aprovados. Mais a configuração de controlo de acesso no ponto de acesso. Exigido a partir do SL 1. Quem não opere nenhuma ligação sem fios na rede de processo declara-o exatamente assim por escrito e apoia-o com uma vista de configuração que mostre o sem fios desativado.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.2 RE 1 **Os dispositivos sem fios não autorizados nas imediações da rede de automação são detetados e comunicados.**

Como se comprova: Um registo da monitorização sem fios ou de uma verificação sem fios periódica com data, lista de resultados e uma nota sobre cada dispositivo desconhecido. É identificada a via de comunicação à função responsável. Melhoria de requisito, exigida a partir do SL 2, não no SL 1. Uma operação pequena pode realizar uma verificação trimestral com um portátil e arquivar o resultado como registo.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.3 **A utilização de dispositivos portáteis e móveis no sistema, por exemplo portáteis de assistência, armazenamento USB ou tablets, é regida por regras e tecnicamente limitada a dispositivos explicitamente aprovados.**

Como se comprova: O conjunto de regras para a utilização de dispositivos, uma lista dos dispositivos de assistência aprovados com os respetivos identificadores, e evidência da restrição técnica, por exemplo portas USB no HMI e no posto de engenharia desativadas ou limitadas a dispositivos específicos. Exigido a partir do SL 1. Uma operação pequena trabalha com duas pens de assistência etiquetadas que só são gravadas numa única estação de transferência.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.3 RE 1 **Antes da ligação, o estado de segurança de um dispositivo portátil ou móvel é verificado, e os dispositivos que não cumpram os requisitos são impedidos de obter acesso.**

Como se comprova: Os critérios de verificação do estado do dispositivo, por exemplo proteção antimalware atualizada e nível de correções, mais registos de verificação por dispositivo de assistência e evidência da aplicação técnica, por exemplo através de uma estação de transferência ou de um controlo de acesso à rede. Melhoria de requisito, exigida a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.4 **Para o código móvel executado no sistema, por exemplo scripts em interfaces de operador ou conteúdo ativo em relatórios, é definido quais os tipos permitidos, e a execução dos tipos não permitidos é impedida.** Documento

Como se comprova: Uma definição de que código móvel é permitido em que sistemas, mais evidência de configuração da restrição, por exemplo execução de scripts no browser do HMI desativada, macros em ficheiros de avaliação bloqueadas. Exigido a partir do SL 1. É suficiente uma definição de uma página que cubra os três ou quatro casos que realmente existem.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.4 RE 1 **Antes de o código móvel ser executado, é verificado que provém da fonte esperada e que não foi alterado.**

Como se comprova: Evidência de configuração da verificação de assinatura ou do controlo de soma de verificação, mais um registo de teste em que código manipulado ou não assinado é rejeitado. Melhoria de requisito, exigida a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.5 **Uma sessão é bloqueada após um período definido sem ação do operador e só é libertada novamente após uma nova autenticação, sem perder a visualização da informação de processo relevante para a segurança.**

Como se comprova: Um extrato de configuração com o tempo de bloqueio configurado por posto de trabalho, mais uma justificação para os postos de trabalho em salas de controlo permanentemente ocupadas em que o bloqueio é deliberadamente definido de forma diferente. Exigido a partir do SL 1. Evidência visual: uma captura de ecrã do ecrã de bloqueio com a linha de alarmes ainda visível.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.6 **As sessões remotas são terminadas após um período definido sem atividade ou a pedido do operador, de modo que nenhuma ligação remota aberta fique sem vigilância.**

Como se comprova: A configuração do acesso remoto com o respetivo limite de tempo de inatividade, registos de auditoria de sessões remotas terminadas, e uma descrição de como o operador pode desligar imediatamente uma sessão de manutenção remota em curso, por exemplo através de um interruptor de chave ou de uma libertação por sessão. Exigido a partir do SL 2, não no SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.7 **O número de sessões simultâneas por conta ou função é limitado, e as tentativas de início de sessão que ultrapassem esse limite são rejeitadas.**

Como se comprova: Um extrato de configuração com o limite máximo definido por função, por exemplo <= 1 sessão simultânea para contas de engenharia, mais um registo de teste da segunda tentativa de início de sessão rejeitada. Exigido a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.8 **Os eventos relevantes para a segurança são registados, e cada entrada indica pelo menos a hora, a origem, a conta que desencadeou o evento, o tipo de evento e o resultado.** Documento

Como se comprova: Uma definição dos tipos de evento a registar, por exemplo início de sessão, início de sessão falhado, alteração de privilégios, alteração de programa, alteração de configuração, mais um extrato real do registo de auditoria que mostre os campos indicados. Exigido a partir do SL 1. Uma operação pequena reúne os registos do sistema de controlo, do HMI e da firewall numa pasta com um período de retenção fixo.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.8 RE 1 **Os registos de auditoria dos vários componentes são reunidos num ponto central e formam um único registo, ao nível de todo o sistema, que pode ser avaliado em conjunto.**

