MATRIZ DE AUDITORIA DE CIBERSEGURANÇA

ENCRYPT 4.0

Cofinanciado pelo Programa Erasmus+ da União Europeia

O Projeto ENCRYPT4.0 (2020-1-RO01-KA202-079983) foi financiado com o apoio da Comissão Europeia. Esta publicação reflete apenas os pontos de vista do autor e a Comissão não pode ser responsabilizada por qualquer utilização que possa ser feita das informações contidas.

Conteúdo

1. INTRODUÇÃO

A produtividade, qualidade e custos de fabrico podem potencialmente beneficiar de melhorias drásticas através da conectividade crescente da Indústria 4.0, da utilização de computação digital e do armazenamento de dados fora do local. No entanto, existem riscos associados para as PME da área do fabrico, tais como a potencialidade dos concorrentes e adversários de acederem aos seus dados. Os ciberataques são cada vez mais comuns e são geralmente implementados para extrair ou roubar dados confidenciais e/ou de propriedade, manipular dados capturados para causar efeitos indesejados e destruir bens de capital (Margot Hutchins & Stefanie Robinson, 2015). Os ciberataques podem ser definidos como "um ataque, através do ciberespaço, visando a utilização do ciberespaço de uma empresa para perturbar, desativar, destruir ou controlar maliciosamente um ambiente/infraestrutura informática; ou destruir a integridade dos dados ou roubar informação controlada" (National Institute for Standards and Technology, 2012, p. B3). O Fórum Económico Mundial (2017) dá prioridade a duas soluções para abordar os ciber riscos impulsionados pela inovação: i) Medição dos ciber riscos e ii) Avaliação da cibersegurança. Em 2019, a fraude ou roubo de dados e os ciberataques foram identificados pelo Fórum Económico Mundial (FEM) como o quarto e quinto riscos mais prováveis de ocorrer (World Economic Forum, 2020), em 2020, identificou as questões relacionadas com o ciberataque, tais como ciberataques e fraude ou roubo de dados, dentro da lista dos 10 principais riscos a longo prazo.

O ENCRYPT 4.0 foca a avaliação da Cibersegurança através do desenvolvimento da Matriz para Auditoria de Ciber-riscos

A Indústria Transformadora precisa de ferramentas para incorporar os ciber riscos nos seus processos de gestão de risco existentes. Neste contexto, o ENCRYPT 4.0 responde a esta necessidade identificada, centrando-se na avaliação da Cibersegurança, ao desenvolver a Matriz de Auditoria de Cibersegurança (CRAM). A CRAM é uma ferramenta abrangente destinada a apoiar os responsáveis das PME na área do fabrico a realizar uma análise abrangente dos seus processos tendo em conta a utilização de soluções tecnológicas inovadoras com base na Indústria 4.0, identificando os riscos e apoiando-os na conceção e estabelecimento de controlos eficazes. A CRAM foi desenvolvida tendo em conta as informações de normas nacionais, da europeias e mundiais (Anexo A), bem como o feedback de peritos em cibersegurança de seis países europeus - Áustria, Portugal, Roménia, Bulgária, Chipre e Espanha.

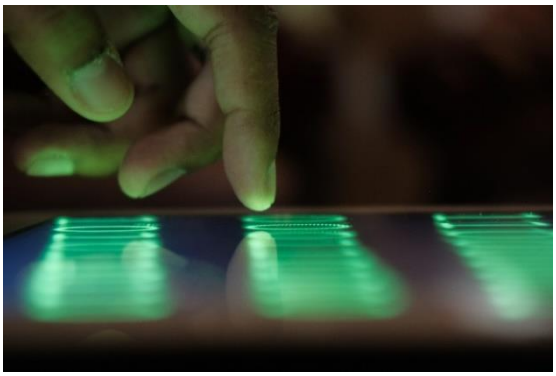
- Este documento inclui a) a proposta de valor CRAM, b) a metodologia CRAM, c) a descrição das categorias da Matriz de Auditoria de Ciber-riscos c) os passos para realizar auditorias de Cibersegurança e d) as referências bibliográficas.

2. PROPOSTA DE VALOR CRAM

A **Matriz de Auditoria de Cibersegurança (CRAM)** vai permitir que as fábricas inteligentes executem uma análise sistemática da sua situação e criem um perfil preciso do risco e das ameaças existentes. A CRAM Encrypt 4.0, permitirá às fábricas inteligentes efetuar uma análise consistente de dados em tempo real e avaliar os riscos, com base numa matriz específica e extensa.

A Matriz de Auditoria de Cibersegurança é uma ferramenta analítica que vai apoiar as empresas de fabrico a identificar, analisar, dar prioridade aos riscos e a estabelecer rapidamente medidas de proteção. Nos últimos anos, um dos problemas mais prementes do mundo digital é a cibersegurança e a proteção da privacidade de dados. Em 2019, o Fórum Económico Mundial classificou os ciberataques entre os cinco principais riscos globais.

Em 2020, com a pandemia COVID-19, a maior dependência da conectividade e das infraestruturas digitais devido ao bloqueio global aumentou as oportunidades de intrusão e ataques cibernéticos. Ao mesmo tempo, para maximizar os danos e ganhos financeiros, os cibercriminosos estão a transferir os seus alvos de indivíduos e pequenas empresas para grandes empresas, governos e infraestruturas críticas, que desempenham um papel crucial na resposta ao surto. (INTERPOL G. S., 2020). “Os ciberataques representam mais perigo para as democracias e as economias do que as armas e tanques” (Juncker, 2017).



O Cybersecurity Ventures, o investigador líder mundial na ciber-economia global, previu que "os danos globais relacionados com o cibercrime em 2021 atingirão seis biliões de dólares, o que será mais do que todos os desastres naturais num ano” (Cybersecurity Ventures, 2020). O Relatório Anual Oficial de Cibercrime de 2019 declarou que "no final de 2016, a cada 40 segundos uma empresa foi vítima de um ataque de ransomware" (Cybersecurity Ventures, 2019) e as previsões são de que esse número aumentará para a cada 11 segundos até 2021.

Os ciberataques em infraestruturas críticas, classificados como o quinto maior risco em 2020 pela rede de especialistas do FEM, tornaram-se o novo padrão em setores como energia, saúde e transporte. No entanto, a indústria do fabrico está a sofrer com o aumento dos ciberataques, como o Relatório de Investigações de Violação de Dados de 2020 mostrou, detalhando 922 incidentes, 381 com divulgação de dados confirmados, apenas nos Estados Unidos (Verizon, 2020). As organizações de cibercrime organizado estão a unir esforços e estima-se que a sua probabilidade de deteção e perseguição seja muito baixa, por volta de 0,05% nos Estados Unidos, o cibercrime prestado como um serviço é um modelo de negócio em crescimento, uma vez que a crescente sofisticação das ferramentas na Darknet torna os serviços maliciosos mais acessíveis e facilmente acessíveis a qualquer pessoa" (World Economic Forum, 2020).

