EUROPEAN TLD ISAC

# CENTR Member Security Maturity Model

# Registo de alterações

- **Versão 1.0 (31/01/2018)**
  Primeira publicação do CENTR Member Security Maturity Model
- **Versão 1.1 (17/02/2020)**
  Introdução do Nível de Maturidade 0 (ML0) para o tornar mais lógico.
  No caso raro de se ter de responder a uma afirmação de ML1 com um "não", existe um cenário de recurso (ML0 = inexistente).
- **Versão 1.2 (01/03/2022)**
  Aditamento de uma vários termos utilizados no glossário. Pequenas alterações à redação de várias afirmações com base no feedback dos utilizadores.
- **Versão 1.3 (09/01/2024)**
  Alinhamento do modelo com a nova versão da ISO/IEC 27001:2022.

# Créditos

## Agradecimentos


- **Anne-Marie Eklund-Löwinder** (v. 0.68), por rever o modelo,
- **Anthony Hubbard** (v. 1.11) por rever o modelo,
- **Sarah McCreesh** (v. 1.01), pela revisão do documento,
- **Lydia Pernal-Stoddart** (v. 1.01, v. 1.05) pela revisão do documento,
- **Paul Lewis** (v. 1.23) pela revisão do documento.


# Modelo de licenciamento



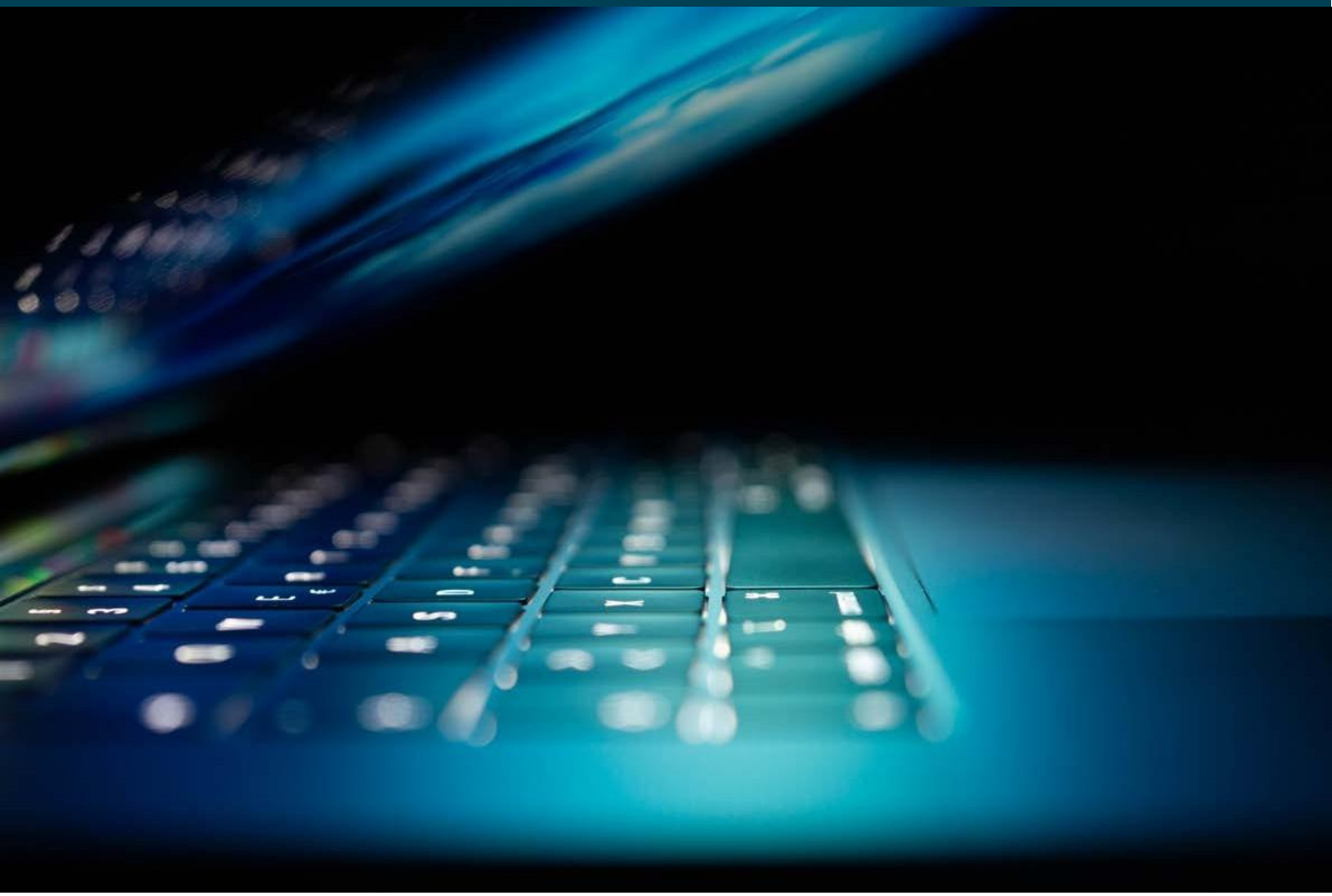
### NOTA DA VERSÃO PORTUGUESA

Este documento é uma tradução para português do documento original publicado pelo CENTR. A tradução apresentada foi realizada no âmbito do programa de capacitação digital da LusNIC e CDA/ICANN, sendo esta fornecida apenas para fins informativos. Em caso de divergência, inconsistência ou dúvida de interpretação, a versão original prevalece.

A LusNIC agradece ao CENTR, entidade responsável pelo documento original, pela produção e disponibilização destes conteúdos, que serviram de base à presente tradução para português, realizada com o objetivo de apoiar a capacitação e a partilha de conhecimento entre os membros da comunidade LusNIC.

# Índice

# Introdução



O CM-SMM (CENTR Member – Security Maturity Model) é uma iniciativa dos membros do CENTR que visa avaliar o nível de maturidade da sua gestão da segurança da informação.

O CM-SMM foi desenvolvida através da incorporação de conceitos provenientes de vários modelos de maturidade (cibersegurança) existentes, normas de segurança e melhores práticas.

A natureza de alto nível do CM-SMM é intencional, uma vez que visa apoiar organizações de diferentes dimensões, cumprindo diferentes normas de segurança (internacionais e/ou nacionais), em cada fase de desenvolvimento.

## O CM-SMM tem como objetivo capacitar as organizações para que estas possam:

- **Reforçar** a sua resiliência e capacidades em matéria de segurança da informação.
- **Permitir** uma avaliação coerente e efetiva das práticas de segurança da informação de referência.
- **Fornecer** meios para avaliar e aferir o desempenho.
- **Identificar** lacunas e desenvolver planos de melhoria.
- **Dar prioridade** a ações e investimentos que melhorem a segurança da informação.
- **Demonstrar** os resultados dos esforços de melhoria.
- **Partilhar** conhecimentos, melhores práticas e capacidades relevantes dentro da organização como forma de melhorar as práticas de segurança da informação.

O CM-SMM oferece uma base abrangente para qualquer organização que pretenda avaliar as suas capacidades de segurança da informação e identificar e avaliar onde os investimentos futuros aportaram os maiores benefícios. Deve ser claramente indicado que a referência CM-SMM tem como âmbito todos os Operadores de Registry.

Contudo, é possível que uma organização específica não consiga completar o modelo na íntegra, ou que um ou mais subdomínios não se apliquem. Nesse caso, o CM-SMM deve ser encarado como uma orientação que oferece uma visão geral; as organizações podem ainda beneficiar deste se se concentrarem nos domínios aplicáveis.

O CM-SMM oferece uma visão geral das melhores práticas, entre outras, nas disciplinas de gestão de riscos, continuidade de negócios e resiliência operacional.

Incorpora as melhores práticas num único modelo que permite às organizações atingir os objetivos de gestão da segurança da informação sem perder o foco da direção estratégica da organização.

Ao avaliar e pontuar a organização em relação ao CM-SMM, é importante ter em conta que o modelo foi elaborado atribuindo igual peso a todos os subdomínios. Isto significa que não é dada prioridade a um subdomínio em detrimento de outro.

# Níveis de maturidade

## Visão geral

O CM-SMM define cinco níveis de maturidade que vão do ML1 ao ML5. Os níveis de maturidade definem uma progressão de maturidade. O ML0 não é considerado um nível de maturidade (tal como o "0" indica) e não é considerado no modelo.

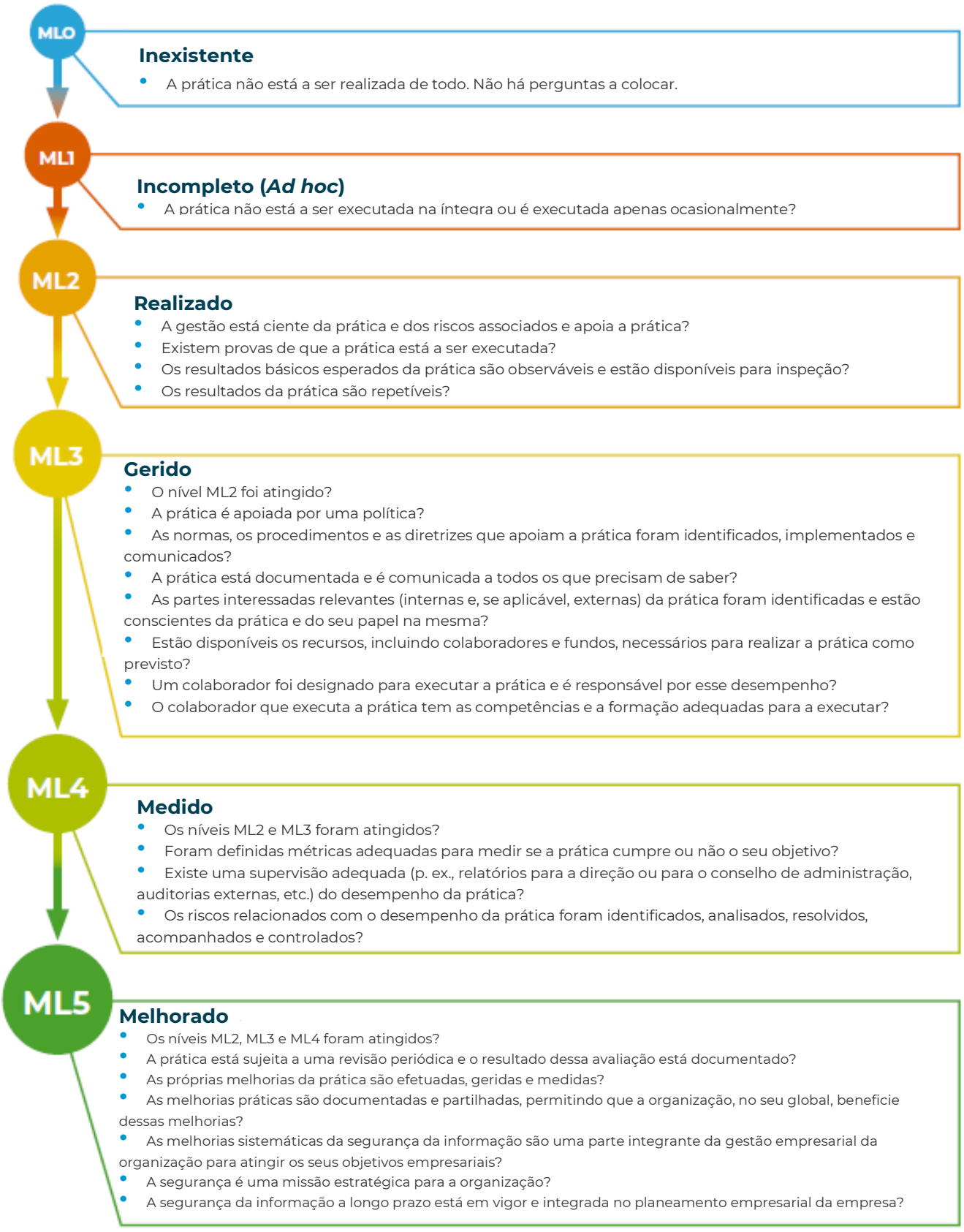
Os níveis de maturidade são cumulativos; para o ML2 e superiores, a prática já deve ter atingido os níveis de maturidade anteriores.