Como se comprova: Um esquema de arquitetura da recolha de registos que mostre todas as fontes ligadas, mais uma avaliação que coloque eventos de pelo menos dois componentes numa mesma linha temporal. Melhoria de requisito, exigida a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.9 **É disponibilizado armazenamento suficiente para os registos de auditoria, de modo que os eventos sejam conservados durante o período de retenção definido e não sejam sobrescritos involuntariamente.**

Como se comprova: Um cálculo ou estimativa da necessidade de armazenamento a partir do volume diário de registos multiplicado pelo período de retenção, mais o tamanho de armazenamento configurado e a regra de arquivo. Exigido a partir do SL 1. Na prática basta uma cópia diária para um local de armazenamento separado com um período de retenção documentado.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 2.9 RE 1 **Quando é atingido um limiar definido de nível de ocupação do armazenamento de auditoria, é emitido um aviso à função responsável antes de a capacidade de armazenamento ficar totalmente esgotada.**

Como se comprova: Um extrato de configuração do limiar, por exemplo um aviso a partir de >= 80 por cento de utilização, mais um exemplo da notificação disparada e a lista de destinatários. Melhoria de requisito, exigida a partir do SL 3.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

SR 2.10 **Se o registo de auditoria falhar ou o armazenamento de auditoria ficar cheio, o sistema reage de uma forma previamente definida e a função responsável é informada, sem colocar em risco a operação segura da instalação.**

Como se comprova: A reação definida para cada caso de falha, por exemplo sobrescrever as entradas mais antigas e gerar uma notificação em vez de parar a instalação, com uma justificação do ponto de vista do processo. Evidência através de uma notificação de teste disparada e da correspondente entrada de auditoria. Exigido a partir do SL 1.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

SR 2.11 **Cada registo de auditoria tem uma marca temporal proveniente de uma fonte horária identificada, de modo que os eventos de diferentes componentes possam ser ordenados entre si.**

Como se comprova: Uma indicação da fonte horária utilizada por componente e um extrato de registo com uma marca temporal visível que inclua o fuso horário. Exigido a partir do SL 2, não no SL 1.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

SR 2.11 RE 1 **Os relógios de todos os componentes participantes estão sincronizados com uma fonte horária comum, de modo que o desvio se mantenha dentro de um limite definido.**

Como se comprova: A configuração de sincronização horária, por exemplo servidor NTP e intervalo de sincronização, mais um registo de verificação com o desvio medido por componente face ao limite definido, por exemplo <= 1 segundo. Melhoria de requisito, exigida a partir do SL 3.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

SR 2.11 RE 2 **A própria fonte horária está protegida contra manipulação, e uma referência horária inverosímil ou alterada é detetada e comunicada.**

Como se comprova: Uma descrição de como a fonte horária é protegida, por exemplo sincronização horária autenticada, restrição a uma fonte interna, monitorização de saltos temporais, mais notificações ou registos de auditoria de um desvio detetado. Melhoria de requisito, exigida apenas a partir do SL 4.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

SR 2.12 **Para ações críticas definidas, é possível determinar sem margem para dúvidas, a posteriori, quem as desencadeou, de modo que a pessoa que atuou não possa negar de forma credível tê-lo feito.** Documento

Como se comprova: Uma lista das ações a que se aplica esta evidência, por exemplo alteração de receita, libertação de lote, alteração de valores-limite, mais os registos correspondentes com um identificador de pessoa único e evidência de que as contas de grupo estão excluídas para estas ações. Exigido a partir do SL 3.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

SR 2.12 RE 1 **A atribuição inegável da pessoa que atua aplica-se não só a ações críticas selecionadas, mas a todos os utilizadores e a todas as ações que desencadeiam.**

Como se comprova: Evidência de que cada conta está associada a uma única pessoa e de que não subsistem inícios de sessão partilhados, mais um extrato de registo de ações quaisquer no qual aparece consistentemente um identificador de pessoa único. Melhoria de requisito, exigida apenas a partir do SL 4.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

7 FR 3: Integridade do sistema, proteção de dados, software e sessões contra alterações não autorizadas 19

SR 3.1 **O sistema de controlo deteta quando a informação foi alterada durante o trânsito num canal de comunicação, e fá-lo tanto para dados de controlo como para dados de configuração e tráfego de gestão. A proteção abrange também as ligações que saem do sistema ou atravessam segmentos de rede não fiáveis.**

Como se comprova: Uma visão geral de rede e protocolos que indique qual o canal que utiliza qual mecanismo de integridade (soma de verificação, código de autenticação de mensagem, telegramas assinados), um extrato de configuração das definições de segurança do barramento de campo ou do OPC UA, e um registo de teste que mostre que um telegrama adulterado foi demonstravelmente rejeitado. Uma operação pequena capta isto numa tabela por ligação com as colunas origem, destino, protocolo e mecanismo de integridade, e comprova a eficácia uma vez com uma captura de tráfego. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 3.1 RE 1 **A proteção de integridade em trânsito assenta em mecanismos criptográficos, de modo que uma manipulação deliberada por um atacante com meios próprios não possa passar despercebida. Uma simples soma de verificação contra erros de transmissão não é suficiente aqui.**