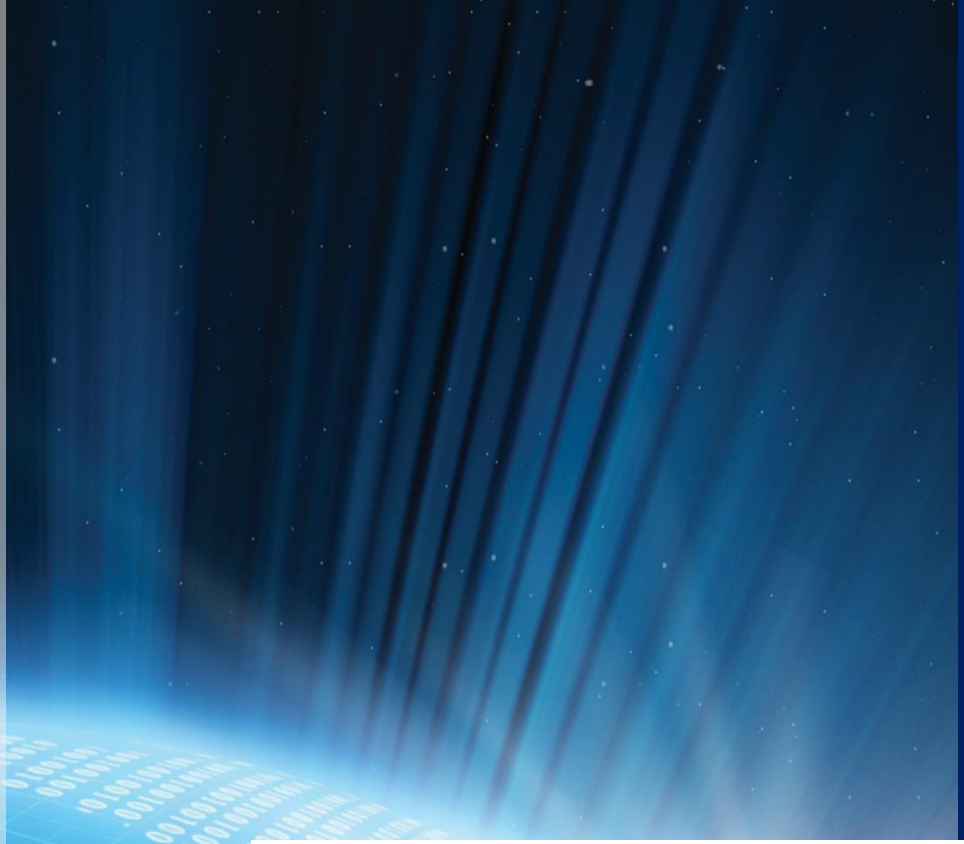
A capacidade de defesa das PME é tipicamente mais fraca do que a das grandes empresas e os números sugerem que apenas 14% das PME afetadas conseguem recuperar sozinhas. A Aliança Nacional de Cibersegurança afirma que 60% das PME que sofrem um ciberataque perdem o seu negócio no prazo de 6 meses e "a produção é muito mais propensa a ameaças à sua segurança devido à conectividade nos sistemas de TI e TO através da digitalização da Indústria 4.0" (Verizon, 2017).

A maioria das empresas transformadoras na sua tentativa de manter uma vantagem competitiva adapta-se às práticas da Indústria 4.0, fazem esforços investindo em sistemas de controlo e consultores externos, mas carecem de uma abordagem integrada da gestão dos ciber riscos. Os seus esforços não conseguem combater eficazmente as ameaças cibernéticas em rápida evolução, porque a maioria dos sistemas foram tradicionalmente desenvolvidos para se concentrarem na ausência de dano e no alto desempenho, em vez da segurança. Além disso, no que diz respeito à segurança, os fabricantes estavam historicamente preocupados principalmente em assegurar o seu ambiente de TO, negligenciando frequentemente a segurança das TI, “o surgimento da Indústria 4.0 introduz novas tecnologias nos ambientes tradicionais de OT e, portanto, as pessoas familiarizadas com o OT que trabalham nesses ambientes precisam de se adaptar” (EU Agency for Cybersecurity, 2019). Os colaboradores usam frequentemente informações potencialmente conflituosas para descrever ou avaliar alguns aspetos do ciber risco.

A CRAM descreve os indicadores de risco chave para aplicação aos dados em tempo real. A CRAM permitirá aos colaboradores não só fazer uma estratégia de cibersegurança a longo prazo, mas também realizar rapidamente relatórios diários. Isto vai mostrar os níveis reais de risco dos processos em qualquer momento, de importância crucial para a indústria da transformação, uma vez que manter a produção em curso é crítico e a mais curta indigência de certos processos pode ter um impacto irreparável e causar enormes perdas financeiras. Os riscos de segurança na produção estão a tornar-se cada vez mais complexos e a evoluir, o que torna de enorme importância dotar as PME de fabrico com o instrumento analítico adequado para delinear as precauções a tomar em consideração no dia-a-dia no contexto da produção. Ao contrário de falhas em processos mecânicos que podem ser classificadas como estáticas, as falhas de cibersegurança são dinâmicas, uma vez que incorporam intimamente as interações humanas.

O **objetivo principal da CRAM** é facultar aos **líderes das PME de fabrico** uma visão sobre os **potenciais riscos de cibersegurança** nos seus sistemas e apoiá-los para **adotar uma estratégia eficaz para mitigar os riscos**. Uma vez que é limitada a investigação disponível no domínio da avaliação da cibersegurança nos sistemas de fabrico, a CRAM do ENCRYPT 4.0 representa uma ferramenta inovadora destinada a ser incorporada na política de gestão de risco das empresas de fabrico.

A Matriz de Auditoria de Cibersegurança descreve os indicadores de risco chave que serão facilmente aplicados aos dados em tempo real.