# Determinação do nível indicador de maturidade adequado

O objetivo é determinar corretamente o nível de desempenho adequado. Para auxiliar na aplicação da escala, cada nível de maturidade contém caraterísticas que devem ser observáveis e verificáveis para cumprir os requisitos desse nível antes de se avançar para um nível superior.

# Determinação das características de cada nível indicador de maturidade

Para ajudar a formular as afirmações adequadas para cada nível, podem-se utilizar as seguintes perguntas como orientação.



# Domínios

## 1 Estabelecer

### Estratégia de segurança da informação

Uma estratégia de segurança da informação é um grupo integrado de atividades concebidas e geridas para cumprir os objetivos de segurança da informação da organização. Fornece governação, planeamento estratégico e patrocínio para as atividades de segurança da informação da organização de forma a alinhar os objetivos de segurança da informação com os objetivos estratégicos da organização e com o risco para as infraestruturas (críticas).

#### 1. Estabelecer uma estratégia de segurança da informação

**ML1**

- Existem alguns componentes ou elementos, mesmo de forma simplista, de uma estratégia de segurança da informação, independentemente de fornecerem ou não diretivas acionáveis.

**ML2**

- Foi elaborado um esboço genérico de uma estratégia de segurança da informação de alto nível.
- No mínimo, a estratégia deve referir-se à missão da organização e à estratégia empresarial, e deve incluir as intenções da organização de salvaguardar a informação que processa e/ou detém.
- A estratégia é revista, pelo menos, numa base *ad hoc* e o seu alinhamento com os objetivos empresariais é, no mínimo, limitado.
- A direção tem um conhecimento básico das principais ameaças e dos potenciais riscos para a segurança da informação.

**ML3**

- Está operacional e a funcionar uma estratégia pormenorizada de segurança da informação alinhada com os objetivos empresariais.
- A estratégia está ligada aos riscos, prioridades e objetivos organizacionais e fornece diretivas acionáveis.

- A estratégia de segurança da informação estabelece objetivos (de segurança) a longo prazo, determinando o estado atual da organização e o estado desejado em matéria de segurança da informação. O horizonte de planeamento deve abranger um período de vários anos.
- A estratégia de segurança da informação serve de guia para estabelecer o sistema de gestão da segurança da informação (1) e adaptá-lo aos desafios futuros.

**ML4**

- Os processos de revisão e renovação da estratégia são efetuados com regularidade.
- São implementados processos de medição para ajudar a gestão a avaliar a eficácia dos diferentes objetivos de segurança da informação, a eficácia da atenuação dos riscos relacionados com a segurança da informação e para orientar a alocação de fundos.

**ML5**

- A estratégia de segurança da informação é alvo de escrutínio, aperfeiçoamento e adaptação periódicas para se manter atualizada e pertinente num mundo em que as ciberameaças e a tecnologia evoluem rapidamente.

## 2. Desenvolver um sistema de gestão da segurança da informação

**ML1**

- Existem algumas políticas e procedimentos para gerir a informação de forma segura. O sistema de gestão da segurança da informação pode ainda estar incompleto.

**ML2**

- O sistema de gestão da segurança da informação é estabelecido de acordo com a estratégia de segurança da informação.
- São disponibilizados fundos adequados e outros recursos (ou seja, pessoas e ferramentas) para apoiar a criação e o funcionamento do sistema de gestão da segurança da informação.
- A direção patrocina de forma visível e ativa (p. ex., a importância e o valor das atividades de segurança da informação são regularmente comunicados pela direção) o sistema de gestão da segurança da informação.

## ML3

- A organização constrói o seu sistema de gestão da segurança da informação a partir da legislação aplicável, regulamentos e normas aplicáveis, desenvolvendo várias políticas organizacionais, diretrizes e processos integrados de segurança da informação que formam o sistema de gestão global.
- Os processos de segurança da informação estabelecem critérios (p. ex., inputs necessários para o processo, etapas importantes necessárias, outputs do processo, critérios de desempenho - p. ex., objetivos mensuráveis,...) necessários para atingir os objetivos de segurança da informação.
- O sistema de gestão da segurança da informação reforça a sensibilização e as competências da organização em matéria de segurança da informação, procura melhorar a eficácia da gestão da segurança da informação e estabelece capacidades de prevenção, deteção, resposta e recuperação de incidentes.
- A gestão dos riscos da organização é uma componente essencial do sistema de gestão da segurança da informação.
- O sistema de gestão da segurança da informação reflete-se numa política de segurança da informação escrita que é disponibilizada aos colaboradores da organização.
- A política de segurança da informação é interpretada em regras e diretrizes de segurança da informação e comunicada aos colaboradores da organização.
- As alterações ao sistema de gestão da segurança da informação estão a ser implementadas de forma planeada. Fatores como o objetivo da alteração, o potencial impacto noutros processos do SGSI, a disponibilidade de recursos e a alocação ou realocação de responsabilidades e autoridades são tidos em consideração.

## ML4

- A eficácia do sistema de gestão da segurança da informação é monitorizada com base em critérios estabelecidos a fim de garantir o seu alinhamento com a estratégia global de segurança da informação.
- O sistema de gestão da segurança da informação é revisto de forma independente (ou seja, por revisores que não são responsáveis pela sua aplicação) para atingir os objetivos do sistema de gestão da segurança da informação.
- O sistema de gestão da segurança da informação abrange o acompanhamento e/ou a participação em normas e iniciativas de segurança da informação selecionadas pela indústria.

**ML5**

- O sistema de gestão da segurança da informação contém um processo de melhoria que incorpora o resultado da análise das causas dos incidentes, os ciclos de revisão periódica e o esforço de monitorização.

# Governação e conformidade

Um processo organizacional que proporciona uma direção estratégica para a organização, assegurando simultaneamente que esta cumpre as suas obrigações, gere adequadamente os riscos e utiliza eficazmente os recursos humanos (RH) e financeiros. Por norma, a governação inclui também os conceitos de patrocínio, conformidade e alinhamento com os objetivos estratégicos.

A conformidade indica que a organização está a funcionar de acordo com as leis, regulamentos, obrigações contratuais, normas e políticas internas estabelecidas que decidiu implementar.

## 1. Estabelecer uma estratégia de gestão da governação

**ML1**

- A organização reconhece a necessidade de segurança da informação, pelo menos de forma limitada.
- A organização tem em consideração, até certo ponto, os impactos empresariais associados às vulnerabilidades de segurança e às incertezas dos projetos empresariais. A gestão do risco pode ainda não ter sido identificada como relevante para a aquisição de soluções de processamento da informação e para a prestação de serviços.
- Existe, pelo menos, uma compreensão limitada dos riscos, vulnerabilidades e ameaças às instalações de tratamento da informação ou do impacto da perda de serviços na atividade. A continuidade do serviço pode não ser identificada ou considerada como necessitando de atenção por parte da gestão empresarial.
- As responsabilidades e a responsabilização são atribuídas, pelo menos vagamente, para garantir a segurança.
- A segurança da informação é abordada, mesmo que numa base reativa e/ou quando não é medida.
- Os recursos de segurança da informação são atribuídos e geridos de forma *ad hoc*.

## ML2

- Existem políticas de segurança autónomas, mas não estão necessariamente incorporadas nos processos empresariais primários e críticos da organização.
- São efetuadas avaliações informais dos riscos do projeto, pelo menos numa base *ad hoc*, conforme determinado por cada projeto. A necessidade de tais avaliações pode não estar prevista na política da empresa.
- As responsabilidades e a responsabilização pela segurança da informação são atribuídas a um coordenador da segurança da informação, possivelmente sem autoridade de gestão.
- As responsabilidades pela segurança da informação são atribuídas, mas podem não ser aplicadas de forma consistente.
- A sensibilização para a segurança é generalizada, mas pode ainda faltar uma estratégia para aumentar a sensibilização global e pessoal dos colaboradores e consultores que atuam em funções semelhantes.
- No mínimo, a segurança tende a responder de forma reativa aos incidentes de segurança da informação, mas possivelmente sem dar resposta às necessidades específicas da organização.
- Os relatórios de segurança da informação são, pelo menos, orientados para a técnica, embora seja preferível que sejam orientados para a atividade.
- Os recursos de segurança da informação são geridos no âmbito de projetos e operações diárias, mas pode faltar um orçamento de segurança a nível empresarial.
- A direção promove ocasionalmente a importância da segurança da informação para a organização.

## ML3

- O desenvolvimento e a manutenção de políticas de segurança da informação são patrocinados.
- Os processos de segurança da informação são coordenados com as funções e/ou processos empresariais globais da organização.
- A direção identifica os processos críticos de informação e empresarial da organização.
- A direção determinou os níveis de risco que a organização tolera.
- Uma política de gestão de risco para toda a organização define quando e como realizar avaliações de risco. As avaliações de risco seguem um processo definido documentado e disponibilizado a todos os colaboradores para ajudar a melhorar o seu empenhamento e por uma questão de transparência.

- A responsabilidade pelo sistema de gestão da segurança da informação é atribuída a uma função com a autoridade necessária e o apoio da direção.
- A sensibilização para a segurança existe e é promovida pela gestão. As reuniões de sensibilização para a segurança foram normalizadas e formalizadas.
- A direção comunica constantemente a necessidade de salvaguardar a confidencialidade, a integridade e a disponibilidade dos serviços da organização.
- A segurança da informação é um tema recorrente na ordem de trabalhos das reuniões do conselho de administração.
- O planeamento dos recursos de segurança da informação é parte integrante do planeamento financeiro e da gestão orçamental da organização.
- A segurança da informação está integrada nos objetivos de segurança da empresa e os requisitos de informação estão ligados aos objetivos empresariais.

## ML4

- A medida em que os esforços de segurança da informação são alinhados com a estratégia empresarial para apoiar os objetivos organizacionais é monitorizada e os resultados são comunicados à direção e ao conselho de administração.
- A eficácia do processo de gestão da segurança da informação é controlada e os resultados são comunicados à direção e ao conselho de administração.
- A eficácia do processo de gestão de risco empresarial é controlada e os resultados são comunicados à direção e ao conselho de administração.
- A eficácia do programa de sensibilização empresarial é controlada e os resultados são comunicados à direção e ao conselho de administração.
- A eficácia dos investimentos em segurança da informação é controlada e os resultados são comunicados à direção e ao conselho de administração.

## ML5

- A direção assegura a eficácia da política de segurança da organização através da sua revisão e aprovação numa base regular.
- As responsabilidades documentadas dos colaboradores em matéria de segurança da informação (2) são revistas regularmente para validar se continuam completas e se refletem a estrutura organizacional atual.

- A direção melhora continuamente a gestão da segurança da informação para cumprir as responsabilidades da organização e as expectativas relevantes das partes interessadas internas e externas.
- Os programas de sensibilização são incorporados nos processos de RH, como o planeamento do desenvolvimento pessoal.
- Os investimentos em segurança da informação são otimizados para apoiar a realização dos objetivos organizacionais. O orçamento para a segurança é alocado e gasto com as pessoas, processos e tecnologia adequados, para que os objetivos gerais da organização possam ser alcançados.

## 2. Estabelecer uma estratégia de gestão da conformidade

Embora relacionadas, a gestão da conformidade (3) e a gestão do risco são distintas. A gestão do risco envolve prever e gerir riscos para ajudar uma organização a proteger-se dos riscos que podem eventualmente conduzir ao incumprimento. Por outro lado, a gestão da conformidade envolve gerir a conformidade dentro dos limites de um prazo e de um orçamento. A não conformidade com os regulamentos de conformidade é também um risco.

**ML1**

- Existem procedimentos e responsabilidades que informam sobre como a conformidade é gerida na organização.
- Realiza-se um acompanhamento *ad hoc* das alterações regulamentares.

**ML2**

- Uma estratégia de conformidade, de preferência centralizada, foi implementada.
- A organização monitoriza periodicamente as alterações regulamentares. As obrigações de conformidade são identificadas e documentadas. Estas constituem a base para as práticas que a organização tem de implementar para cumprir as obrigações.
- A organização identificou e documentou as normas da indústria e as melhores práticas de segurança da informação que pretende cumprir. Os colaboradores são instados a respeitá-las nas suas operações diárias.