Como se comprova: Uma lista dos mecanismos criptográficos e comprimentos de chave em uso por canal, uma referência à gestão de chaves subjacente, e extratos de configuração (por exemplo conjuntos de cifras TLS, SecurityPolicy do OPC UA, perfis IPsec). As operações pequenas apoiam-se nos perfis seguros predefinidos dos seus controladores e arquivam uma captura de ecrã da definição ativa. Melhoria de requisito, exigida a partir do SL 3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 3.2 **Existem mecanismos de proteção contra código malicioso que impedem a execução de código de programa indesejado nos componentes do sistema e que comunicam qualquer deteção. Os mecanismos são escolhidos de forma a não perturbarem a operação prevista da instalação, e são mantidos atualizados.**

Como se comprova: Uma visão geral por componente de qual o mecanismo aplicável (antivírus, lista branca de aplicações, sistema operativo reforçado sem direitos de execução), evidência de que as assinaturas ou listas brancas são atualizadas, e alertas do sistema de proteção. Quando o antivírus não é viável, por exemplo num controlador, a medida compensatória é registada com a respetiva justificação. As operações pequenas resolvem bem com listas brancas no PC do operador e uma regra escrita para suportes USB. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 3.2 RE 1 **A proteção contra código malicioso produz efeito também nos pontos de entrada e saída da instalação, onde os dados entram ou saem, e não apenas nos próprios dispositivos finais.**

Como se comprova: Uma lista de todos os pontos de entrada e saída (acesso de manutenção remota, gateway de transferência de dados, suportes amovíveis, entrega à rede de escritório, via de correio eletrónico para versões de programa) com o mecanismo de verificação efetivo em cada um, mais registos das entregas que foram verificadas. As operações pequenas configuram um único PC de entrega com verificação de vírus como gateway e fixam isto numa instrução de trabalho. Melhoria de requisito, exigida a partir do SL 2.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 3.2 RE 2 **Os mecanismos de proteção contra código malicioso são geridos a partir de um ponto central, as atualizações são distribuídas de forma centralizada, e as deteções são reunidas num único local para avaliação.**

Como se comprova: A configuração da consola de gestão central, um relatório sobre o estado de atualização de todos os componentes ligados, e uma avaliação das deteções comunicadas ao longo de um período de tempo. Melhoria de requisito, exigida a partir do SL 3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 3.3 **As funções de segurança do sistema são verificadas em intervalos planeados e após alterações, para confirmar que realmente funcionam. Os testes são programados de forma a não colocarem em risco a operação da instalação, e os resultados são registados.** Documento

Como se comprova: Um plano de testes que indique o objeto em teste, o intervalo e a janela temporal, juntamente com os registos de teste que mostrem data, testador, comportamento esperado e comportamento observado. Testes individuais úteis são: um início de sessão com uma conta desativada falha, o antivírus reage a um ficheiro de teste, o acesso de manutenção remota é inacessível sem libertação. As operações pequenas associam os testes à paragem de manutenção já planeada e seguem uma lista de verificação fixa. Exigido a partir do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.3 RE 1 **A verificação das funções de segurança é realizada com meios automatizados, de modo a ser repetível sem esforço manual e a produzir um resultado consistente.**

Como se comprova: Os scripts ou ferramentas de teste juntamente com o respetivo calendário, os ficheiros de saída, e uma comparação de várias execuções que demonstre que os desvios são detetados. Melhoria de requisito, exigida a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.3 RE 2 **A verificação das funções de segurança também é possível durante a operação normal, sem ser necessário parar a instalação nem colocá-la num estado especial.**

Como se comprova: Uma descrição do procedimento de teste com evidência de que não tem efeito adverso sobre o processo, por exemplo uma análise do impacto nos tempos de ciclo e na carga de rede, mais registos de teste retirados da operação produtiva. Melhoria de requisito, exigida a partir do SL 4.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.4 **As alterações não autorizadas a software, firmware e informação em repouso são detetadas. Isto aplica-se igualmente a programas de controlo, conjuntos de parâmetros, receitas e ficheiros de configuração.**

Como se comprova: Um inventário das versões dignas de proteção com os valores de verificação ou assinaturas armazenados, os resultados das comparações de integridade, e a reconciliação documentada com a versão guardada no controlo de versões. As operações pequenas guardam a versão de programa lançada juntamente com a respetiva soma de verificação num local protegido contra escrita e comparam em caso de suspeita ou após a manutenção. Exigido a partir do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.4 RE 1 **Se for detetada uma violação da integridade do software ou da informação, o sistema comunica-a automaticamente a um ponto responsável, sem que ninguém tenha de a procurar ativamente.**

Como se comprova: A configuração das vias de notificação (alarme na sala de controlo, correio eletrónico, mensagem para o sistema de monitorização), uma lista de destinatários com disposições de substituição, e pelo menos um alarme de teste com um tempo de resposta documentado. Melhoria de requisito, exigida a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.5 **As entradas que o sistema aceita de dados de processo, interfaces ou interfaces de utilizador são verificadas quanto à sintaxe permitida, ao intervalo de valores permitido e ao comprimento permitido antes de serem processadas. As entradas inválidas não conduzem a um comportamento descontrolado.**