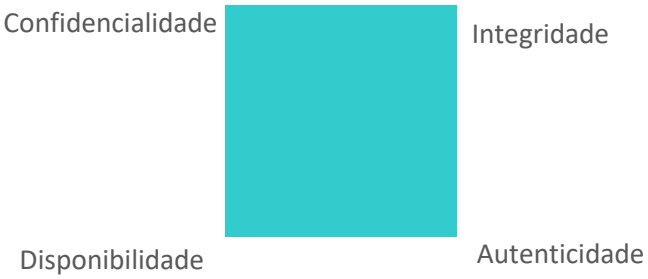


O principal objetivo da CRAM é fornecer aos líderes das PME de fabrico uma visão dos potenciais riscos de cibersegurança nos seus sistemas e apoiá-los a adotar uma estratégia eficaz para mitigar os riscos.

O CRAM foi projetado considerando o quarteto CIAA

3. METODOLOGIA DA MATRIZ DE AUDITORIA DE CIBER RISCOS

A CRAM foi desenhada tendo em conta o quarteto **CIAA** de **confidencialidade**, **integridade**, **disponibilidade** e **autenticidade**. Dois aspetos principais serão medidos: **Probabilidade de risco** e **Impacto do risco**, adaptada para **responder às** necessidades específicas das PME de fabrico com o potencial de ser facilmente moldada e adaptada na cultura organizacional específica de uma determinada empresa.



A CRAM também inclui: i) número do risco, ii) categoria do risco, iii) fonte do risco, iv) descrição do risco, v) potenciais custos associados às consequências do risco, vi) departamento da organização que pode ser afetado, vii) mitigação/ações previamente implementadas, viii) impacto do risco, ix) probabilidade de risco, x) nível global de risco, xi) triggers, xii) mitigação/ações a implementar, xiii) custos potenciais de mitigação, xiv) prazo, xv) pessoa responsável pela gestão do risco, xvi) supervisor responsável pela monitorização e xvii) avaliação da eficácia.

Abaixo, a descrição dos principais conceitos que compõem a Matriz de Auditoria de Ciber Riscos:

Disponibilidade: Garantir o acesso a informação em tempo oportuno e fiável.

Autenticidade: Assegurar a propriedade dos dados, de serem genuínos e originais, suscetíveis de verificação e confiança na validade de uma transmissão, de uma mensagem, ou do autor da mensagem. (Encrypt 4.0 project, 2020).

Avaliação de cibersegurança: Mecanismos de orientação e avaliação da cibersegurança reforçados, incluindo princípios comuns para avaliações de cibersegurança, um mecanismo de avaliação baseado em pontos e passos práticos para melhorar, que permitem às empresas avaliar e melhorar a sua prontidão em cibersegurança (World Economic Forum , 2017).

Confidencialidade: Preservação de restrições (controladas) no acesso e divulgação de informação, incluindo meios para proteger a privacidade pessoal e informações de propriedade.

Impacto: O impacto potencial avaliado resultante de um compromisso da confidencialidade, integridade ou disponibilidade de um tipo de informação, expressado num valor de *baixo*, *moderado* ou alto.

Integridade: Proteção contra modificação ou destruição imprópria de informação e inclui a garantia de não-repúdio e autenticidade da informação.

Probabilidade: Um fator ponderado com base numa análise subjetiva da probabilidade de uma determinada ameaça ser capaz de explorar uma determinada vulnerabilidade ou um conjunto de vulnerabilidades.

Descrições inspiradas no Guide for Conducting Risk Assessments (National Institute of Standards and Technology, 2012).

4. MATRIZ DE AUDITORIA DE CIBER RISCOS (CRAM)

A CRAM Encrypt 4.0 representa uma ferramenta abrangente destinada a apoiar os responsáveis pelas PME na área do fabrico a realizar uma análise abrangente dos seus processos, tendo em conta a utilização de soluções tecnológicas inovadoras com base na Indústria 4.0, identificar os ciber riscos e apoiar também na conceção e estabelecer controlos eficazes.

4.1 CATEGORIAS DA MATRIZ DE AUDITORIA DE CIBER RISCOS

Estas categorias derivaram de uma investigação e análise conduzidas de mais de 20 normas (Anexo A) no domínio da segurança da informação e da proteção de dados e de 12 entrevistas realizadas com especialistas em cibersegurança da Áustria, Portugal, Roménia, Bulgária, Chipre e Espanha.

Tabela 1. Categorias da Matriz de Auditoria de Cibersegurança

Categoria de Risco	Descrição da Categoria de Risco
Recursos humanos	Identificação dos riscos que estão relacionados com os recursos humanos da empresa, riscos relacionados com as funções e responsabilidades do pessoal da empresa, tomada de decisão, gestão de identidades, controlo de acessos, sensibilização...
Propriedade Intelectual	Identificação dos riscos que estão relacionados com a Propriedade Intelectual da empresa. A Propriedade Intelectual inclui a Propriedade Industrial, Direitos de Autor e Direitos Conexos e confere o direito ao uso exclusivo das respetivas informações técnicas, comerciais e industriais. A Propriedade Industrial visa proteger invenções, patentes, marcas e projetos abrangidos por direitos de uso exclusivo, produção e comercialização.
Segurança dos Sistemas de Controlo Industrial (ICS)	A segurança dos ICS envolve a preservação e a segurança dos sistemas de controlo industrial, bem como do software e hardware necessários que são utilizados pelo sistema.
Produtos	Identificação dos riscos que estão relacionados com os produtos. A ocorrência deste tipo de risco pode comprometer os produtos produzidos pela organização.
Riscos Legais de Cibersegurança	Identificação dos riscos que estão relacionados com responsabilidades legais e regulamentares. A ocorrência deste tipo de risco pode comprometer responsabilidades legais e/ou regulamentares da organização.
Ataques na cadeia de abastecimento	Identificação de vulnerabilidades na cadeia de abastecimento. A organização deve definir, avaliar e gerir processos de gestão de risco da cadeia de abastecimento e logística. Identificação das ligações a fornecedores com más posturas de segurança.
Tecnologia, TIC e segurança operacional	Identificação dos riscos relacionados com a tecnologia, TIC e operações da empresa. Para fazer face aos perigos resultantes de insuficiências funcionais da funcionalidade pretendida, perturbações operacionais ou por utilização/erros razoavelmente previsíveis pelos colaboradores relacionados com a tecnologia, TIC e operações.
Clientes	A ocorrência de um determinado risco pode comprometer o serviço prestado aos clientes da organização ou comprometer os dados dos clientes.
Cibersegurança física	A cibersegurança física é a proteção de ciber sistemas físicos, dispositivos de Internet das Coisas, proteção de pessoas, propriedade e bens físicos de ações e eventos que possam causar danos ou perdas.