## ML3

- O colaborador (ou departamento) responsável pela conformidade envolve a direção, fornecendo um inventário das obrigações de conformidade (internas e externas) que funciona como uma base a partir da qual novas obrigações podem ser identificadas e integradas nos processos de conformidade da organização.
- A documentação das obrigações de conformidade é utilizada para identificar e analisar os riscos decorrentes da gestão de projetos e mudanças.
- A organização tem um processo formal de aceitação de riscos de conformidade e de responsabilização pelo cumprimento das obrigações de conformidade. A abordagem formal mapeia as obrigações legais e regulamentares aplicáveis, as quais são documentadas e utilizadas para demonstrar como a organização as cumpre.
- A organização desenvolveu uma política de segurança da informação, que é apoiada por procedimentos e diretrizes, que exprime a intenção de proteger a informação, que estabelece as regras para o comportamento esperado dos processadores de informação, que define e autoriza as consequências da violação, que define a base de segurança da organização, que ajuda a minimizar o risco e que ajuda a acompanhar o cumprimento das leis e regulamentos.
- A organização assegura que os acordos com terceiros não põem em causa a gestão da conformidade, garantindo que os novos contratos são compatíveis com a política de segurança da organização.

## ML4

- A organização mede o nível de conformidade, em linha com os seus objetivos estratégicos.
- São divulgados relatórios periódicos de conformidade sobre a situação atual da organização em matéria de conformidade.

## ML5

- A gestão da conformidade é utilizada para tomar decisões centradas na organização. A conformidade está integrada na cultura organizacional e faz parte dos processos empresariais.
- O processo de conformidade é periodicamente revisto, melhorado e adaptado conforme necessário.

# Gestão de risco

A gestão do risco centra-se no estabelecimento e manutenção de processos internos que identificam, analisam e tratam os riscos de segurança da informação para a organização, para os seus ativos críticos, para as suas filiais e para as partes interessadas. Ao estabelecer um processo de gestão de riscos deste tipo, as organizações estão preparadas para agir de forma proativa e não reativa. Ao acompanhar a evolução dos riscos de segurança da informação, as organizações devem esforçar-se por recolher e documentar informações que lhes permitam avaliar as ameaças e os perigos para as suas operações e agir de forma adequada.

## ML1

- Existe um conhecimento aproximado dos riscos de segurança da informação a nível da organização e/ou do segmento de atividade.
- As avaliações de risco estão a ser realizadas, pelo menos ocasionalmente.
- As opções de tratamento dos riscos inaceitáveis são identificadas e as ações são selecionadas. No mínimo, são implementadas ações de tratamento dos riscos inaceitáveis.
- Os responsáveis pelos riscos devem ser identificados para os riscos inaceitáveis.

## ML2

- Os riscos organizacionais, estratégicos e operacionais são conhecidos, ou identificados e documentados. Existe alguma forma de comunicação à direção.
- A avaliação dos riscos operacionais faz parte das tarefas e responsabilidades do departamento de TIC.
- As avaliações de risco incluem a ameaça, os controlos de mitigação existentes e a pontuação do risco.
- Os responsáveis pelos riscos são identificados para todos os riscos documentados.
- O resultado das avaliações de risco é transmitido à direção.
- Os planos de tratamento de riscos para riscos inaceitáveis são definidos, documentados e têm alguma forma de patrocínio da gestão.
- Os resultados do tratamento dos riscos são documentados.

## ML3

- Os riscos organizacionais, estratégicos e operacionais são recolhidos e documentados regularmente e com uma frequência adequada (p. ex., como parte de informações sobre ameaças, gestão da mudança, gestão de projetos, análises de incidentes, relatórios de auditoria, etc.).
- As avaliações de risco são realizadas formalmente e de forma consistente, e existem responsáveis pelos riscos nomeados (a nível de gestão) para cada risco individual.

- As avaliações de risco são exaustivas e bem documentadas. Aplicam-se medidas coerentes que têm em consideração todos os segmentos da atividade.
- Os responsáveis pelos riscos e pela segurança da informação reúnem-se regularmente, e *ad hoc* se necessário, para avaliar novos riscos e discutir os controlos aplicados.
- Um registo de riscos (um repositório estruturado de riscos organizacionais, estratégicos e operacionais identificados) circula no seio da organização em conformidade com o princípio da necessidade de saber (4) e é utilizado para apoiar as atividades de gestão dos riscos.
- Os responsáveis pelos riscos são responsáveis pela aceitação do risco e pela execução do(s) plano(s) de tratamento do risco definido(s).
- Os planos de tratamento dos riscos são classificados por ordem de prioridade e incluídos no planeamento empresarial.
- A organização desenvolveu uma política de gestão do risco que especifica a metodologia de gestão do risco adotada e que é apoiada por procedimentos e diretrizes.
- Os indicadores de gestão do risco são definidos e comunicados à direção.

**ML4**

- A recolha de riscos organizacionais, estratégicos e operacionais é periodicamente avaliada e atualizada. Existe uma visão geral pormenorizada e bem documentada dos riscos organizacionais, estratégicos e operacionais - que pode fazer parte do seu catálogo de riscos - revista, atualizada e divulgada no seio da organização de forma periódica e de acordo com o princípio da necessidade de saber.
- A progressão dos planos de tratamento de riscos e de outras medidas definidas durante as avaliações de riscos é monitorizada e comunicada à direção.

**ML5**

- O próprio processo de delimitação do âmbito e de identificação dos riscos é reavaliado periodicamente para captar e adaptar-se às mudanças no ambiente de risco da segurança da informação.
- São investigados métodos e/ou fontes alternativas para identificar novos riscos ou alterações aos riscos existentes.
- O processo de avaliação e tratamento dos riscos e as políticas e procedimentos relacionados são revistos regularmente e, se necessário, melhorados.
- Os relatórios sobre a avaliação e o tratamento dos riscos são apresentados periodicamente à direção e/ou ao conselho de administração, que incorpora a avaliação no futuro planeamento operacional e/ou estratégico.

# Gestão da força de trabalho

A gestão da força de trabalho facilita uma organização consciente da segurança, estabelecendo e mantendo planos, procedimentos, controlos e tecnologias para criar uma cultura de segurança da informação e para garantir a adequação e competência permanentes do pessoal.

## 1. Responsabilidades em matéria de segurança da informação

**ML1**

- As responsabilidades em matéria de segurança da informação são identificadas e atribuídas a colaboradores específicos, eventualmente a um nível mais informal.

**ML2**

- As responsabilidades em matéria de segurança da informação são identificadas a nível empresarial.
- As responsabilidades pela segurança da informação são atribuídas de acordo com as competências.

**ML3**

- As responsabilidades e obrigações em matéria de segurança da informação são atribuídas a papéis e funções específicos.
- As responsabilidades pela segurança da informação são atribuídas a prestadores de serviços externos.
- As responsabilidades pela segurança da informação são documentadas (p. ex., em descrições de cargos).
- As responsabilidades pela segurança da informação são geridas de forma a garantir uma cobertura adequada e redundante.

**ML4**

- As responsabilidades pela segurança da informação são incluídas nos critérios de avaliação do desempenho das funções.

**ML5**

- As responsabilidades em matéria de segurança da informação e os requisitos das funções são regularmente revistos e atualizados para satisfazer as necessidades da organização e para antecipar ou responder a alterações na organização ou no panorama da segurança da informação.

## 2. Desenvolver e controlar a segurança da informação durante o ciclo de vida da força de trabalho

### ML1

- No mínimo, existe um número limitado de procedimentos de recursos humanos que incluem controlos da segurança da informação.
- Os candidatos são submetidos a um número mínimo de controlos de antecedentes (p. ex., verificação de identidade) antes de serem contratados.

### ML2

- A verificação básica do pessoal (ao abrigo das obrigações legais e regulamentares relevantes) é realizada durante o processo de contratação para todos os cargos.
- Os procedimentos de integração, alteração e cessação de funções do pessoal abordam sistematicamente a segurança da informação.
- A formação em segurança da informação é disponibilizada ao pessoal com responsabilidades atribuídas em matéria de segurança da informação.

### ML3

- Os acordos contratuais com pessoal incluem as suas responsabilidades em matéria de segurança da informação, utilização aceitável dos ativos da empresa e procedimentos de devolução de ativos.
- As funções, responsabilidades, competências e qualificações em matéria de segurança da informação estão incluídas nos perfis de funções de todo o pessoal. Estas descrições de funções refletem as expectativas de segurança da informação da direção relativamente ao seu papel na organização.
- Antes de conceder acesso aos ativos que suportam a função (p. ex., novos funcionários ou mudanças de posição), os colaboradores recebem formação em segurança da informação e, se forem considerados essenciais, são submetidos a uma verificação mais exaustiva. Se a organização determinar que é necessária uma verificação exaustiva, esta é realizada a intervalos regulares para garantir a adequação contínua do pessoal em causa.
- Para funções/cargos com elevado risco de fraude ou erros que possam conduzir a incidentes graves, é implementada uma separação de funções.
- As formações de sensibilização são ministradas ao pessoal com base na exposição ao risco.

## ML4

- Os programas de formação são alinhados para apoiar os objetivos de segurança da informação empresarial.
- São identificadas lacunas de conhecimentos, competências e aptidões em matéria de segurança da informação. As lacunas identificadas são colmatadas através de recrutamento e/ou formação.
- A eficácia dos programas de formação é avaliada com uma frequência definida pela organização.
- Os incidentes relacionados com violações de políticas e procedimentos por parte do pessoal são recolhidos e analisados, sendo disponibilizado à gestão um relatório de alto nível.

## ML5

- Os programas de formação incluem educação contínua e oportunidades de desenvolvimento profissional para o pessoal com responsabilidades significativas em matéria de segurança da informação. O planeamento da sucessão do pessoal é efetuado com base nas suas funções, responsabilidades e plano de desenvolvimento pessoal.
- As cláusulas e diretrizes relacionadas com a segurança da informação nas políticas e procedimentos de RH são revistas periodicamente para avaliar a sua eficácia e identificar oportunidades de melhoria (p. ex., com base em relatórios de gestão de incidentes, conclusões de auditorias).

# Gestão de ativos

A gestão de ativos é um processo sistemático de desenvolvimento, exploração, manutenção, modernização e eliminação de ativos de forma eficaz em termos de custos.

A gestão dos ativos centra-se principalmente na identificação dos ativos de infraestruturas críticas, vitais para os processos empresariais, e em que uma perturbação desses ativos teria um impacto substancial na segurança e nas atividades operacionais globais da organização.

## ML1

- Os ativos TIC são inventariados.

## ML2

- Existe um inventário dos ativos da infraestrutura de informação (p. ex., edifícios, salas de dados, routers, servidores). Pode-se ter realizado uma categorização formal dos ativos de infraestrutura críticos para as atividades operacionais.
- Existe um inventário dos ativos de informação (p. ex., licenças de software, informações sobre clientes, dados financeiros, registos). Pode-se ter realizado uma categorização formal dos ativos de informação críticos para as atividades operacionais.
- É necessário realizar um inventário dos ativos para desenvolver, operar e manter as necessidades de proteção (p. ex., pessoal, competências, capacidades, trabalho remoto). Pode-se ter realizado uma categorização formal destes ativos críticos para as atividades operacionais.

## ML3

- É implementado um processo documentado de gestão de ativos para todo o inventário de ativos. O processo abrange todo o ciclo de vida do ativo, incluindo a propriedade e a classificação.
- Os atributos do inventário incluem informações para apoiar os requisitos de proteção e manutenção. No mínimo, incluem a localização, o tipo, o proprietário do ativo e a sua importância para a empresa. Outros metadados podem ser dependências de serviço, acordos ao nível de serviços, requisitos de segurança aplicáveis, conformidade dos ativos com as normas relevantes da indústria, etc.
- Os ativos inventariados são classificados em termos de impacto (confidencialidade, integridade e/ou disponibilidade) nas atividades operacionais que apoiam em caso de indisponibilidade, dano, roubo, modificação não autorizada, etc.
- Os bens inventariados são classificados por ordem de prioridade com base na análise do impacto potencial em caso de interrupção de serviço (é feita uma distinção entre bens críticos e serviços essenciais para as atividades quotidianas), ou indisponibilidade ou perda de informação e sistemas de tratamento da informação.

- A utilização aceitável dos ativos (incluindo o tratamento de cópias temporárias ou permanentes da informação, à sua transferência eletrónica, física ou verbal e o acesso autorizado) está documentada numa política destinada a sensibilizar para os riscos associados à segurança da informação e a fornecer orientações aos colaboradores sobre a utilização desses ativos.
- Existe um processo que descreve as etapas para devolver, reutilizar e eliminar todos os ativos da organização de forma segura após a cessação do emprego, contratos ou acordos.