Como se comprova: Uma especificação dos limites e formatos por entrada, extratos da lógica de validação no controlador ou na aplicação, e casos de teste com entradas deliberadamente inválidas (um valor demasiado elevado, um tipo de dados errado, uma cadeia de carateres demasiado longa) juntamente com o comportamento documentado do sistema. As operações pequenas registam os limites de plausibilidade por ponto de medição numa tabela e verificam-nos durante a entrada em funcionamento. Exigido a partir do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.6 **Para o caso de uma avaria é definido qual o estado que as saídas para a instalação assumem, e o sistema assume exatamente esse estado. O estado definido está alinhado com a segurança funcional da instalação.**

Como se comprova: Uma definição por saída ou grupo de saídas (manter o valor, valor substituto definido, estado de encerramento seguro) com uma justificação proveniente da avaliação de riscos, um extrato de configuração do controlador, e evidência de um teste de falha, por exemplo uma rotura de cabo ou perda de comunicação, que mostre o comportamento esperado. Exigido a partir do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.7 **O sistema trata as condições de erro de forma que a operação permaneça sob controlo e não seja divulgada informação que ajude um atacante. As mensagens de erro apresentadas aos operadores mantêm-se breves, enquanto os detalhes técnicos vão apenas para os registos internos.**

Como se comprova: Uma visão geral das classes de erro com o comportamento do sistema previsto para cada uma, exemplos das mensagens apresentadas comparadas com as correspondentes entradas de registo interno, e evidência de teste de que não aparecem na interface do operador caminhos de ficheiro, nomes de conta, saídas de base de dados ou detalhes de versão. Exigido a partir do SL 1.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.8 **As sessões ativas estão protegidas contra o sequestro e contra a injeção de mensagens estranhas. Uma sessão termina após o fim de sessão ou após um período definido sem atividade, e a partir daí não pode ser reutilizada.**

Como se comprova: A configuração da gestão de sessões com os limites configurados para o tempo de inatividade e a duração máxima, evidência do mecanismo de proteção contra a repetição de mensagens, e um registo de teste em que uma sessão capturada deixa de funcionar após o fim de sessão. Exigido a partir do SL 2.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.8 RE 1 **Os identificadores de sessão perdem a validade quando a sessão termina e não voltam a ser aceites pelo sistema, mesmo quando são apresentados novamente a partir do exterior.**

Como se comprova: Um extrato de configuração da gestão de sessões que cubra a invalidação, mais um registo de teste em que um identificador anteriormente válido é enviado novamente após o fim de sessão e é rejeitado pelo sistema. Melhoria de requisito, exigida a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.8 RE 2 **Para cada nova sessão é gerado um identificador dedicado de utilização única. Os identificadores não são reutilizados entre sessões, utilizadores ou dispositivos.**

Como se comprova: Uma descrição do procedimento de geração e evidência do registo ou de uma captura de tráfego de que vários inícios de sessão consecutivos recebem identificadores diferentes. Melhoria de requisito, exigida a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.8 RE 3 **Os identificadores de sessão são gerados com mecanismos aleatórios reconhecidos, de modo que não possam ser adivinhados nem derivados de identificadores anteriores.**

Como se comprova: Uma indicação do gerador de números aleatórios utilizado e da respetiva fonte de entropia, uma declaração do fornecedor ou um relatório de teste sobre o mesmo, e uma avaliação estatística de uma amostra de identificadores gerados. Melhoria de requisito, exigida a partir do SL 4.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 3.9 **Os registos relacionados com a segurança e as ferramentas utilizadas para os avaliar estão protegidos contra acesso, alteração e eliminação não autorizados. O círculo de pessoas autorizadas a alterar ou remover registos é mantido reduzido e está identificado.** Documento

Como se comprova: Um conceito de autorização para os dados de registo com atribuição nominal, a configuração do encaminhamento para um sistema de registo separado, períodos de retenção, e evidência de teste de que um operador comum não consegue eliminar entradas. As operações pequenas encaminham os registos para um dispositivo separado ao qual os operadores da instalação não têm acesso de escrita. Exigido a partir do SL 2.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 3.9 RE 1 **Os registos relacionados com a segurança são ainda armazenados num suporte que exclui a sobrescrita posterior, de modo que uma entrada uma vez escrita já não possa ser alterada, mesmo com direitos administrativos.** Documento

Como se comprova: Uma descrição do armazenamento utilizado (suporte de escrita única, arquivo resistente a adulteração, cadeia de assinaturas continuamente alargada), evidência de uma tentativa falhada de alterar uma entrada, e a regra de conservação e recuperação dos suportes. Melhoria de requisito, exigida a partir do SL 3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

8 FR 4: Confidencialidade dos dados 6

SR 4.1 **O sistema de automação protege a informação confidencial contra divulgação não autorizada, tanto em trânsito como em repouso. É definido quais os dados considerados confidenciais, por exemplo receitas, conjuntos de parâmetros, credenciais, ficheiros de configuração ou dados de diagnóstico com referência pessoal.** Documento