5. AUDITORIAS DE CIBERSEGURANÇA

5.1 O QUE É UMA AUDITORIA DE CIBERSEGURANÇA?

A Indústria 4.0 trouxe novas tecnologias que ligam os mundos físico e digital dos processos empresariais em sistemas inteligentes integrados. Isto traz muitas oportunidades para melhorar os processos e o desempenho global, mas também muitas novas responsabilidades e ameaças. O maior nível de conectividade entre todos os sistemas através da IoT, computação na nuvem e muitas outras tecnologias, além de muitos benefícios, possui novos desafios para empresas relacionados com a segurança da informação, Big data, etc. que são processados por estes sistemas integrados. Por isso, as empresas e, em especial, as PME precisam de ferramentas para as apoiar no processo de verificação e análise das suas fraquezas no que respeita à segurança das tecnologias da Indústria 4.0 que possuem.

Uma auditoria de cibersegurança representa uma avaliação do desempenho em função de especificações, normas, controlos ou orientações.

Uma auditoria de cibersegurança representa uma avaliação do desempenho em função de especificações, normas, controlos ou orientações (CyLumena, 2020). Estas auditorias são normalmente feitas através de uma lista de verificação de controlos (biblioteca de controlos) que é definida com base em normas de cibersegurança (nacionais, internacionais, internas para a empresa) e/ou procedimentos e/ou políticas da empresa. O objetivo de uma auditoria de cibersegurança é ajudar as organizações a avaliar se dispõem de mecanismos de segurança adequados, identificando lacunas de segurança ou validando os procedimentos e políticas aplicados. As auditorias ajudam as empresas a verificar o que está na sua rede, o que precisa de ser protegido e quais as lacunas que existem nas suas proteções existentes para que possam fazer melhorias (Dosal, 2020).

AUDITORIAS DE CIBERSEGURANÇA VS. AVALIAÇÃO DA CIBERSEGURANÇA

As auditorias de cibersegurança diferem das avaliações de cibersegurança. Embora a auditoria de cibersegurança analise a possibilidade de existirem certos controlos estabelecidos, a avaliação da cibersegurança visa avaliar a eficácia destes controlos. (Aldorisio, 2020). As avaliações podem incluir algum grau de auditoria, mas nem sempre. As auditorias, dependendo do objetivo, também poderiam ser aplicadas quando uma organização quer avaliar o seu cumprimento de certas leis ou normas, neste caso normalmente a auditoria é realizada por um terceiro (externo) com a competência necessária. As avaliações, por outro lado, podem ser realizadas internamente por pessoas internas que tenham um bom conhecimento da infraestrutura de cibersegurança.

AUDITORIAS DE CIBERSEGURANÇA EXTERNAS VS. INTERNAS

As auditorias externas são realizadas por profissionais, especialmente quando o objetivo da auditoria é oferecer bases para uma certificação ao abrigo das normas de cibersegurança e uma avaliação de conformidade em função das normas oficiais, leis, etc. As auditorias internas de cibersegurança podem ser conduzidas por um especialista interno bem ciente dos processos da empresa e da arquitetura de cibersegurança. De acordo com o RGPD, cada empresa é legalmente obrigada a ter um responsável pela proteção de dados que domine a gestão de dados – que informação entra e sai da empresa, em que processos é usada e como é gerida. Portanto, uma escolha acertada para a realização de uma auditoria interna de cibersegurança poderia ser pelo Responsável pela Protecção de Dados ou uma equipa interna, dependendo do âmbito da auditoria. Nas próximas secções deste documento, apresentamos uma abordagem combinada para a realização de auditorias e avaliação internas de cibersegurança com base nas categorias definidas anteriormente e que devem ser tidas em conta no processo de auditoria.

5.2 COMO REALIZAR UMA AUDITORIA INTERNA DE CIBERSEGURANÇA?

O objetivo desta secção é apresentar orientações simples para a auto-condução de uma auditoria cibersegurança (auditoria interna de cibersegurança) que possa servir como uma ferramenta eficaz para avaliar a cibersegurança e os dados dentro da uma organização e/ou como preparação para auditorias externas (por terceiros) de cibersegurança.

PASSO 1: Definir as prioridades de segurança e o âmbito da auditoria

Nesta fase, a pessoa ou a equipa nomeada para a realização da auditoria deve de identificar qual será o âmbito do processo de auditoria. Um bom ponto de partida é enumerar todos os ciber-bens da empresa, que podem ser ativos associados a bens críticos, tais como: Sistemas de controlo; Sistemas de aquisição de dados; Equipamento de rede; Plataformas de hardware para máquinas virtuais ou armazenamento; Sistemas secundários ou de suporte, tais como scanners de vírus, Sistemas de AVAC, e fontes de energia ininterruptas (UPS) (n.d., Versify Solutions);

Em seguida, é preciso avaliar quais são os ativos cibernéticos críticos (CCA). De acordo com a norma de Proteção de Infraestruturas Críticas (CIP), versão 4 pela North American Electric Reliability Corporation (NERC) um CCA é "qualquer dispositivo que utilize um protocolo de encaminhamento para comunicar para fora do perímetro de segurança eletrónica (ESP), que utilize um protocolo de encaminhamento dentro de um centro de controlo, ou que seja acessível por linha telefónica." (2011, Flick & Morehouse).

Em palavras mais simples, os bens podem variar desde equipamento informático até vários sistemas e informação sensível sobre clientes e empresas, documentação interna, e sistemas de comunicação.

Uma vez identificados os ciber-ativos críticos, deverá ser identificado onde estão os parâmetros críticos de segurança e, assim, segmentar o que será incluído no âmbito da auditoria (2019, LeCount). Os parâmetros de segurança e os ativos vão variar muito de empresa para empresa, portanto, este passo inicial e a definição correta do âmbito de auditoria são de importância crucial para a eficácia do processo de auditoria. Uma vez definido o âmbito de auditoria, pode avançar para o passo seguinte – identificação de potenciais ameaças.

PASSO 2: Identificar os potenciais riscos e ameaças

Com base em 12 entrevistas feitas a especialistas no campo da cibersegurança, o consórcio ENCRYPT 4.0 identificou nove categorias de risco possíveis e compilou uma lista de potenciais riscos que cada uma destas categorias pode representar para ativos cibernéticos críticos. O modelo ENCRYPT4.0 engloba as seguintes nove categorias de risco a ter em conta: (1) Recursos humanos; (2) Propriedade intelectual; (3) Segurança dos Sistemas de Controlo Industrial (ICS); (4) Produtos; (5) Riscos legais de cibersegurança; (6) Ataques à cadeia de abastecimento; (7) Tecnologia, TIC e Segurança operacional; (8) Clientes; (9) Cibersegurança física. É necessário ter presente que, dependendo das atividades comerciais da empresa, o modelo de negócio e o setor de operações em que atua, nem todas as categorias se aplicam à empresa ou pode-se decidir que não existem ativos cibernéticos críticos ligados a

estas categorias. Para fazer esta avaliação, consulte o anexo 1 e escolha as categorias aplicáveis à sua organização e as ameaças que considera relevantes em função dos ativos críticos identificados na empresa.