## ML4

- Foi estabelecido um procedimento documentado para controlar as alterações ao inventário de ativos. O inventário de ativos está atualizado (tal como definido pela organização).
- O impacto potencial dos ativos inventariados na confidencialidade, integridade e/ou disponibilidade das atividades operacionais que apoiam é reavaliado periodicamente para se adaptar às alterações no ambiente de risco da segurança da informação.
- Regularmente, realiza-se uma avaliação pormenorizada dos ativos críticos e as oportunidades de melhoria identificadas são tratadas.
- A eficácia da política de utilizadores aceitáveis é medida através do programa de sensibilização da organização e/ou da gestão de incidentes.

## ML5

- O próprio processo de gestão de ativos é periodicamente reavaliado para captar e adaptar-se às mudanças no ambiente de risco da segurança da informação.
- As oportunidades de melhoria, identificadas a partir da monitorização e revisão dos processos de identificação e classificação de ativos, são incorporadas no guia empresarial da organização.
- Existe um procedimento estabelecido para garantir que as atualizações do inventário não podem ser ignoradas no processo de instalação, alteração e/ou remoção de um ativo.

# Gestão da cadeia de abastecimento

Os fornecedores externos e os serviços de computação em nuvem são uma componente importante das operações empresariais. Os fornecedores podem ter acesso a uma vasta gama de informações da organização apoiada. Uma vez partilhadas com um fornecedor ou um prestador de serviços de computação em nuvem, perde-se o controlo direto destas informações, independentemente da sua sensibilidade ou valor. Consequentemente, devem-se estabelecer controlos adequados e processos de mitigação com todos os fornecedores externos.

## ML1

- Pelo menos algumas das dependências de fornecedores e/ou riscos relacionados com fornecedores são identificados e geridos.
- A segurança é abordada nos acordos empresariais mais importantes.

## ML2

- As dependências importantes dos fornecedores (p. ex., fonte única, etc.) são identificadas e classificadas por ordem de prioridade.
- Os requisitos de segurança da informação são tidos em conta aquando do estabelecimento de relações com fornecedores e outros terceiros.
- As dependências dos fornecedores e outros riscos significativos para a segurança da informação associados aos fornecedores são identificados e tratados.
- Os acordos com fornecedores exigem a notificação de incidentes de segurança da informação relacionados com a entrega do produto ou serviço.

## ML3

- Os requisitos de segurança da informação são estabelecidos para os fornecedores de acordo com práticas definidas, incluindo requisitos para o desenvolvimento seguro de software e práticas de engenharia, quando apropriado.
- Os critérios para a seleção de fornecedores num processo de aquisição, o tipo e a natureza da colaboração prevista com as obrigações mútuas daí resultantes e os critérios para a revisão regular das relações contratuais existentes estão documentados e estabelecidos.
- A avaliação e seleção de fornecedores e outras entidades externas inclui a consideração da sua capacidade para cumprir os requisitos de segurança da informação da organização.
- As dependências dos fornecedores são identificadas e classificadas por ordem de prioridade com base nos critérios de risco da função ou da organização e são incluídas nas avaliações de risco.
- O pessoal externo identificado como tendo um envolvimento significativo nas operações ou desenvolvimentos quotidianos faz parte do programa de sensibilização.

- Os produtos e/ou serviços das entidades externas são incluídos na gestão da capacidade da própria organização e na gestão da continuidade de Negócios (BCM).
- As responsabilidades entre a organização e os fornecedores externos e os direitos de propriedade da informação e dos ativos decorrentes da relação contratual (p. ex., código) estão regulamentados.
- Existe um plano para a transferência, eliminação e manutenção da confidencialidade da informação caso um fornecedor cesse as suas atividades ou um produto/serviço ou no caso de uma relação contratual terminar de forma regular.

**ML4**

- Os fornecedores e outras entidades externas são periodicamente analisados quanto à sua capacidade de cumprir continuamente os requisitos de segurança da informação (tal como definidos nos acordos).
- Os produtos e serviços são verificados, testados e/ou monitorizados para garantir que cumprem os requisitos previstos e não têm quaisquer efeitos indesejáveis.

**ML5**

- Os requisitos de segurança da informação aplicáveis aos fornecedores são regularmente revistos e atualizados para satisfazer as necessidades da organização e para antecipar ou responder a alterações na organização ou no panorama da segurança da informação.
- O próprio processo de seleção de fornecedores é periodicamente reavaliado para captar e adaptar-se às mudanças no ambiente de risco da segurança da informação, com base em análises de fornecedores, produtos, serviços, etc.

# 2 Prevenir

## Gestão da mudança

A gestão da mudança centra-se em abordagens para preparar e apoiar as pessoas, os processos e a tecnologia afetados por uma mudança organizacional. Num contexto de gestão de projetos, refere-se ao processo de controlo de alterações em que as alterações ao âmbito de um projeto são formalmente introduzidas e aprovadas.

### ML1

- As atividades e os procedimentos associados à gestão das alterações, como a apresentação de pedidos de alteração e a avaliação do impacto, são concluídos, pelo menos, de forma *ad hoc*.

### ML2

- As alterações significativas que afetam a segurança da informação são identificadas e registadas.
- As alterações significativas são objeto de avaliações de risco e os riscos (e benefícios) associados são comunicados à gestão antes de as alterações serem implementadas.
- Sempre que possível, as alterações aos ativos são testadas antes de serem implementadas.

### ML3

- As práticas de gestão das alterações abrangem todo o ciclo de vida dos ativos (ou seja, aquisição, implementação, funcionamento, retirada e eliminação).
- As práticas de gestão das alterações incidem sobre as alterações efetuadas pelos fornecedores aos serviços que oferecem.
- São disponibilizados recursos adequados (pessoas, financiamento e ferramentas) para apoiar as atividades de gestão da mudança.
- Existe um processo formal de gestão da mudança com responsabilidades atribuídas às partes interessadas, que inclui procedimentos documentados.
- Existe um procedimento formal de aprovação das alterações propostas. As alterações são avaliadas para cumprir os requisitos de segurança aplicáveis.
- Os pormenores das alterações são comunicados a todos os intervenientes relevantes.
- As alterações são priorizadas e planeadas.
- É estabelecido um processo de alteração de emergência para permitir a implementação rápida e controlada das alterações necessárias para resolver um incidente.
- São desenvolvidos procedimentos de recurso para abortar e recuperar de alterações sem sucesso.

## ML4

- As alterações aos ativos são monitorizadas para validar o facto de cumprirem as metas e objetivos estratégicos, incluindo a segurança da informação (p. ex., sendo validadas por um comité de projeto ou pelo proprietário da empresa, cumprindo os requisitos funcionais ou não funcionais da empresa, etc.).
- Os resultados das alterações são revistos para validar a sua eficácia e a medida em que satisfazem as expectativas das partes interessadas (processo de feedback).
- As atividades de gestão da mudança são revistas periodicamente para garantir a sua conformidade com a política e validar à sua eficácia.

## ML5

- O processo de gestão das alterações contém uma via de melhoria baseada nos resultados dos ciclos periódicos de revisão das alterações e no esforço de monitorização especificado no ponto ML4.
- O próprio processo de gestão de ativos é periodicamente reavaliado para captar e adaptar-se às mudanças no ambiente de risco da segurança da informação.

# Gestão da configuração e automação

A gestão da configuração é um processo de governação e engenharia de sistemas que assegura a correta contabilização dos elementos de configuração de uma empresa, dos seus atributos físicos e capacidades funcionais e da inter-relação entre eles num ambiente operacional.

A gestão da automação é o processo de automatização do ciclo de vida da configuração e do software de uma infraestrutura. Ambos os processos apoiam a gestão da mudança.

## ML1

- No mínimo, são dados os passos iniciais para a gestão da configuração dos ativos de serviço e dos elementos da infraestrutura.

## ML2

- São estabelecidas linhas de base de configuração para os bens inventariados, sempre que seja desejável assegurar que múltiplos bens de serviço ou elementos de infraestrutura sejam configurados de forma semelhante.
- A automação (5) é implementada quando vários ativos ou elementos necessitam da mesma configuração.
- As linhas de base de configuração são utilizadas para configurar os ativos de serviço e os elementos da infraestrutura aquando da implementação.
- A automação está em vigor para garantir que os ativos e itens adequados satisfazem a linha de base de configuração.
- A automação é criada para evitar alterações de configuração não autorizadas ou incorretas.

## ML3

- A conceção das linhas de base de configuração inclui objetivos de segurança da informação e baseia-se em normas, diretrizes e melhores práticas de segurança da indústria.
- Os elementos de configuração são armazenados e continuamente atualizados numa base de dados de gestão da configuração.
- Todas as configurações associadas a software e hardware (quando exequível) nos diferentes ambientes (TIC) é gerida através da automação.
- Os elementos de configuração e as linhas de base de configuração (6) são documentados para poderem ser imediatamente (re)aplicados em caso de emergência ou de recuperação de desastres.

- A responsabilidade e a autoridade pelo desempenho das atividades de configuração dos bens de serviço e dos elementos da infraestrutura são atribuídas ao pessoal.
- As linhas de base de configuração devem apoiar a política de segurança da informação da organização e outros requisitos de segurança necessários para os ativos a que se aplicam e garantir que os objetivos de segurança da informação definidos podem ser alcançados com base no risco.

**ML4**

- Os elementos de configuração são monitorizados quanto à sua coerência com as bases de referência ao longo do ciclo de vida de um produto ou aplicação a que aplica-se essa base de referência, incluindo processos como a gestão do código-fonte e o aprovisionamento de servidores.
- São definidos, medidos e comunicados os resultados dos indicadores de conformidade com as bases de referência.
- Os resultados da monitorização são comunicados regularmente à direção.

**ML5**

- As linhas de base de configuração são revistas e atualizadas com uma frequência definida pela organização para se manterem atualizadas e eficazes.
- O processo de gestão da configuração é avaliado e os resultados são utilizados para implementar melhorias.

# Engenharia e desenvolvimento seguros

As preocupações crescentes e os riscos empresariais associados ao software inseguro chamaram a atenção para a necessidade de integrar plenamente a segurança no ciclo de vida do desenvolvimento de sistemas, desde o início até à sua eliminação.

A experiência demonstrou que é difícil e dispendioso introduzir medidas de segurança corretamente e com êxito depois de um sistema ter sido desenvolvido, pelo que a segurança deve ser implementada na fase de conceção de todos os novos sistemas de informação e, sempre que possível, na modificação e funcionamento contínuo de todos os sistemas antigos.

## 1. Requisitos de segurança

A prática dos requisitos de segurança centra-se na especificação proativa do comportamento esperado do software no que respeita à segurança. Em conjunto com as atividades de análise ao nível do projeto, os requisitos de segurança são inicialmente recolhidos com base no objetivo empresarial de alto nível do software. À medida que uma organização avança, são utilizadas técnicas mais avançadas para descobrir novos requisitos de segurança que inicialmente poderiam não ser evidentes.

### ML1

- A segurança é considerada durante o processo de requisitos de software.

### ML2

- As leis e os regulamentos são avaliados quanto aos requisitos de segurança obrigatórios.
- As melhores práticas da indústria, que as equipas de projeto devem tratar como requisitos, são determinadas.
- Os requisitos de segurança são baseados em riscos conhecidos.
- Os requisitos de segurança são incluídos em requisitos empresariais mais globais que constituem o ponto de partida para o desenvolvimento (seguro).

### ML3

- Os requisitos de segurança não funcionais, incluindo as expectativas de segurança dos dados, a integridade das transações de controlo de acesso, a importância da função empresarial, a segregação de funções, tempo de atividade, etc., fazem parte do processo de requisitos de software.
- Os requisitos de segurança são, por defeito, integrados nos acordos com os fornecedores.
- As partes interessadas relevantes são identificadas e envolvidas na redação dos requisitos de segurança.

- Está a ser cumprido um processo documentado sobre a forma de desenvolver requisitos (de segurança).
- Os requisitos de segurança incluem critérios de aceitação, ou seja, as condições que têm de ser cumpridas para aceitar a aplicação do requisito.