Como se comprova: Uma lista dos tipos de dados dignos de proteção, indicando onde são guardados e como são transmitidos, mais a medida de proteção específica para cada entrada, por exemplo uma ligação encriptada, um suporte de armazenamento encriptado ou uma partilha restrita. Uma operação pequena gere-se com uma tabela de uma única página: tipo de dado, onde se encontra, quem o pode ver, o que o protege. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 4.1 RE 1 **Para a informação que viaja através de redes não fiáveis ou é armazenada fora do ambiente protegido, a confidencialidade é assegurada por meios técnicos e não meramente prometida numa regra organizacional.**

Como se comprova: Um extrato de configuração da encriptação de transporte ou de armazenamento em uso, por exemplo o perfil VPN para manutenção remota, as definições TLS da interface do sistema de controlo, ou a encriptação dos suportes de cópia de segurança. Uma captura de ecrã datada da definição ativa é suficiente como evidência. Exigido a partir do SL 2, não a partir do SL 1, por se tratar de uma melhoria de requisito.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 4.1 RE 2 **A confidencialidade é assegurada também nas fronteiras entre zonas, de modo que a informação não se torne visível em texto claro quando passa de uma zona para outra.**

Como se comprova: Um plano de zonas e condutas que assinale quais os cruzamentos encriptados, juntamente com a configuração do componente de fronteira, tal como uma gateway, uma firewall ou um díodo de dados. Uma captura de tráfego ou um registo de teste que mostre que não aparecem dados em texto claro na fronteira. Exigido a partir do SL 4.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 4.2 **É definido como é removida de forma fiável a informação confidencial quando os dispositivos são desativados, mudam de proprietário, são enviados para reparação ou são reutilizados, de modo que não fiquem dados residuais legíveis.** Documento

Como se comprova: Um procedimento de desativação escrito com o método de higienização por tipo de dispositivo, mais registos de eliminação que indiquem a identificação do dispositivo, a data e a pessoa que a realizou. Uma operação pequena regista isto como uma linha por dispositivo numa lista partilhada e arquiva junto os certificados dos contratantes externos de eliminação. Exigido a partir do SL 2.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 4.2 RE 1 **As áreas de armazenamento partilhadas são limpas antes de serem reatribuídas a outro utilizador ou processo, de modo que o conteúdo pertencente ao utilizador anterior não possa ser lido.**

Como se comprova: Uma declaração do fornecedor ou um registo de configuração que cubra a limpeza das áreas de memória e de buffer reutilizadas, complementado com um registo de teste da receção ou da manutenção. Quando um componente não o consegue fazer, a medida compensatória documentada serve como evidência, por exemplo não partilhar o dispositivo entre diferentes funções. Exigido a partir do SL 3, não a partir do SL 1, por se tratar de uma melhoria de requisito.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 4.3 **Onde quer que seja utilizada criptografia, os algoritmos, os comprimentos de chave e a gestão de chaves seguem boas práticas reconhecidas, e é definido como as chaves são geradas, distribuídas, armazenadas, rodadas e revogadas.** Documento

Como se comprova: Uma visão geral dos mecanismos utilizados por sistema, indicando algoritmo, comprimento de chave e período de validade, mais as regras de gestão de chaves e registos de rotações de chaves e renovações de certificados. As recomendações públicas servem como referência, por exemplo as diretrizes técnicas do BSI alemão. Uma operação pequena mantém uma lista de certificados com datas de expiração e um lembrete >= 30 dias antes da expiração. Exigido a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

9 FR 5: Fluxo de dados restrito, zonas e condutas 11

SR 5.1 **O sistema de controlo pode ser dividido em zonas separadas, e o tráfego entre essas zonas passa apenas por condutas definidas. A divisão segue uma lógica explicável, por exemplo pela necessidade de proteção, pela propriedade ou pela função das secções de instalação envolvidas.** Documento

Como se comprova: Diagrama de rede que mostre as zonas e as condutas entre elas, uma lista de zonas com a lógica de cada fronteira, e a configuração dos componentes de separação, tais como definições de VLAN ou interfaces de firewall. Uma operação pequena contenta-se com um esquema de uma única página que mostre escritório, rede de máquinas e acesso remoto como três caixas com as ligações entre elas, mais uma captura de ecrã da configuração de VLAN do switch.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.1 RE 1 **A separação de zonas é implementada fisicamente, ou seja, através de componentes de rede dedicados e cablagem dedicada, e não assenta apenas na configuração lógica dentro de dispositivos partilhados. Secção 9.1 desta lista, exigida a partir do SL 2. As melhorias de requisito desta norma nunca são obrigatórias já no SL 1.**

Como se comprova: Inventário de componentes de rede que indique qual o switch ou router que serve qual zona, fotografias ou plano do armário das distribuições separadas, etiquetagem dos cabos. As operações pequenas comprovam isto com dois switches separados, claramente etiquetados, em vez de um único dispositivo partilhado, e uma fotografia do armário de comando na documentação da instalação.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.1 RE 2 **A rede de automação pode ser operada de forma independente das redes exteriores à automação. Se as tecnologias de informação de escritório ou uma ligação externa falharem, o controlo e a monitorização da instalação continuam a funcionar. Exigido a partir do SL 3.**