PASSO 3: Priorizar os riscos

Neste passo crucial, é necessário verificar a lista de potenciais ameaças que considere aplicáveis à sua empresa e de acordo com um conjunto de critérios para decidir quais os riscos altamente prováveis e com um impacto adverso potencialmente mais grave. Por esta razão, o consorcio ENCRYPT 4.0 elaborou uma metodologia de avaliação do risco que tem em conta os seguintes componentes:

- Custos potenciais associados às consequências do risco;
- Departamento(s) da organização que podem ser afetados;
- Potencial impacto;
- Probabilidade – ao avaliar a probabilidade, ter em conta as tendências do setor, falhas de segurança anteriores;
- Nível de risco.

Pode aplicar diretamente a ferramenta ENCRIPT 4.0 Matriz de Avaliação de Ciber Riscos (CRAM) desenvolvida para priorizar facilmente os riscos potenciais.

PASSO 4: Auditoria das medidas de segurança em vigor

Tendo identificado as categorias de risco aplicáveis e as ameaças à sua organização, o próximo passo é avaliar se os seus ativos e ciber infraestruturas críticas estão vulneráveis a qualquer uma destas ameaças. Para o efeito, é necessário avaliar os protocolos/procedimentos/medidas de segurança estabelecidos no que respeita à identificação de potenciais lacunas de segurança que precisam de ser resolvidas. Na tabela 2, encontra algumas questões orientadoras e dicas sobre como avaliar se as medidas de segurança em vigor são adequadas, no entanto, também depende das ameaças que considere aplicáveis em cada categoria.

Tabela 2. Dicas sobre como identificar medidas de segurança em vigor

Nº.	Categoria	Dicas sobre como auditar medidas de segurança em vigor
1	**Recursos humanos**	Verificar a distribuição de funções e responsabilidades ligadas à gestão e segurança de dados; cibersegurança; controlo do sistema, etc. Falar com os colaboradores responsáveis nomeados dentro destes domínios – pergunte-lhes como reagiriam em determinadas situações, que protocolos de segurança implementariam, pelo que poderá avaliar se o pessoal está consciente e preparado em caso de se verificarem determinados riscos de cibersegurança; se precisam de formação ou não. Analisar acidentes e falhas de segurança devido a erros dos funcionários e à forma como foram tratados. Analisar se há algo mais que poderia ser feito para minimizar ainda mais a ocorrência desta ameaça no futuro.
2	**Propriedade intelectual**	Verificar a distribuição das funções e responsabilidades ligadas à gestão da propriedade intelectual, bem como dos segredos comerciais, etc. Entrevistar os colaboradores responsáveis, rever documentação relevante sobre a proteção de bens/ativos, tais como patentes, direitos de autor de marcas. Como é que esta documentação é mantida e gerida, quem tem acesso a ela? Houve incidentes no passado ligados a violações de informação, faltam informações neste domínio? Como foram tratados este incidentes, o protocolo de segurança está atualizado?
3	**Segurança dos Sistemas de Controlo Industrial (ICS)**	Quem tem acesso remoto e/ou físico ao ICS? Como é administrado o acesso remoto ao ICS? Existem controlos de segurança como a autenticação forte, o controlo de acessos e a encriptação para proteger contra o acesso não autorizado e a exploração destes sistemas? Quais são as medidas de controlo de acesso físico? Utiliza firewalls com reconhecimento do protocolo ICS para impor controlos de acesso ao tráfego na rede ICS? Tem um sistema de prevenção de intrusões definido?
4	**Produtos**	Dependendo do processo de produção, é necessário identificar em que processos se está a lidar com informação sensível e de que forma está a ser gerida e administrada. Verificar se existem segredos comerciais relacionados com a produção de produtos, etc.

		Como é que a empresa garante que esta informação é gerida com segurança? Qual é o protocolo – funções e responsabilidades, procedimentos, etc.? Existe algum controlo do acesso físico e remoto a computadores e redes; sistemas de produção, etc.? Como estão os seguros e controlados?
5	**Riscos legais de cibersegurança**	Existe algum controlo do acesso físico e remoto aos computadores e redes da empresa? Como é que estes são protegidos e controlados? Como é que os dados legais estão a ser geridos e administrados? O servidor está seguro? Quem tem acesso a esta informação? Houve alguma falha de segurança no passado? Como lidaram com a situação? Existe uma forma de melhorar os protocolos de segurança com base nas tendências/eventos/desenvolvimentos tecnológicos recentes?
6	**Ataques à cadeia de abastecimento**	Quem tem acesso aos sistemas de gestão de aprovisionamento? Existe uma Gestão dos Acessos Privilegiados? Quem tem acesso aos dados sensíveis? Como é assegurado este acesso? Tem Honeytokens implementados? Qual é o nível de controlo do acesso dos fornecedores de serviços? Quantos fornecedores têm acesso a software? A rede de fornecedores é monitorizada para vulnerabilidades?
7	**Tecnologia, TIC e Segurança Operacional**	Tem políticas rígidas de segurança móvel e salvaguarda de dados? Verificar se as aplicações de software e sistemas operativos estão atualizadas? Existem controlos de acesso em vigor para ativos críticos de cibersegurança? É monitorizada a atividade das contas dos utilizadores, registo e acesso à sua rede? Verificar se as firewalles estão devidamente configuradas, assegurando que existe uma encriptação de ponta a ponta para dados sensíveis. Existem mecanismos definidos para reconhecer e evitar ataques como phishing e pharming?
8	**Clientes**	Quem tem acesso a dados importantes do cliente? Tem cópias de segurança de dados e informações comerciais importantes?

9	**Cibersegurança física**	Como é gerida a manutenção dos equipamentos e dos ativos críticos de cibersegurança? Quem tem acesso físico a equipamento e ativos críticos de cibersegurança? Como é garantido o acesso?