**ML4**

- Os artefactos existentes (7) que indicam riscos específicos da organização ou do projeto são explicitamente revistos, a fim de compreender melhor o perfil de risco global do software.
- Os critérios de avaliação técnica são, por defeito, acrescentados aos contratos dos fornecedores relevantes.
- As verificações da conformidade dos requisitos de segurança são incorporadas nas auditorias de rotina do projeto.
- É documentada uma lista clara dos requisitos de segurança não cumpridos e um calendário estimado para a sua disponibilização em futuras versões.

**ML5**

- O carácter exaustivo e a maturidade dos requisitos de segurança são melhorados com base nos conhecimentos que a organização adquire com a gestão de incidentes, a gestão de projetos, a gestão de riscos, etc.

## 2. Conceção seguro

A prática de revisão da conceção centra-se na avaliação da conceção e da arquitetura do software para detetar problemas relacionados com a segurança. Tal permite que uma organização detete problemas numa fase precoce do desenvolvimento do software, evitando assim potenciais custos elevados de refabrico devido a preocupações de segurança.

**ML1**

- As considerações básicas de segurança são tidas em conta na conceção do software e/ou durante a arquitetura do sistema.
- No mínimo, são efetuadas revisões *ad hoc* da conceção do software e/ou da arquitetura do sistema para garantir mitigações de base para os riscos conhecidos.

**ML2**

- São criadas algumas conceções de software de alto nível baseadas em requisitos empresariais e nas melhores práticas da indústria.

- Estão a ser utilizados princípios de desenvolvimento e engenharia seguros, mas podem não estar em vigor normas e regras para toda a organização. A aplicação destes princípios baseia-se no nível de risco estimado associado aos dados a ser processados.
- São identificadas as bibliotecas e estruturas de software de terceiros mais utilizadas nos projetos de software da organização.
- Para cada projeto, é identificada a superfície de ataque do software.
- A validação é efetuada para verificar se todos os requisitos de segurança foram contemplados na conceção e na arquitetura.
- São considerados os seis principais mecanismos de segurança: autenticação, autorização, validação de entrada, codificação de saída, tratamento de erros e registo. Quando pertinente, são também considerados os mecanismos de criptografia e de gestão de sessões.
- Existe uma separação clara entre os diferentes ambientes de desenvolvimento.
- Os dados de produção que contenham informações pessoais identificáveis ou quaisquer outras informações sensíveis (8) não são utilizados para fins de ensaio, a menos que os dados sejam ofuscados, codificados ou protegidos de forma adequada contra o acesso indesejado e/ou não autorizado, o roubo ou qualquer outra divulgação ilegal de dados.

**ML3**

- Os princípios de desenvolvimento seguro são identificados, documentados e comunicados aos colaboradores relevantes.
- O processo de conceção do software é formalmente controlado e a utilização de componentes seguros é validada.
- Estão a ser utilizadas técnicas de engenharia segura que fornecem orientações sobre os mecanismos de autenticação dos utilizadores, o controlo seguro das sessões e a validação dos dados, a sanitização e a eliminação dos códigos de depuração.
- São aplicados procedimentos de desenvolvimento de aplicações que aplicam técnicas de engenharia segura.
- A segurança é tratada como parte integrante da conceção global do sistema;  tal inclui o estabelecimento de políticas de segurança, compreensão dos requisitos de segurança resultantes, participação na avaliação de produtos de segurança e na engenharia, conceção, implementação e eliminação do sistema.

- Quando o desenvolvimento é externalizado, a organização obteve garantias, através de contratos ou outros acordos vinculativos, de que a parte externa cumpre as suas regras de desenvolvimento seguro.
- Quando o desenvolvimento é externalizado, a organização obteve o direito contratual de auditar os processos e controlos de desenvolvimento.
- A organização garante que os programadores recebem formação adequada em matéria de conceção, desenvolvimento, controlo da configuração, integração e ensaio de software seguro antes de desenvolverem o sistema.
- Foi estabelecido um processo através do qual as partes interessadas do projeto podem solicitar uma revisão da conceção. Todos os revisores devem receber formação para efetuar as revisões de forma completa e consistente.
- As conceções de segurança utilizam uma abordagem em camadas para abordar ou proteger contra ameaças ou para reduzir a vulnerabilidade. Ao utilizar várias abordagens de proteção sobrepostas, a falha ou a evasão de qualquer abordagem de proteção individual não deixará o sistema desprotegido.
- A organização documentou os fluxos de processo para todas as fases do ciclo de vida de desenvolvimento de sistemas, desde a conceção até à desativação.

### ML4

- A organização mede a eficácia do processo de desenvolvimento em termos da sua capacidade de descobrir defeitos e do tempo necessário para reagir adequadamente a esses defeitos.
- São igualmente comunicados à direção outros parâmetros que medem a eficácia do processo, como o momento em que os defeitos são descobertos após a sua introdução, o número de defeitos descobertos e a gravidade desses.

### ML5

- Os princípios de desenvolvimento e engenharia seguros são regularmente revistos para garantir que contribuem efetivamente para o reforço das normas de segurança, para garantir que se mantêm atualizados em termos de combate a quaisquer novas ameaças potenciais e para garantir que continuam a ser aplicáveis aos avanços nas tecnologias e soluções que estão a ser aplicadas.
- O processo de revisão da conceção inclui uma vertente de melhoria baseada nos resultados dos ciclos de revisão do projeto e nas reações das partes interessadas.

## 3. Revisão do código (9) e testes de segurança

**ML1**

- As vulnerabilidades fundamentais a nível do código e outros riscos de segurança de elevada gravidade são, pelo menos, procurados de forma oportunista.
- No mínimo, são efetuados testes de segurança básicos antes da implementação do software.
- Uma análise externa da segurança ou testes de penetração (10) são efetuados, pelo menos, de forma fragmentada.

**ML2**

- É criada uma lista de controlo ligeira de revisão do código que contém requisitos de segurança funcionais e não funcionais.
- É realizada uma análise do código de alto risco.
- São realizados testes de segurança básicos, com base nos requisitos de implementação e de software, antes da implementação final do software (versão).
- Os testes de vulnerabilidade são realizados regularmente ou aquando realização de alterações importantes a um ou mais sistemas.
- Os resultados dos testes de vulnerabilidade são apresentados à gestão.

**ML3**

- É estabelecida uma base de segurança a nível do código, uma norma mínima para os resultados da revisão do código para todos os projetos de software.
- A revisão e a análise do código, incluindo a das bibliotecas de terceiros utilizadas, são mais precisas e eficientes através da automatização durante o desenvolvimento.
- A revisão do código consiste em revisões manuais e revisões através de ferramentas.
- Os resultados da revisão estão disponíveis no início da fase de desenvolvimento, permitindo que as equipas de desenvolvimento efetuem uma auto-verificação ao longo do processo antes do lançamento.
- As conclusões não abordadas da revisão do código que permanecem no lançamento são revistas e aceites pelas partes interessadas do projeto.
- Foi identificado um conjunto de casos de teste para verificar a funcionalidade correta do software. Por norma, estes casos de teste específicos da aplicação são derivados de preocupações de segurança em torno dos requisitos funcionais e da lógica empresarial do sistema, e também incluem testes genéricos para vulnerabilidades comuns com base na linguagem de implementação ou pilha de tecnologia.

- Os testes de segurança estão integrados no processo de desenvolvimento, o que significa que, para todos os projetos (relevantes) dentro da organização, os testes de segurança são executados por rotina e os resultados dos testes são revistos durante o desenvolvimento.
- São necessários testes de segurança específicos das aplicações para garantir a segurança de base antes da implementação.
- Os testes de penetração são realizados regularmente e os resultados são analisados, classificados por ordem de prioridade e são tomadas medidas de atenuação.
- Todas as aplicações são testadas periodicamente de acordo com um calendário estabelecido. Um aspeto importante dos testes periódicos é garantir que os problemas identificados num teste de vulnerabilidade ou de penetração são efetivamente corrigidos e não voltam a surgir na construção.

## ML4

- As revisões de código analisam e monitorizam a adesão às práticas internas de codificação. Os casos de teste candidatos são revistos quanto à sua aplicabilidade, eficácia e viabilidade pelos responsáveis pelo desenvolvimento, segurança e garantia de qualidade.
- Os objetivos relacionados com o número de defeitos de segurança identificados (e a sua gravidade) que entram em produção, a sua gravidade e o tempo necessário para os corrigir são definidos pela gestão, medidos e comunicados. Existe um controlo suficiente para comunicar os dados reais.
- A evolução das análises de segurança e dos resultados dos testes de penetração é monitorizada numa base contínua.
- É desenvolvida uma capacidade interna de testes de penetração na organização. Esta capacidade pode fazer parte da equipa de desenvolvimento, da equipa de testes, de um grupo de segurança ou de uma equipa especializada e formada noutra parte da organização.

## ML5

- A base de segurança a nível do código é melhorada através da adição de critérios adicionais baseados nas melhores práticas de codificação, avisos, conhecimentos adquiridos no próprio processo de revisão do código, etc.
- A base de referência dos testes de segurança é melhorada através da seleção de questões de segurança adicionais e da inclusão de uma variedade de casos de teste correspondentes.
- Os resultados dos testes de penetração são utilizados para manter a base de segurança atualizada e eficaz.

# Operações seguras

Operações seguras é a prática em que existem controlos de segurança operacionais, procedimentos e instruções de trabalho para garantir a CIA da infraestrutura TIC. Exemplos de controlos de operações seguras são: procedimentos documentados, controlos físicos (instalações) como energia, alojamento seguro, manutenção, cablagem, controlos de conteúdo como anti-malware, firewall, segurança de correio, VPN para trabalho remoto, manuseamento de equipamento fora das instalações, gestão de chaves de encriptação, controlos de dispositivos móveis.

Alguns controlos de operações seguras (ou seja, cópia de segurança) estão incorporados noutros (sub)domínios do presente modelo.

## 1. Operações seguras gerais

**ML1**

- As operações seguras dos sistemas e processos TIC são, pelo menos, parcialmente realizadas.
- Pelo menos alguns colaboradores e/ou equipas implementaram procedimentos e controlos como mensagens seguras, VPN e software anti-malware.
- As medidas de melhoria da segurança são aplicadas, na pior das hipóteses, numa base *ad hoc* ou na sequência de incidentes de segurança.

**ML2**

- A gestão apoia operações seguras com financiamento adequado e incentiva os colaboradores a desempenharem tarefas de operações seguras.
- Os colaboradores são incentivados a documentar os seus procedimentos operacionais.
- São aplicadas medidas de segurança física para o equipamento TIC.
- O pessoal técnico utiliza os guias de instalação e manutenção publicados.

**ML3**

- Os procedimentos e controlos de operações seguras estão documentados e implementados em todas as fases do ciclo de vida de um bem de informação.
- Os colaboradores sabem onde encontrar os procedimentos relevantes e atuam de acordo com esses procedimentos.
- Os colaboradores recebem formação para trabalharem de acordo com esses procedimentos e para aplicarem os controlos.

- São definidas e aplicadas bases de controlo para as infraestruturas TIC.
- O pessoal técnico garante que os controlos de segurança do host e da rede necessários estão a funcionar e monitoriza proativamente o software, incluindo as entradas de aplicações (11).
- Tanto os dados em repouso como os dados em trânsito estão devidamente protegidos com base no seu perfil de risco. Não são utilizados protocolos não encriptados para trocar (interna e externamente) informações pessoais identificáveis ou outras informações sensíveis.
- A organização implementou todas as medidas técnicas identificadas e avaliadas como necessárias para reduzir os riscos relacionados com os sistemas de informação para um nível aceitável. Estas medidas técnicas incluem, pelo menos: bloqueio de acesso/privilégio mínimo (13), registo de eventos centralizado (14), reforço da infraestrutura (15), restrições a nível do sistema operativo (16), segurança da rede (encriptação, firewall, gestão de portas), restrições de acesso físico, automação da configuração e da implementação e controlo das versões alteradas (17).

**ML4**

- São definidas métricas para medir se os procedimentos e controlos operacionais seguros atingem a eficácia esperada.
- A gestão recebe relatórios sobre as operações seguras.
- Os riscos relacionados com a segurança das operações são identificados e revistos periodicamente.
- A eficácia da base de segurança técnica dos sistemas de informação é monitorizada e revista através de testes de segurança e da comunicação de incidentes.