Como se comprova: Lista de dependências dos serviços utilizados dentro da rede de automação, tais como servidor horário, resolução de nomes, serviço de diretório ou servidor de licenças, indicando onde cada um está alojado, juntamente com um registo de teste de um ensaio de desligamento em que a ligação às TI de escritório foi retirada. Uma operação pequena anota o resultado desse ensaio no registo de manutenção: ligação ascendente retirada, a instalação continuou a funcionar, só faltaram os relatórios de escritório.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.1 RE 3 **As zonas que albergam funções particularmente críticas, por exemplo funções de segurança funcional ou de proteção, estão separadas das restantes zonas tanto lógica como fisicamente. Exigido a partir do SL 4.**

Como se comprova: Marcação das zonas críticas no diagrama de zonas com a justificação da classificação, evidência de componentes de rede dedicados e cablagem dedicada para essas zonas, configuração das condutas com evidência de que não existe nenhuma via partilhada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.2 **Nas fronteiras de zona, o tráfego é controlado, monitorizado e permitido ou negado de acordo com regras definidas. Não existe nenhuma via entre duas zonas que contorne este ponto de controlo.**

Como se comprova: Conjunto de regras exportado da firewall ou do dispositivo de fronteira, registos de ligações negadas e permitidas, evidência de que não existem vias laterais, por exemplo através de uma verificação de placas de rede adicionais, modems ou routers de rede móvel nos computadores da instalação. Uma operação pequena comprova isto com a exportação de regras da sua única firewall e uma breve nota de verificação a confirmar que não existe nenhum router não planeado em qualquer armário de comando.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.2 RE 1 **O conjunto de regras na fronteira de zona funciona segundo o princípio de que tudo é negado a menos que tenha sido explicitamente permitido. Cada regra de permissão é individualmente justificada e associada a uma finalidade. Exigido a partir do SL 2.**

Como se comprova: Conjunto de regras com uma regra final visível que descarta o restante, e uma lista de permissões que indique origem, destino, serviço, finalidade e pessoa responsável para cada regra. As operações pequenas mantêm esta lista como uma tabela de cinco colunas juntamente com a exportação da firewall e revêm-na uma vez por ano à procura de regras de que já ninguém precisa.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.2 RE 2 **A rede de automação pode ser deliberadamente isolada de todas as ligações externas e mantida a funcionar em modo ilha. A ação pode ser acionada sem ser necessário parar a instalação. Exigido a partir do SL 3.**

Como se comprova: Descrição do procedimento de isolamento que indique quem o pode acionar e como, evidência da implementação técnica tal como um conjunto de regras de emergência ou um interruptor de isolamento etiquetado, mais o registo de um simulacro em que o isolamento foi efetivamente exercitado. Uma operação pequena realiza o simulacro uma vez por ano durante a manutenção e anota data, duração e qualquer ocorrência anómala.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.2 RE 3 **Se o dispositivo na fronteira de zona falhar ou perder as suas regras, este nega o tráfego em vez de o deixar passar. Uma falha não pode deixar para trás uma ligação aberta. Exigido a partir do SL 4.**

Como se comprova: Declaração do fornecedor ou evidência de configuração sobre como o componente se comporta em caso de avaria e no reinício, registo de teste de uma falha deliberadamente induzida com o resultado observado, alinhamento com a avaliação de riscos da instalação, porque uma fronteira que nega o tráfego pode ela própria ter consequências consoante o processo.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.3 **Os serviços gerais de comunicação de pessoa a pessoa, tais como correio eletrónico, mensagens ou videochamadas, podem ser impedidos nos dispositivos de automação e dentro das redes de automação. O âmbito do bloqueio está definido e justificado.**

Como se comprova: Definição de quais os serviços não permitidos na rede de automação, mais a implementação técnica: portas e destinos bloqueados no conjunto de regras, aplicações removidas ou bloqueadas nos postos de operador, evidência a partir do inventário de software dos dispositivos. Uma operação pequena resolve isto com um bloqueio de aplicações no posto HMI e uma regra que nega o tráfego de correio e web de saída a partir da rede de máquinas.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.3 RE 1 **Esses serviços de comunicação de pessoa a pessoa são impedidos em toda a rede de automação, e não apenas restringidos parcialmente ou limitados a dispositivos individuais. Exigido a partir do SL 2.**

Como se comprova: Evidência de que o bloqueio se aplica a todos os dispositivos da zona, por exemplo através de uma revisão do software instalado em cada computador da zona e de um teste de ligação a partir de um computador da instalação qualquer. As operações pequenas comprovam isto com uma lista de dispositivos em que cada linha está assinalada com a data de verificação, e uma captura de ecrã da tentativa de ligação falhada.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 5.4 **Os dados e as funções das aplicações estão compartimentados de modo que os processos com diferentes necessidades de proteção ou diferentes privilégios não possam aceder às mesmas áreas. A separação está integrada na arquitetura do sistema e não é deixada ao acaso da instalação.**

Como se comprova: Visão geral das aplicações que indique que dados e serviços utilizam e que contas estão por trás delas, configuração de instâncias, bases de dados, diretórios ou máquinas virtuais separadas, e uma lista de privilégios por área. Uma operação pequena resolve isto com contas de utilizador separadas e pastas de dados separadas para engenharia e operação, mais uma nota sobre que aplicação acede a que pasta.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