PASSO 5: Definir/atualizar os protocolos de segurança com base na auditoria

Após a conclusão do PASSO 4, deverá fazer uma lista das ameaças identificadas aplicáveis à sua organização, para estar ciente do que já está a fazer e do que talvez esteja em falta e identificar os controlos adequados de segurança da informação para neutralizar ou erradicar o risco de ameaça (2020, LeCount).

Os controlos de segurança da informação são medidas tomadas para reduzir os riscos de segurança da informação, tais como violações de sistemas de informação, roubo de dados e alterações não autorizadas em informações ou sistemas digitais (Garcia, 2019). O principal objetivo dos controlos de segurança é proteger a disponibilidade, confidencialidade e integridade de dados e redes dentro de uma empresa. Como mencionado, os controlos de segurança são normalmente implementados após uma avaliação de risco de informação ou cibersegurança e representam um resultado desejado de avaliações e auditorias de cibersegurança no que diz respeito à resolução de lacunas de segurança reais ou potenciais identificadas.

Na tabela 3, em linha com o modelo de avaliação de riscos em cibersegurança ENCRYPT 4.0 com base em entrevistas com especialistas em cibersegurança de 6 países da UE, identificamos dois tipos de controlos – preventivos e corretivos em cada uma das nove categorias de risco. Com base na auditoria realizada no PASSO 4 já existe um conhecimento dos procedimentos de cibersegurança em vigor dentro da sua organização. Na tabela 3, são apresentadas algumas sugestões de controlos preventivos e corretivos para cada uma das categorias para implementação na sua organização.

Tabela 3. Controlos preventivos e corretivos de cibersegurança

Categoria do risco	Medidas Preventivas	Medidas Corretivas
Recursos humanos	Estabelecer um programa de formação e sensibilização Identificar claramente a gestão de identidades, autenticação e controlo de acessos A empresa dispõe de uma política que inclua: ● Lista de software autorizado. ● Repositório de software autorizado e registo de licenças. ● Sanções disciplinares associadas ao incumprimento destes regulamentos. Alterar as palavras-passe trimestralmente (política de palavras-passe fortes)	Controlo de permissões do utilizador Implementar o Sistema de Deteção de Intrusões (IDS) para detetar o acesso não autorizado a um pc ou a uma rede Alterar todas as palavras-passe após uma possível violação de dados Bloquear as contas suspeitas de acesso não autorizado Configurar a autenticação de dois fatores quando possível

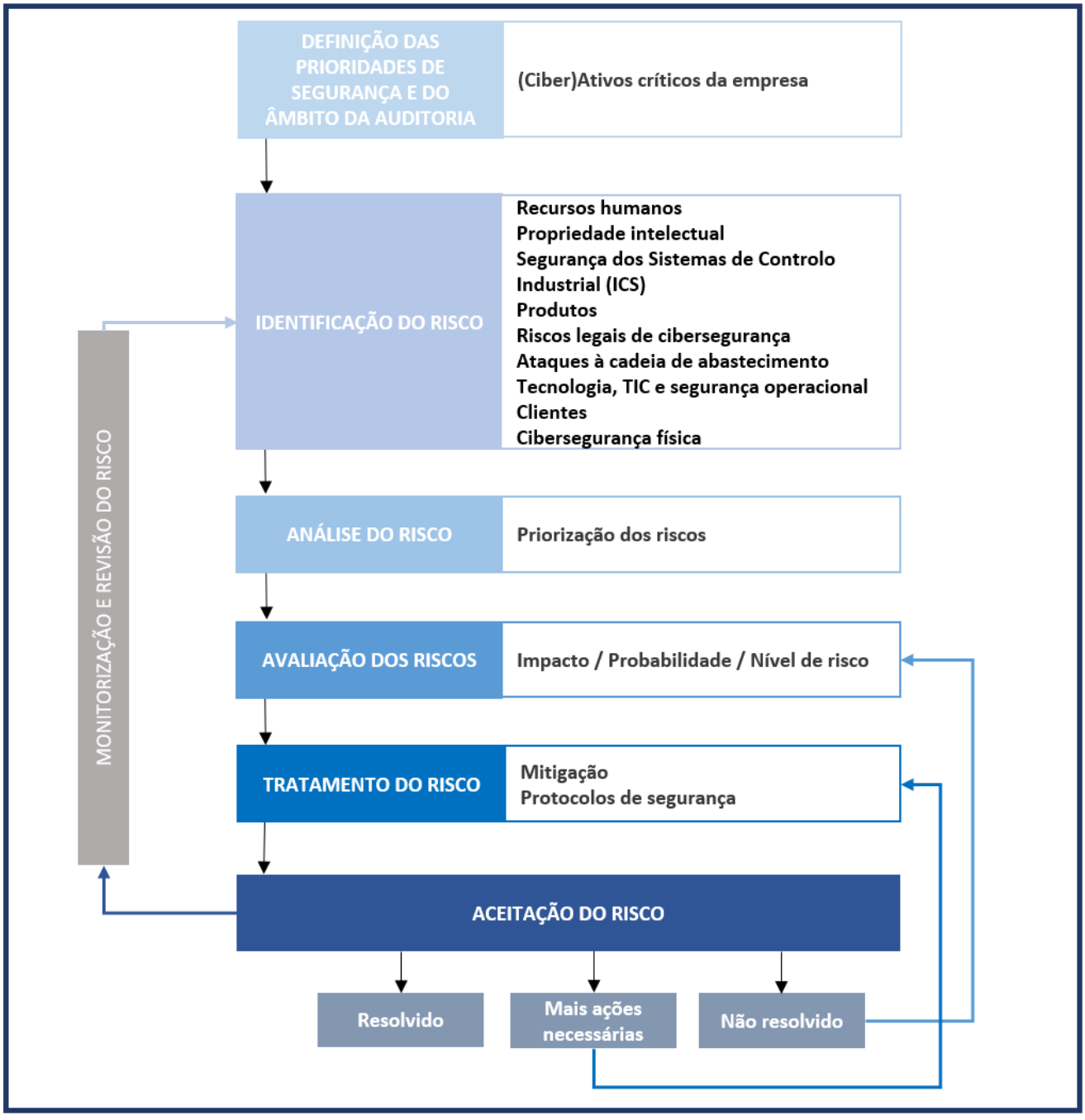
Categoria do risco	Medidas Preventivas	Medidas Corretivas
	Desenvolver soluções de recuperação de desastres e planos de continuidade de negócios	
Propriedade Intelectual	Políticas e responsabilidades adequadas na gestão da propriedade intelectual Todos os ativos aplicáveis devem ser protegidos por patentes registadas, direitos de autor e marcas comerciais. Os ativos relevantes devem ser monitorizados e protegidos por seguros Desenvolvimento de medidas, políticas e responsabilidades na gestão da reputação	Avaliação e atualização regulares das políticas e responsabilidades Se faltar uma patente registada, deve ser obtida uma patente provisória, marca registada e direitos de autor Avaliação e atualização regulares das políticas e responsabilidades
Segurança dos Sistemas de Controlo Industrial (ICS)	Desenvolvimento de medidas, políticas, responsabilidades e resposta rápida em caso de incidência	Avaliação e atualização regulares das políticas e responsabilidades.
Produtos	Avaliação dos processos de fluxo de trabalho Normalização e evolução Controlar o acesso físico a computadores e componentes de rede	Implementar uma abordagem em camadas para cada risco ou pelo menos para aqueles que têm um elevado potencial no caso específico, a fim de ter pelo menos algumas camadas de proteção, não importa quando se trata de tecnologias, funcionários, processos, clientes, etc.
Riscos Legais de Cibersegurança	Mantenha apenas o que precisa. Inventário do tipo e quantidade de informação nos ficheiros e nos computadores Proteção de Informação Destruir antes de eliminar Procedimentos de atualização Formar/Sensibilizar Colaboradores Controlar a utilização do computador Proteger todos os computadores	Identificar as partes afetadas Notificar as pessoas afetadas Procurar aconselhamento jurídico
Ataques à cadeia de abastecimento	Implementar Honeytokens Gestão Segura de Acessos Privilegiados Identificar todos os potenciais canais de informação privilegiada	Verificar as licenças em todas as cadeias de abastecimento das PME Procurar informações de contacto de fornecedores de manutenção preventiva e corretiva de máquinas para PME em toda a