**ML5**

- A prática de operações seguras é revista/avaliada periodicamente.
- As melhorias resultantes dessas revisões são implementadas.
- O planeamento de operações seguras é incorporado no planeamento estratégico anual da segurança.
- A base de segurança técnica é regularmente adaptada para garantir que se mantém atualizada em termos de combate a quaisquer novas potenciais ameaças e para garantir que continua a ser aplicável aos avanços nas tecnologias e soluções que estão a ser aplicadas.

## 2. Manutenção segura

### ML1

- A instalação de patches e outras tarefas de manutenção são realizadas quando ocorrem problemas técnicos. A manutenção é realizada, no mínimo, de forma reativa.

### ML2

- Se o fornecedor disponibilizar correções de software, são avaliados os riscos associados à instalação e à não instalação da correção e são tomadas as medidas adequadas decorrentes dessa avaliação.
- Na maior parte das vezes, as correções são testadas antes de serem instaladas para garantir que são eficazes e não provocam efeitos secundários.
- A manutenção é feita tanto de forma proativa como reativa, com base na estimativa dos riscos.

### ML3

- A manutenção dos equipamentos é efetuada de acordo com os intervalos de manutenção e as especificações recomendadas pelo fornecedor, para garantir à sua disponibilidade e integridade permanentes.
- É adotada uma estratégia de recurso (18) antes da aplicação de alterações.
- É definido um calendário para reagir a notificações de vulnerabilidades de software potencialmente relevantes.
- Existe um processo (semi)automatizado de gestão cíclica de correções.
- À exceção das alterações de emergência, as restantes tarefas de manutenção são geridas pelo processo de gestão de alterações da organização.
- Quando a manutenção é subcontratada, existem acordos contratuais suficientes que abrangem as responsabilidades em matéria de segurança da informação e os riscos avaliados.
- Existe um processo para detetar e identificar as atualizações e correções (de segurança) necessárias.

### ML4

- Existe um processo para gerir as tarefas de manutenção recorrentes a serem executadas.

### ML5

- O processo cíclico de gestão de correções é periodicamente revisto e melhorado com base nos requisitos da empresa, no prazo de entrega das correções, nas alterações do panorama da segurança da informação, etc.

## 3. Eliminação/remoção segura

### ML1

- Os suportes de dados são, por vezes, apagados ou destruídos no final do seu ciclo de vida.

### ML2

- Os suportes de dados são apagados, encriptados ou destruídos no final do seu ciclo de vida ou quando o sistema de informação em que foram utilizados é eliminado.
- Quando já não são necessários para fins empresariais, legais ou outros válidos, os dados são apagados de forma segura, adequada e suficiente para o nível de sensibilidade dos mesmos.
- As etiquetas e marcas de identificação da organização ou dos seus colaboradores são removidas antes da eliminação, revenda ou doação.

### ML3

- São desenvolvidos procedimentos para eliminar os ativos de um sistema de informação de forma adequada e segura no final do ciclo de vida de um sistema. São implementados procedimentos para garantir que os discos rígidos, as memórias voláteis e outros suportes do sistema são eliminados a um nível aceitável e não retêm informações residuais.
- A eliminação de itens sensíveis é registada de forma a manter um registo de auditoria.
- Existe um inventário de retenção de dados (para registos, material PKI, etc.) que especifica o método de eliminação após o termo do período de retenção.

### ML4

- Realiza-se uma validação (19) para verificar se os dados e suportes de dados são efetivamente removidos e/ou destruídos em conformidade com os requisitos empresariais ou de conformidade documentados.

### ML5

- O processo de eliminação segura é revisto periodicamente e, quando necessário, atualizado com base em alterações nos requisitos empresariais ou de conformidade, alterações no panorama da segurança da informação, etc.

# Gestão da identidade e acesso

O objetivo da gestão da identidade e do acesso (IAM) é criar e gerir identidades às quais pode ser concedido acesso aos ativos da organização. Através da aplicação de mecanismos de controlo eficazes, o acesso aos bens da organização pode basear-se no risco potencial para as infraestruturas críticas e os objetivos organizacionais.

Um IAM eficaz deve analisar, documentar e gerir as identidades dos utilizadores e respetivas permissões.

Uma identidade é um carácter único e distintivo e/ou uma propriedade de pessoas/máquinas/ativos.

As identidades podem ter acesso aos ativos da organização através de credenciais únicas. Todas as credenciais têm privilégios associados.

Os privilégios determinam o que as identidades estão autorizadas a fazer com os ativos.

**ML1**

- A organização utiliza as identidades para obter acesso aos ativos, sempre que possível.
- A organização documenta as identidades que requerem acesso aos ativos quando tal é considerado relevante.

**ML2**

- O acesso concedido aos ativos é sempre gerido e controlado. As identidades são fornecidas para o pessoal e outras entidades (p. ex., serviços, dispositivos) que requerem acesso aos ativos.
- Os níveis de acesso são classificados em diferentes níveis de confiança. Os privilégios de raiz, o acesso administrativo, o acesso de emergência e as contas partilhadas recebem atenção adicional e são tratados com cautela.
- São emitidas credenciais adequadas (p. ex., identificação de utilizador/palavras-passe, cartões inteligentes, certificados, chaves) a todas as identidades que necessitam de acesso.
- É criado e está operacional um repositório central que facilita a gestão do acesso a alguns ativos.
- As identidades são revistas numa base *ad hoc*, para garantir que refletem o ambiente atual das pessoas, objetos e entidades associadas.
- As identidades são revogadas quando deixam de ser necessárias.
- O conceito de "privilégio mínimo", que não fornece mais autorizações do que as necessárias para executar as funções requeridas, é implementado, no mínimo, em sistemas de informação críticos para a atividade.

## ML3

- É criado e está operacional um repositório central de identidades que apresenta uma visão geral das identidades de todos os ativos que têm a capacidade de se interligar com este repositório central.
- Os repositórios de identidades são periodicamente revistos, atualizados e corrigidos para minimizar as incoerências.
- É utilizado um processo de aprovação formal para apoiar o fornecimento de acesso (pedido, alteração e eliminação).
- A utilização de contas/identidades partilhadas é reduzida ao mínimo absolutamente necessário. Quando são utilizadas contas/identidades partilhadas, foram implementadas medidas adicionais para poder registar, monitorizar e auditar a utilização dessas credenciais partilhadas.
- Os requisitos para as credenciais baseiam-se nos critérios de risco da organização (p. ex., credenciais multifator para acesso de alto risco).
- Os privilégios (e restrições) de acesso são definidos e descrevem o nível e a extensão do acesso.
- Os privilégios de acesso são concedidos pelo proprietário do ativo, com base nos requisitos da função/cargo e no risco.
- As alterações nos sistemas e dispositivos de controlo de processos são identificadas e monitorizadas para garantir a conformidade da identidade.
- A organização determinou o prazo desejado para revogar as identidades que já não são necessárias e monitoriza o cumprimento desses prazos. O acesso à informação definido (p. ex., autorizações, segregação de funções) é assegurado ao longo de todo o fluxo de informação e para além dos limites da rede.
- O processo de gestão do acesso utilizado para apoiar o processo de pedido e aprovação de acesso deve basear-se em várias fases, sempre que possível, de acordo com a dimensão da organização.

## ML4

- As tentativas de acesso, o comportamento e as anomalias dos utilizadores são registados, monitorizados e auditados a fim de minimizar o risco de abuso. As identidades com um elevado nível de confiança (p. ex., privilégios de raiz, acesso administrativo, acesso de emergência, e contas partilhadas) são sujeitas a um controlo e monitorização adicionais.
- O conceito de "privilégio mínimo", que consiste em não fornecer mais autorizações para além das necessárias para desempenhar as funções requeridas, é implementado a nível empresarial e é objeto de auditorias regulares.
- São definidas, implementadas e comunicadas métricas para a gestão da identidade e do acesso.
- São efetuadas avaliações regulares para medir e avaliar a eficácia do(s) processo(s) de gestão da identidade e do acesso.

## ML5

- O próprio processo de gestão da identidade e do acesso e as ferramentas de apoio são periodicamente revistos e adaptados quando necessário.

# Sensibilização e formação

## ML1

- Existe alguma forma de formação e sensibilização em matéria de segurança da informação.
- O pessoal TIC com formação é designado para apoiar as questões de segurança da informação à medida que estas ocorrem.
- No mínimo, a gestão tem alguma consciência da segurança da informação e das ameaças associadas.

## ML2

- Existe um plano de sensibilização e formação em matéria de segurança da informação.
- Existe uma pessoa interna responsável pela sensibilização e formação em matéria de segurança da informação.
- A gestão investe em formação sobre segurança da informação para os colaboradores, quando necessário.
- Existe um número limitado de pessoal com formação para tratar de potenciais problemas de segurança.
- A gestão tem um conhecimento básico da segurança da informação e das principais ameaças.
- Os colaboradores têm uma consciência básica de um bom comportamento em matéria de segurança, que consiste, por exemplo, em utilizar palavras-passe, bloquear ecrãs, guardar os procedimentos de trabalho à distância, enviar correio eletrónico seguro e utilizar dispositivos móveis.

## ML3

- Existe um programa organizacional de sensibilização e formação em matéria de segurança da informação. O programa é coordenado, documentado, ligado à estratégia da empresa e ao planeamento anual e adaptado às necessidades e objetivos da organização.
- Uma pessoa interna foi designada formalmente como responsável pela sensibilização e formação em matéria de segurança da informação.
- A gestão investe estruturalmente na formação em segurança da informação para todos os colaboradores.
- Existe pessoal suficiente e com formação adequada para resolver potenciais problemas de segurança.
- A gestão tem uma boa e desenvolvida compreensão da segurança da informação e encoraja o desenvolvimento de uma consciência de segurança;  dá o exemplo.

- Os colaboradores têm uma boa consciência do comportamento responsável em matéria de segurança (p. ex., em relação a palavras-passe, ecrãs de bloqueio, procedimentos seguros de teletrabalho, correio eletrónico seguro e manuseamento de dispositivos móveis), em conformidade com as políticas, procedimentos e instruções de trabalho empresariais.
- Os colaboradores estão conscientes dos riscos de um comportamento de segurança insuficiente.

## ML4

- Está disponível um catálogo com cursos de formação internos e externos de elevada qualidade no domínio da segurança da informação.
- As competências de segurança em falta são identificadas e os cursos de formação obrigatórios devem ser seguidos.
- A eficácia da formação é monitorizada e os planos e cursos de formação são adaptados em conformidade.
- São estabelecidas métricas para monitorizar a eficácia de campanhas de sensibilização e formação selecionadas.
- A disponibilidade e a utilização eficiente do pessoal com formação em segurança são monitorizadas. Por exemplo, através de análises de causas profundas ou como parte da gestão global de incidentes.

## ML5

- O programa de formação em segurança da informação é adaptado anualmente e otimizado de acordo com as necessidades organizacionais.
- A coordenação da sensibilização para a segurança da informação é continuamente adaptada e melhorada para responder às necessidades da organização.
- Os investimentos na sensibilização para a segurança são redirecionados de acordo com os resultados da monitorização da eficácia.
- O conhecimento sobre segurança da informação é trocado entre os colaboradores para promover o desenvolvimento contínuo da sensibilização para a segurança.
- A gestão revê periodicamente a estratégia de formação e de sensibilização em matéria de segurança e adapta-a às necessidades da empresa e às que resultam das avaliações de risco.
- A gestão integrou a segurança da informação na sua missão e estratégia empresariais globais.

# Proteção da informação

Um ativo de informação é um elemento de informação, como um registo de colaborador, uma lista de clientes ou um relatório financeiro, que é valioso para a organização.

A informação pode assumir muitas formas, incluindo, mas não se limitando a, dados em papel, dados armazenados eletronicamente em sistemas informáticos, comunicações enviadas por correio físico ou por correio eletrónico, dados armazenados em suportes eletrónicos como unidades USB, discos e fitas, e texto e desenhos em quadros brancos e flip charts.

## ML1

- Existe uma compreensão informal do valor da informação.
- Existe um mínimo de regras informais que especificam como tratar a informação da empresa.
- Pelos menos alguns controlos para a proteção da informação estão implementados.

## ML2

- A informação é classificada e categorizada relativamente à sua importância no apoio à prestação de serviços.
- São identificados os riscos críticos para a empresa relacionados com os ativos de informação ou com o tratamento da informação.
- No mínimo, existe um ciclo de vida da informação informal.
- A gestão apoia iniciativas para proteger a informação com recursos suficientes.
- Existem controlos administrativos, técnicos e físicos para a proteção da informação.
- Tanto os dados em repouso como os dados em trânsito são considerados na proteção da informação.