10 FR 6: Resposta oportuna a eventos 3

SR 6.1 **Os registos de auditoria recolhidos no sistema podem ser lidos e avaliados pelas pessoas e funções autorizadas para o efeito sem perturbar a operação em curso da instalação, e o acesso a esses registos está, por sua vez, restringido a utilizadores autorizados.**

Como se comprova: Uma matriz de funções e permissões que mostre quem pode ver os dados de registo, mais uma captura de ecrã ou exportação de uma vista de registo efetivamente obtida, com uma marca temporal. Acrescentar uma breve nota sobre a via utilizada para a obtenção, por exemplo a interface de operador do controlador, um servidor de registo ou uma exportação de ficheiro. As operações pequenas contentam-se com uma visão geral de uma página por instalação: onde está o registo, quem tem acesso de leitura, como é obtido. Uma obtenção de teste uma vez por ano, registada no diário de manutenção, demonstra que a via funciona. Aplica-se a partir do SL 1 para todos os níveis de segurança.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 6.1 RE 1 **Os registos de auditoria podem ser obtidos através de uma interface automática, de modo que as ferramentas de análise os possam processar sem nova transcrição manual, e os dados são disponibilizados num formato documentado e de utilização comum.**

Como se comprova: Uma descrição da interface em uso juntamente com o formato, por exemplo syslog, OPC UA Alarms and Conditions, uma consulta REST ou uma exportação CSV, mais um registo de amostra e a configuração do sistema recetor. A evidência pode ser um extrato da configuração do SIEM ou do coletor de registos, juntamente com a prova dos registos recebidos. Sem um SIEM, basta um coletor de registos num servidor simples que obtém os registos durante a noite através de um script e os armazena; o próprio script mais uma listagem do diretório dos ficheiros recolhidos constitui a evidência. Como melhoria, isto só é exigido a partir do SL 3, não a partir do SL 1.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 6.2 **A atividade relevante para a segurança no sistema é monitorizada continuamente, a monitorização deteta tentativas de ataque e utilização indevida e comunica-as prontamente a um ponto de contacto identificado, e são definidas as ferramentas, as vias de comunicação e as responsabilidades utilizadas para o efeito.**

Como se comprova: Uma visão geral das ferramentas de monitorização por zona, por exemplo um sensor de rede, alertas de antivírus, alarmes de firewall ou verificação de integridade, indicando quem recebe o alerta e em que prazo se espera uma resposta. Configurações de alarme, uma lista de alertas gerados nos últimos meses e as respetivas notas de tratamento servem como evidência. As operações pequenas não precisam de uma sala de controlo permanente: uma caixa de correio partilhada ou uma caixa de tickets que reúna os alertas dos sistemas existentes, mais uma regra fixa de que uma pessoa identificada a revê em cada dia útil, é suficiente e é comprovada através do histórico da caixa de correio. Exigido a partir do SL 2.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

11 FR 7: Disponibilidade de recursos 13

SR 7.1 **Perante sobrecarga ou ataques de inundação deliberados, o sistema mantém-se num estado de operação definido, as funções de controlo essenciais continuam a funcionar, e a falha de um serviço individual não arrasta consigo toda a instalação.**

Como se comprova: Configuração dos mecanismos de proteção (limitação de taxa, limites de ligação, controlo de tempestades de broadcast nos switches), declarações do fornecedor sobre o comportamento sob carga, mais um registo de um teste de carga ou de um evento real de sobrecarga com observação da função de controlo. Exigido a partir do SL 1. Uma operação pequena cobre isto com capturas de ecrã das definições do switch e da firewall e uma breve nota sobre que função continuou a funcionar durante um teste da célula mais importante.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.1 RE 1 **A carga de comunicação que os componentes individuais podem injetar na rede está limitada, de modo que um componente avariado ou comprometido não possa inundar o segmento de rede.**

Como se comprova: Limites de largura de banda e de multicast por porta nos componentes de rede, evidência do limite para cada ligação, mais uma medição da carga base real por dispositivo. Exigido a partir do SL 2, não a partir do SL 1. Sem switches geridos esta linha não pode ser comprovada, sendo esse então o ponto em aberto.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.1 RE 2 **Uma situação de sobrecarga dentro do sistema em consideração não se propaga a sistemas ou redes adjacentes; o impacto para o exterior está tecnicamente contido.**

Como se comprova: Regras de segmentação e filtragem nas fronteiras, evidência de que o tráfego de saída está limitado, mais um registo de teste que mostre que uma carga gerada na rede de célula não degradou a rede de escritório nem uma rede vizinha. Exigido a partir do SL 3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.2 **A utilização de tempo de processamento, memória, espaço de armazenamento e largura de banda de rede está limitada, de modo que um único processo ou serviço não possa consumir os recursos necessários para o controlo.**

Como se comprova: Configuração dos limites de recursos (quotas, prioridades de processo, limites de memória), avaliação da monitorização de utilização durante um período representativo, mais os limiares a partir dos quais é emitido um aviso. Exigido a partir do SL 1. As operações pequenas utilizam os meios integrados do sistema operativo e uma monitorização simples com um alerta de espaço em disco e CPU por correio eletrónico.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.3 **Existem cópias de segurança das configurações do sistema, dos dados de aplicação e das versões de programa; estas podem ser produzidas sem interromper a operação em curso e estão protegidas contra acesso e alteração não autorizados.** Documento