Categoria do risco	Medidas Preventivas	Medidas Corretivas
	Identificar e proteger recursos vulneráveis Minimizar o acesso a dados sensíveis Enviar regularmente avaliações de risco de terceiros Monitorizar possíveis vulnerabilidades na rede de fornecedores Identificar todas as fugas de dados de fornecedores	cadeia de abastecimento a nível local/regional
Tecnologia, TIC e Segurança operacional	Descarregar e instalar atualizações de software para os sistemas operativos e aplicações à medida que ficam disponíveis Atualizar os sistemas operativos e firmware Instalar firewall entre a internet e a LAN Identificar ativos críticos Consciência de segurança Cópias de segurança e recuperação Gestão de vulnerabilidades e correção Aplicar controlos de acesso Utilizar conteúdo e filtrar da lista branca (whitelist) Configurar adequadamente os *endpoints* Estabelecer processos de resposta a incidentes Utilizar sistemas e soluções inteligentes contra ameaças Firewalls devidamente configuradas Políticas rígidas de segurança móvel Encriptação ponta a ponta Registo de auditorias e a autorização de dispositivos de acesso à rede são algumas das práticas que reduzem as ameaças da utilização de dispositivos móveis numa rede empresarial Avaliar o software em relação aos princípios de cibersegurança	Verificar os prazos de sistema e firmware na PME e supervisionar se está tudo atualizado Instalar firewall entre a Internet e a LAN. Remover software ilegal ou não permitido no repositório de software Instalações padrão para todos os equipamentos informáticos Configurar a VPN se for necessário ligar a partir do exterior Identificação e correção do risco. Auditoria e atualização das políticas e regras de segurança.

Categoria do risco	Medidas Preventivas	Medidas Corretivas
	Todos os sistemas operativos e aplicações de software devem estar atualizados Os dados sensíveis devem estar encriptados Utilizar um software de proteção de dados Monitorizar regularmente a atividade das contas de utilizador Gerir definições de privacidade para aplicações móveis Aplicar controlos rigorosos para dispositivos portáteis Estabelecer mecanismos para reconhecer e evitar ataques como phishing e pharming Operar com base em políticas e regras de segurança	
Clientes	Fazer cópias de segurança de dados e informações importantes da empresa	Configurar a autenticação de dois fatores quando possível Bloqueie contas suspeitas de acesso não autorizado Bloquear endereços de IP de suspeitos de ameaças com base em atividades detetadas
Cibersegurança física	Implementar um Plano de Segurança em caso de incêndios, inundações, roubos, perdas... Desligue todas as ferramentas ou equipamentos que não estejam a ser utilizados Ter uma fonte de alimentação ininterrupta e de reserva ou adquirir uma segunda fonte de energia de emergência Verifique regularmente todos os dispositivos Fazer cópias de segurança Ter todos os dados alojados na nuvem	A PME deve ter medidas anti-incêndio em vigor e os responsáveis e funcionários devem estar atualizados sobre a segurança do edifício Para ter uma bateria de reserva para o seu computador ou obter uma segunda fonte de energia de emergência Fazer uma "cópia de segurança" Ter interruptores de segurança Substituir ou reparar dispositivos danificados ou com falhas

VISÃO GRÁFICA DO PROCESSO COM A CRAM

A imagem seguinte apresenta uma visão gráfica do processo de auditoria, utilizando a CRAM Encrypt 4.0 como ferramenta, salientando as medidas correspondentes a serem tomadas pela pessoa responsável para realizar uma análise exaustiva dos seus processos. Esta ferramenta ajuda a identificar os ciber riscos e apoia na conceção e definição dos controlos eficazes em conformidade com a natureza do ciberataque em curso.



A CRAM do ENCRYPT 4.0 é um processo sistemático e contínuo. É um processo cíclico em que, uma vez identificados, analisados, avaliados, dirigidos e aceites os riscos, deve efetuar um processo de controlo e revisão dos riscos. Caso o problema persista, terá de aplicar mais ações complementares para resolver o problema, e para isso terá de voltar ao passo anterior do tratamento de risco. E se o problema não for resolvido, terá de reavaliar o risco.

6. PROJETO E PARCEIROS

ENCRYPT 4.0

Joint Cyber Workforce Development Initiative to Enable The European Industry to Overcome the Shortage of Cybersecurity Professionals

O Projeto ENCRYPT4.0 (2020-1-RO01-KA202-079983) tem como objetivo apoiar os responsáveis das PME a adotar uma abordagem proactiva em relação à cibersegurança, apoiando-as no processo de análise, identificação e combate aos riscos e ameaças cibernéticas aplicáveis à sua organização. Através da elaboração de uma aprendizagem interativa baseada em projetos no que diz respeito ao reforço das competências e competências de cibersegurança dos colaboradores das PME ou/e dos profissionais de cibersegurança.