## ML3

- Existe um processo documentado e implementado para a gestão da informação que contém a classificação e categorização da informação e dos ativos de informação, relativamente à sua importância no apoio à prestação de serviços.
- Os riscos relacionados com a perda de confidencialidade, integridade e/ou disponibilidade da informação ou dos ativos de informação, ou dos processos a que pertencem, são identificados e geridos.
- Existe um ciclo de vida da informação formal (26), sustentado por procedimentos documentados que são comunicados a todos os colaboradores relevantes.
- A gestão da identidade e do acesso é controlada através de um processo formal a nível da empresa.

- A gestão apoia a proteção da informação com recursos e investimentos para cumprir os objetivos de segurança da organização.
- São identificados, implementados e geridos controlos administrativos, técnicos e físicos para proteger a informação.
- As considerações de confidencialidade e privacidade das informações são geridas.
- Os controlos atenuantes, baseados nos resultados do processo de gestão de riscos, são sempre tidos em conta na proteção da informação. Os controlos possíveis são (lista não exaustiva): controlos criptográficos, procedimentos de cópia de segurança e de restauro, proteção da rede, destruição de dados, proteção contra fugas de dados, etc.
- Existem políticas e linhas de base da empresa que especificam os controlos criptográficos permitidos e mínimos exigidos (20) para todos os dados em repouso e em trânsito considerados confidenciais ou sensíveis.
- A confidencialidade, disponibilidade, integridade e fiabilidade dos ativos de informação são geridas de acordo com a análise de risco.

**ML4**

- O desempenho da proteção da informação é monitorizado e controlado de acordo com as conclusões da gestão de incidentes, da gestão de riscos e das auditorias de segurança, entre outros.
- A utilização da criptografia e das chaves criptográficas é acompanhada e controlada. Os controlos para a proteção da informação são periodicamente monitorizados quanto à sua adequação (incluindo a sua eficácia).

**ML5**

- Os desvios das linhas de base e das políticas criptográficas são comunicados e ajustados quando necessário.
- A proteção da informação através de controlos é continuamente monitorizada e os controlos são continuamente melhorados com base em conclusões de gestão de incidentes, gestão de riscos e auditorias de segurança, entre outros.

# 3 Detetar

## Registo e Monitorização

### ML1

- Existe alguma forma de recolha de registos.
- Os registos são recolhidos intencionalmente.
- Os registos recolhidos são armazenados num formato estruturado.
- No mínimo, é efetuado um nível básico de monitorização da segurança da informação.

### ML2

- São definidos requisitos de monitorização e análise para os ativos mais importantes da organização.
- Os registos são recolhidos e armazenados centralmente para os ativos mais importantes da organização, sempre que possível.
- Os registos são sincronizados no tempo.
- Os registos são analisados na eventualidade de um evento de segurança.
- São realizadas atividades de monitorização da segurança da informação (p. ex., análises periódicas dos dados de registo).
- Os ambientes operacionais são monitorizados para detetar comportamentos anómalos que possam indicar um evento de segurança da informação.
- Existe algum tipo de ferramenta disponível para a monitorização da segurança e dos eventos.

### ML3

- Os requisitos de registo e monitorização foram definidos para todos os ativos (p. ex., âmbito da atividade e cobertura dos ativos, requisitos de segurança da informação).
- Os dados de registo são agregados numa plataforma central inviolável.
- Os registos são analisados de forma regular e exaustiva para detetar anomalias.
- O princípio da necessidade de saber é aplicado ao registo. O próprio acesso aos dados de registo é registado.
- Os dados de registo e os resultados da monitorização são apresentados através de painéis de controlo para um apoio visual rápido.
- Os alertas e alarmes são configurados para ajudar a identificar os eventos de segurança da informação.

- Os indicadores de atividade anómala (casos de uso ou de abuso) foram definidos e são monitorizados em todo o ambiente operacional.
- A monitorização é efetuada tanto em banda (21) e fora de banda (22) para obter a cobertura mais completa.

## ML4

- Existe uma ferramenta de monitorização de segurança e de eventos disponível para apoiar as operações de segurança.
- Os dados de registo agregados são enriquecidos com informações adicionais, a fim de compreender as ações realizadas.
- Os relatórios são elaborados para mostrar a conformidade da segurança com as linhas de base da segurança, por exemplo.
- Os dados de registo apoiam outros processos empresariais e de segurança (p. ex., resposta a incidentes, gestão de ativos).
- A monitorização é integrada com outros processos empresariais e de segurança (p. ex., gestão de informações e eventos de segurança, gestão de incidentes, gestão de ativos, etc.).
- A monitorização ponta-a-ponta (23) é efetuada para funções empresariais importantes.

## ML5

- Os dados de registo são regularmente revistos para avaliar a sua relevância, utilidade e conformidade legal.
- Os dados recolhidos através da gestão de incidentes, da capacidade e da disponibilidade são utilizados para melhorar os processos de registo e de monitorização.
- Os processos de registo e monitorização são revistos periodicamente e, sempre que possível, melhorados. Exemplos de tópicos para melhoria são: adicionar ou eliminar determinados dados de registo, discutir e implementar casos de utilização, conceção de novos painéis de controlo.

# Gestão de ameaças e vulnerabilidades

## ML1

- A organização está, até certo ponto, sensibilizada para as ameaças e/ou vulnerabilidades e sua respetiva identificação.
- Um mínimo de informações sobre ameaças e vulnerabilidades é partilhado entre as partes interessadas internas e, se necessário, externas.

## ML2

- São identificadas fontes de informação para apoiar as atividades de gestão das ameaças e vulnerabilidades (NVD, CVE, etc.).
- As informações sobre ameaças e vulnerabilidades à segurança da informação são recolhidas e interpretadas em função dos riscos que comportam.
- As ameaças e vulnerabilidades consideradas importantes são tratadas (p. ex., aplicação de controlos atenuantes, monitorização do estado das ameaças, aplicação de correções de segurança).
- As partes interessadas nas atividades de partilha de informações sobre ameaças e vulnerabilidades, internas e externas, são identificadas e envolvidas.

## ML3

- A organização definiu o seu perfil de ameaça. As fontes de informação sobre ameaças e vulnerabilidades que abordam os componentes do perfil de ameaça (24) são monitorizadas.
- As ameaças e vulnerabilidades identificadas são analisadas, classificadas por ordem de prioridade e tratadas de acordo com a prioridade atribuída e os tempos de reação definidos (com base na gravidade).
- São realizadas avaliações das vulnerabilidades da segurança da informação (p. ex., revisões à arquitetura, testes de penetração, exercícios de cibersegurança, ferramentas de identificação de vulnerabilidades).
- A gestão das vulnerabilidades inclui uma combinação de testes manuais e automatizados (p. ex., scanners de vulnerabilidades).
- Foram desenvolvidas políticas, normas e/ou orientações para partilhar informações sobre ameaças e vulnerabilidades com as partes interessadas adequadas de forma segura.
- São identificadas as fontes técnicas que podem ser consultadas sobre questões de segurança da informação.
- A Gestão das Vulnerabilidades está integrada na Gestão das Correções.
- São estabelecidas metas e objetivos que descrevem os resultados desejados da partilha de informações sobre ameaças. Estas metas e objetivos ajudam a organização a medir a eficácia das suas atividades de partilha de informações.

**ML4**

- Os processos de gestão de ameaças e vulnerabilidades medem à sua própria eficácia e a da gestão de patches, comparando o nível de risco antes e depois da correção.

**ML5**

- Os próprios processos de gestão das ameaças e das vulnerabilidades são objeto de avaliação e melhoria periódicas.
- As políticas de partilha de informações são revistas regularmente para verificar a sua conformidade com as normas especificadas, as políticas empresariais e os requisitos legais e contratuais, e ajustadas ou melhoradas, se necessário ou desejado.

## Auditoria

A realização de auditorias internas e/ou externas a intervalos planeados ajuda as organizações a validar que os seus esforços de segurança da informação estão em conformidade com as normas da indústria e com a sua própria política de segurança e bases técnicas de segurança. Estas auditorias, tanto técnicas como não técnicas, devem ser utilizadas para verificar se as medidas de segurança da informação são efetivamente implementadas e mantidas.

**ML1**

- A auditoria dos controlos de segurança da informação é realizada, pelo menos, numa base *ad hoc*.

**ML2**

- As auditorias são realizadas para as atividades críticas da empresa.
- São efetuadas auditorias aos sistemas de informação objeto de incidentes.
- É mantido um registo de auditoria para as etapas realizadas durante a auditoria. Os resultados das auditorias são comunicados às entidades auditadas.
- Os resultados das auditorias são protegidos contra a utilização abusiva e o acesso não autorizado.

**ML3**

- É criado e formalmente aprovado pela gestão um plano de auditoria anual com um âmbito acordado.
- São realizadas auditorias regulares a atividades empresariais importantes.
- Existe um procedimento de auditoria aprovado pela gestão que garante a repetibilidade dos testes.
- Os auditores têm formação adequada para o desempenho da tarefa.
- Os resultados das auditorias são comunicados à gestão através de um canal de comunicação formal.

**ML4**

- A eficácia do programa de auditoria é medida através de alterações (p. ex., aumento ou diminuição) do número e da gravidade das constatações.
- Um universo de auditoria (27) descreve o âmbito da auditoria e o calendário (planeamento) em que é realizada uma auditoria completa e baseada no risco.

**ML5**

- O próprio processo de auditoria é regularmente revisto e melhorado com base nas reações do auditor, das entidades auditadas, da gestão e nos resultados dos relatórios de auditoria.

## Detetar eventos de segurança da informação

**ML1**

- A organização instalou capacidades básicas para detetar eventos de segurança.
- Os eventos de segurança da informação detetados são registados.

**ML2**

- No mínimo, a deteção automatizada de eventos está ativada em todos os sistemas críticos para a atividade.
- Os registos são revistos periodicamente para verificar se existem eventos de segurança da informação.
- A direção está consciente de que os eventos de segurança da informação podem perturbar os serviços, o planeamento e as atividades diárias da organização. Por conseguinte, apoiam a deteção precoce destes eventos.

**ML3**

- São estabelecidos critérios para a deteção de eventos de segurança da informação (p. ex., o que constitui um evento, onde procurar eventos).
- No mínimo, a deteção automatizada de eventos é ativada em todos os sistemas de segurança, sistemas críticos para a atividade e sistemas de infraestruturas críticas.
- Todos os colaboradores, tanto técnicos como não técnicos, são sensibilizados para a sua responsabilidade no que diz respeito à deteção de anomalias durante as suas atividades profissionais diárias. Estes recebem formação adequada para corresponder a esta expectativa.
- As provas relativas a eventos de segurança são recolhidas de forma consistente e adequadamente protegidas.

**ML4**

- As informações sobre os eventos são continuamente correlacionadas para apoiar a deteção de incidentes através da identificação de padrões, tendências e outras caraterísticas comuns.
- Os resultados gerados pelos algoritmos de deteção de eventos de segurança da informação são medidos e avaliados para melhorar os resultados.

**ML5**

- As atividades de deteção de eventos de segurança da informação são periodicamente revistas e ajustadas para ajudar a detetar ameaças conhecidas e monitorizar os riscos identificados, com base nos conhecimentos adquiridos em incidentes anteriores e nas informações do registo de riscos e do perfil de ameaças da organização.

# 4 Responder

Após a organização validar que está perante um incidente de segurança da informação, é fundamental que existam processos internos que permitam uma reação rápida e estabeleçam uma equipa multifuncional que supervisione todos os aspetos da resposta ao incidente.

Uma comunicação eficaz é igualmente essencial. Uma vez identificada a natureza, a extensão e a gravidade do incidente de segurança da informação, a organização tem de tomar decisões informadas o mais rapidamente possível.

## Escalar eventos de segurança da informação e declarar incidentes

**ML1**

- Os eventos de segurança da informação detetados são registados e analisados.
- Os critérios de escalonamento de eventos de segurança da informação e de declaração de incidentes de segurança da informação estão, pelo menos parcialmente, definidos.
- O registo dos incidentes de segurança é, no mínimo, parcialmente efetuado.