Como se comprova: Conceito de cópia de segurança que cubra âmbito, frequência e período de retenção, registos de cópia de segurança das execuções mais recentes, mais evidência da proteção de acesso dos suportes de cópia de segurança (armazenamento separado, encriptação, permissões dedicadas). Exigido a partir do SL 1. Uma operação pequena guarda os projetos do PLC e as versões do HMI num suporte encriptado que é desligado fisicamente após a cópia, e regista data e versão numa lista simples.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.3 RE 1 **A utilidade das cópias de segurança foi verificada; é demonstrado que a partir delas se consegue efetivamente restaurar um estado funcional.**

Como se comprova: Registo de um ensaio de restauro com data, versão de cópia de segurança testada, sistema de destino e resultado, pelo menos para os componentes críticos. Exigido a partir do SL 2, não a partir do SL 1. As operações pequenas verificam, por amostragem, um programa de PLC e uma imagem de HMI num dispositivo de reserva uma vez por ano e registam o resultado em duas frases.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.3 RE 2 **A cópia de segurança é executada automaticamente segundo um calendário definido; uma execução falhada é detetada e comunicada.**

Como se comprova: Calendário da tarefa de cópia de segurança, registos de execução sem lacunas, mais evidência da notificação de falha para uma execução sem sucesso (alarme, ticket, correio eletrónico). Exigido a partir do SL 3.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.4 **Após uma perturbação, avaria ou ataque, o sistema pode ser reposto num estado conhecido e seguro; a recuperação foi ensaiada e as responsabilidades estão identificadas.** Documento

Como se comprova: Plano de reinício para cada componente crítico com sequência, suportes necessários, contactos e tempo alvo, juntamente com o registo do exercício de recuperação mais recente. Exigido a partir do SL 1. Uma operação pequena contenta-se com uma ficha de reinício de uma página por linha, guardada no armário de comando e verificada sempre que uma peça de reserva é substituída.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.5 **Se a alimentação elétrica regular falhar, o sistema passa a um estado definido: ou a alimentação é mantida por uma fonte de reserva, ou tem lugar um encerramento ordenado sem perda do estado seguro.**

Como se comprova: Evidência de dimensionamento e manutenção da fonte de alimentação ininterrupta ou do gerador de emergência, registo de teste do teste de bateria ou de carga mais recente, mais uma descrição do comportamento na comutação e no restabelecimento da rede elétrica. Exigido a partir do SL 1. As operações pequenas testam a UPS sob carga uma vez por ano e registam a data do teste, o tempo de autonomia e a idade da bateria.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.6 **As definições de rede e de segurança do sistema estão fixadas a um estado alvo aprovado, os desvios em relação a esse estado alvo são detetáveis, e o estado atual pode ser consultado a qualquer momento.** Documento

Como se comprova: Configuração alvo aprovada por classe de dispositivo (especificação de reforço), estados de configuração atuais dos dispositivos, mais o resultado de uma comparação entre o estado alvo e o estado real com uma lista de desvios e o motivo de cada um. Exigido a partir do SL 1. Uma operação pequena guarda as exportações de configuração sob controlo de versões e compara-as antes e depois de cada alteração.

◯ Aberto ◯ Em curso ◯ Cumprido ◯ Não aplicável

Evidência / justificação

SR 7.6 RE 1 **O estado atual das definições de segurança pode ser exportado em formato legível por máquina, de modo a poder ser verificado automaticamente em relação ao estado alvo.**

Como se comprova: Saída de amostra num formato legível por máquina (exportação de configuração, ficheiro estruturado, consulta por interface) e o script ou ferramenta que realiza a comparação em relação ao estado alvo, juntamente com o relatório de resultado de uma execução. Exigido a partir do SL 3.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 7.7 **O sistema está restringido às funções necessárias para a operação; os serviços, portas, protocolos e interfaces que não são necessários estão desativados ou removidos.**

Como se comprova: Lista de serviços ativos e portas abertas por componente com uma justificação da necessidade, evidência de que os restantes estão desativados (configuração, resultado de verificação de portas), mais uma regra para as interfaces USB e de manutenção. Exigido a partir do SL 1. As operações pequenas realizam uma verificação de portas simples por segmento e justificam cada item aberto numa linha.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação

SR 7.8 **Está disponível um inventário atualizado de todos os componentes do sistema, com fabricante, tipo, versão de firmware ou software e endereço de rede, e este é mantido atualizado sempre que ocorrem alterações.** Documento

Como se comprova: Inventário de componentes com a respetiva data de revisão e proprietário, evidência de manutenção através do histórico de alterações, mais uma comparação com uma deteção de rede para encontrar dispositivos não registados. Exigido a partir do SL 2, não a partir do SL 1. Uma operação pequena mantém o inventário como uma tabela e atualiza-o como regra fixa sempre que um dispositivo é substituído e sempre que o firmware é atualizado.

○ Aberto ○ Em curso ○ Cumprido ○ Não aplicável

Evidência / justificação