"George Emil Palade" Universidade de Medicina, Farmácia, Ciências e Tecnologia de Târgu Mureş – Roménia

Coordenador do projeto

European Center for Quality Ltd., Empresa de consultoria – Bulgária

Instituto de Soldadura e Qualidade, Instituição tecnológica - Portugal

Avantalia, PME em tecnologia - Espanha

FH Joanneum, Universidade de Ciências Aplicadas - Áustria

PCX Management, Computadores & Sistemas de Informação Ltd. - Chipre

REFERÊNCIAS BIBLIOGRÁFICAS

Aldorisio, J., 2020. Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist]. Security Scorecard. Retrieved from https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit

Cybersecurity Ventures. (2019). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/annual-cybercrime-report-2019/

Cybersecurity Ventures. (2020). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

EU Agency for Cybersecurity. (2019). *Industry 4.0 Cybersecurity: Challenges & recommendations.*

European Union Agency for Cybersecurity. (2015). *Information security and privacy standards for SMEs - Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* ENISA. doi: 10.2824/829076

Juncker, C. P.-C. (2017). Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

Margot Hutchins, R. B., & Stefanie Robinson, J. S. (2015). Framework for Identifying Cybersecurity Risks in. *U.S. Department of Energy*, 17.

National Institute for Standards and Technology. (2012). *Guide for Conducting Risk Assessments.* Gaithersburg: Special Publication 800-30.

Verizon. (2017). *Verizon Data Breach Investigations Report.* Retrieved from https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/

Verizon. (2020). *Manufacturing*. Retrieved from Verizon: https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/manufacturing-data-breaches/

World Economic Forum . (2017). *Innovation-Driven Ciber-risk to Costumer Data in Financial Services.* Cologny/Geneva.

World Economic Forum. (2020). *The Global Risks Report.*

World Economic Forum. (2020). *Wild Wide Web - Consequences of Digital Fragmentation*. Retrieved from World Economic Forum: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/

ANEXO A - CONJUNTO DE NORMAS EXISTENTES PARA RISCOS DE CIBERSEGURANÇA

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Information Security (Cross-Industry)	ISO/IEC 27001:2018 Information security management systems – Requirements
	ISO/IEC 27002:2018 Code of practice for information security controls
	ISO/IEC 27003:2017 Information security management systems guidance
	ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
	International Organisation for Standardisation and International Electrotechnical Commission
	ISO/IEC 27014:2013 Governance of information security
	ISO/IEC TR 27016:2014 Information security management - Organisational economics
	ISO/IEC 27032:2012 Guidelines for information security
	ISO/IEC 27033-1:2015 Network security - Part 1: Overview and concepts
	ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security
	ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
	ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways
	ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
	ISO/IEC 27033-6:2016 Network security - Part 6: Securing wireless IP network access
	ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts
	ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)
	ISO/IEC 27040:2015 Storage security
	CSA Cloud Controls Matrix
	BSI PAS 555:2013 Cybersecurity risk. Governance and management. Specification
	PCI Data Security Standard
	ISF The Standard of Good Practice for Information Security
	UK Gov. Security policy framework
	UK Gov. Cyber essentials scheme
	ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture
	ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence
	BSI 100-1 Information Security Management Systems (ISMS)
	BSI 100-2: IT- Grundschutz Methodology
	BSI 200-1 Information Security Management Systems (ISMS)
	BSI 200-2: IT- Grundschutz Methodology
	ISO/IEC 15408-1:2009 Evaluation criteria for IT security - Part 1: Introduction and general model

	ISO/IEC 15408-2:2008 Evaluation criteria for IT security - Part 2: Security functional components
	ISO/IEC 15408-3:2008 Evaluation criteria for IT security - Part 3: Security assurance components
	ISO/IEC 19790:2012 Security requirements for cryptographic modules
	ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems
	ISO/IEC 27007:2017 Guidelines for information security management systems auditing
	ISO/IEC 27014:2020 Governance of information security
	ISO/IEC 27017:2015: Code of practice for information security controls based on ISO/IEC 27002 for cloud services
	ISO/IEC 29147:2018: Vulnerability disclosure
	ISO/IEC 30111:2019: Vulnerability handling processes
	OENORM A 7700-3:201910 Web Applications - Part 3: Security requirements
	ISO/IEC 27701:2019 Security techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
	ISO/IEC TS 27100:2020 Information technology -Cybersecurity- Overview and concepts

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Risk Management	ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000
	ISO/IEC 27005:2016 Information security risk management
	ISO/IEC 31000 Risk management - Risk assessment techniques
	IEC 31010:2009 Risk management - Risk assessment techniques
	BSI BIP 0076 Information security risk management. Handbook for ISO/IEC 27001
	BSI 100-3: Risk Analysis based on IT-Grundschutz
	BSI 200-3: Risk Analysis based on IT-Grundschutz
	ISO/IEC 27005:2018 Information security risk management
	ISO/IEC 27102:2019 Information security management — Guidelines for cyber-insurance

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Business Continuity Management	ISO 22301:2012 Business continuity management systems – Requirements
	ISO 22313:2012 Business continuity management systems – Guidance
	ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
	100-4: Business Continuity Management
	OENORM A 7700-4:201910 Web Applications - Part 4: Requirements for secure operations

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Data Protection and Privacy	ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29100:2011 Privacy framework
	ISO/IEC 29101:2013 Privacy architecture framework
	BSI BS 10012:2009 Data protection. Specification for a personal information management system
	CEN CWA 16113:2010 Personal Data Protection Good Practices
	OEVE/OENORM 17529:2020: Data protection and privacy by design and by default
	OENORM A 7700-2:201912 Web Applications - Part 2: Data protection requirements
	ISO/IEC 27018:2019: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29134:2017: Guidelines for privacy impact assessment
	ÖNORM EN 419231:2019 11 01: Protection profile for trustworthy systems supporting time stamping
	ÖNORM EN 419241-1:2019 03 15: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
	ÖNORM EN 419241-2:2019 06 01: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Incident Management	ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management
	ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements
	ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
	ISO/IEC 27035-1:2016 Information security incident management — Part 1: Principles of incident management
	ISO/IEC 27035-1:2016 Information security incident management — Part 2: Guidelines to plan and prepare for incident response

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Third-Party Management	ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts
	ISO/IEC 27035:2011 Information security incident management
	ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

	STANDARDS FOR DATA AND CYBERSECURITY PROTECTION
Industrial security	OVE EN IEC 62443-4-1:2018 11 01: Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
	OVE EN IEC 62443-4-2:2020 01 01: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
	OVE IEC TS 62351-100-1:2020 06 01