**ML2**

- Os critérios de escalonamento de eventos de segurança da informação e de declaração de incidentes são definidos e comunicados (ou seja, quando é que um evento de segurança da informação se torna um incidente de segurança).
- Os eventos de segurança da informação são analisados para garantir uma resposta adequada e para apoiar as atividades de recuperação. Se necessário, os fornecedores ou outras partes interessadas na segurança da informação (ou seja, CERT,...) são envolvidos nesta prática.

- Determinados eventos de informação foram classificados, registados como incidentes e, quando necessário, encaminhados para a direção.

## ML3

- Todos os eventos de segurança da informação são analisados e avaliados por colaboradores designados com base no perfil de risco do sistema TIC ou da função empresarial a que se referem.
- Os critérios de escalonamento de eventos de segurança da informação, incluindo os critérios de declaração de incidentes de segurança da informação, são estabelecidos com base no potencial impacto empresariais que pode ser causado pelo incidente de segurança da informação.
- Estão disponíveis políticas, procedimentos e diretrizes que apoiam a classificação e a atribuição de prioridades aos incidentes e o seu conteúdo é comunicado a todas as partes interessadas relevantes.

## ML4

- A eficácia do escalonamento de eventos de segurança da informação e da declaração de incidentes de segurança da informação é medida com base no tempo (médio) entre a descoberta do evento e o registo do incidente.
- A organização mede o número de incidentes de segurança da informação declarados que deveriam ter sido identificados em resultado de um alarme ou evento de segurança, mas para os quais o escalonamento não ocorreu nessa altura.

## ML5

- Os eventos de segurança da informação escalados e os incidentes declarados são correlacionados para melhorar a eficácia da análise e para apoiar a descoberta de padrões, tendências e outras caraterísticas comuns.
- Os critérios de escalonamento de eventos de segurança da informação, incluindo os critérios de declaração de incidentes de segurança da informação, são ajustados de acordo com as informações do registo de riscos e do perfil de ameaças da organização.

# Planeamento da resposta

**ML1**

- A responsabilidade pelo tratamento de incidentes foi alocada, no mínimo informalmente, a um colaborador (ou unidade) reconhecido.
- Foram criados procedimentos de resposta a incidentes ou documentação de apoio para, pelo menos, um número muito limitado de tipos de incidentes.

**ML2**

- O pessoal responsável pela resposta a incidentes de segurança da informação está identificado e as suas funções estão atribuídas.
- Em algumas áreas organizacionais, foi nomeada e designada uma função responsável para recolher, detetar e responder a incidentes de segurança.
- As partes interessadas internas e externas têm a possibilidade de comunicar eventos de segurança relacionados com os sistemas de tratamento da informação da organização.
- São criados e disponibilizados aos colaboradores competente procedimentos de resposta a incidentes ou documentação técnica para tratar e resolver os principais tipos de incidentes.

**ML3**

- Está implementado e operacional um registry central para gerir os incidentes. No mínimo, são registados o nível de gravidade, o impacto e a prioridade.
- Foi nomeada e designada uma função central responsável pela recolha, deteção e resposta a informações sobre incidentes de segurança.
- É estabelecido e publicado um processo coordenado de resposta a incidentes, com funções e responsabilidades claras definidas e linhas de comunicação preparadas para períodos de interrupções/incidentes.
- É ministrada formação aos colaboradores com funções de resposta a incidentes de segurança da informação.
- Os planos e procedimentos de gestão de incidentes de segurança da informação envolvem a colaboração com partes interessadas internas e externas, incluindo autoridades, CERT e ISAC, grupos de interesses especiais, fornecedores e clientes, para melhorar a eficácia da resposta e ajudar a minimizar as consequências para outras organizações.
- A política e os procedimentos de comunicação de informações sobre incidentes de segurança da informação às autoridades designadas estão em conformidade com as leis, regulamentos e acordos contratuais aplicáveis.

**ML4**

- No mínimo, o número, o nível de gravidade, o tempo de resposta e o impacto dos incidentes comunicados são medidos e um relatório de alto nível com as conclusões é apresentado à direção e/ou ao conselho de administração.
- A organização mede qualitativamente a disponibilidade de recursos adequados para a resposta a incidentes, de modo a cumprir os requisitos da atividade. Estes requisitos são determinados, pelo menos, com base nos resultados da análise de risco, da análise do impacto na privacidade, da análise do impacto na atividade, dos objetivos de tempo de recuperação e dos objetivos de ponto de recuperação.
- A organização mede a alocação adequada e a disponibilidade de recursos para a resposta a incidentes com base na contenção e no tempo de resposta. Por norma, para este efeito, utilizam-se avaliações de incidentes com base na causa raiz e reuniões de análise da gestão de incidentes.

**ML5**

- Os procedimentos de resposta a incidentes de segurança da informação e as instruções de resposta a incidentes técnicos são revistos regularmente para validar à sua atualidade e eficácia.
- As estatísticas dos incidentes de segurança da informação são comunicadas à direção e ao conselho de administração para que possam ser utilizadas como base para o planeamento e para as decisões relativas às medidas de segurança.

## Responder a incidentes de segurança da informação

**ML1**

- A resposta a incidentes de segurança da informação é, no mínimo, reativa e *ad hoc*.
- A comunicação de incidentes de segurança é efetuada, pelo menos parcialmente.

**ML2**

- As respostas a incidentes de segurança da informação são implementadas para limitar o impacto na atividade e restabelecer as operações normais.
- As atividades de resposta são registadas para análise posterior.
- As provas dos incidentes de segurança são recolhidas e armazenadas em segurança o mais rapidamente possível após a ocorrência.
- É efetuada uma comunicação interna dos incidentes de segurança da informação à direção e/ou ao conselho de administração.

## ML3

- A resposta a incidentes de segurança da informação é efetuada de acordo com procedimentos definidos que abordam todas as fases do ciclo de vida do incidente (p. ex., triagem, tratamento, comunicação, coordenação e encerramento).
- Durante a resposta ao incidente, os ativos envolvidos (restaurados) são (re)configurados de forma a mitigar o(s) risco(s) associado(s) ao incidente de segurança. A informação do inventário é atualizada após a execução dos procedimentos de resposta.
- As atividades de resposta a incidentes de segurança da informação são coordenadas com as partes interessadas externas relevantes em matéria de segurança da informação, sempre que necessário (ou seja, fornecedores, ISAC setorial, CERT, etc.).

## ML4

- Reuniões sobre as lições aprendidas são realizadas para medir a eficácia dos procedimentos de resposta a incidentes.
- As informações sobre os tempos de resposta a incidentes e a qualidade da contenção de incidentes são recolhidas e avaliadas, para melhorar a eficácia da resposta a incidentes.

## ML5

- São realizadas atividades de análise das causas profundas dos incidentes de segurança da informação e das lições aprendidas, e são tomadas medidas corretivas para melhorar o próprio processo de gestão de incidentes.
- Os planos e procedimentos de resposta a incidentes de segurança da informação são revistos e atualizados com uma frequência definida pela organização, a fim de os manter alinhados com os critérios de risco e o perfil de ameaça da organização e de os manter eficazes com base nos resultados das reuniões sobre as lições aprendidas.

# 5 Recuperar

O objetivo do Planeamento da Continuidade das Atividades (BCP) e da Recuperação de Desastres (DR) é assegurar a continuidade das operações essenciais dos serviços e/ou a recuperação de serviços falhados quando ocorre uma perturbação em resultado de um incidente grave de segurança da informação, de uma crise ou de um desastre.

Por conseguinte, as organizações terão de ter processos e planos de contingência implementados que lhes permitam responder às consequências de um incidente, crise ou catástrofe deste tipo.

## Gestão da Continuidade

### ML1

- Existe pelo menos um estado mínimo de preparação para eventos disruptivos em toda a organização, embora o sucesso e a eficácia da continuidade e da recuperação se baseiem em iniciativas individuais ou de equipa.
- Pelo menos um departamento ou unidade de negócio iniciou esforços para implementar à sua própria continuidade de negócios ou esforços de recuperação de desastres.

### ML2

- Pelo menos um departamento ou unidade de negócio iniciou esforços para sensibilizar a gestão para a importância da continuidade de negócios.
- Foram desenvolvidos e são mantidos planos de continuidade de negócios no âmbito de uma ou mais disciplinas de continuidade de negócios (gestão de incidentes, recuperação tecnológica, gestão da segurança, recuperação da atividade) para funções ou serviços importantes da atividade.
- A direção e os membros do conselho de administração estão sensibilizados para possíveis cenários de catástrofe e medidas de apoio.
- São definidas equipas informais para lidar com a continuidade e a recuperação em partes da organização (possivelmente motivadas por acontecimentos reais).
- São identificadas as atividades necessárias para manter as operações mínimas da organização.
- A sequência de atividades necessárias para regressar às operações normais é identificada em partes da organização.
- São disponibilizados planos de continuidade pró-ativos (25).
- A organização dispõe de, pelo menos, um recurso interno ou externo designado para apoiar os esforços de continuidade de negócios das unidades de negócio e/ou departamentos participantes.

## ML3

- Foi criada uma função responsável pela gestão da continuidade de negócios, que presta serviços de apoio e governação da gestão da continuidade do negócio aos departamentos e/ou unidades empresariais participantes.
- Foi definido um quadro de BCM para toda a organização.
- As partes interessadas nas atividades de continuidade das operações são identificadas e envolvidas, e são disponibilizados recursos adequados (pessoas, financiamento e ferramentas) para apoiar as atividades de continuidade das operações.
- A análise do impacto empresariais das funções-chave é efetuada de forma sistemática. Esta análise constitui a base para o desenvolvimento de planos de continuidade.
- São definidos cenários de catástrofe realistas e criados planos de recuperação adequados para manter e restabelecer o funcionamento da(s) função(ões), em conformidade com os requisitos empresariais.
- Os objetivos de tempo de recuperação (RTO) e os objetivos de ponto de recuperação (RPO) para todas as funções empresariais críticas são definidos e incorporados nos planos de recuperação e continuidade em toda a organização.
- A direção está empenhada na importância estratégica de um quadro de BCM eficaz em toda a organização.
- Os departamentos realizam “testes unitários” dos elementos críticos do plano de continuidade de negócios.
- A direção, juntamente com outras funções relevantes, participam em exercícios de gestão de crises.

## ML4

- O resultado dos testes regulares dos planos de recuperação está a ser comparado com os requisitos pré-determinados de RTO e RPO.
- Os planos de continuidade são avaliados, exercitados e atualizados regularmente, com base na sua importância para a atividade.
- Os processos de continuidade e recuperação, bem como a política de apoio à gestão da continuidade de negócios (BCM), são objeto de análises regulares por parte da direção.
- A eficácia do processo de gestão da continuidade de negócios e os testes associados são medidos.
- Os testes de gestão da continuidade de negócios são avaliados, as possibilidades de melhoria são documentadas e acompanhadas pela gestão.

## ML5

- As análises de impacto empresariais são periodicamente revistas e atualizadas à medida que as operações empresariais se alteram.
- Todas as unidades de negócio e departamentos testaram todos os elementos do seu plano de continuidade de negócios, incluindo dependências internas e externas.
- Os resultados dos testes e/ou da ativação do plano de continuidade são comparados com os objetivos de recuperação e os planos são melhorados em conformidade.
- Os planos de continuidade são periodicamente revistos e atualizados.
- Foi adotado um plano plurianual para “elevar continuamente a fasquia” da sofisticação do planeamento e do estado de preparação de toda a empresa.
- Foi estabelecido um programa de comunicações e formação para manter o elevado nível de sensibilização para a continuidade de negócios, na sequência de um programa estruturado de maturidade de competências BCM.
- Os eventos e incidentes são sistematicamente analisados e as lições aprendidas são integradas no quadro da BCM.
- A direção assegura que o responsável/departamento de continuidade de negócios elabora as conclusões corretas a fim de melhorar a BCM.

# Comunicações

A comunicação (de crise) é a comunicação durante incidentes e crises graves, com o objetivo principal de informar todas as partes interessadas de forma atempada e precisa e de conter e minimizar os possíveis efeitos negativos desses incidentes e crises.

## ML1

- Em caso de catástrofe, a comunicação interna e externa é efetuada, pelo menos, numa base *ad hoc* e casuística.
- As decisões sobre a liderança de crises são tomadas pelo menos *ad hoc*, numa base casuística, dependendo da disponibilidade da gestão no local.

## ML2

- As relações públicas básicas são geridas por partes da organização.
- No mínimo, a organização comunica com os clientes, parceiros e fornecedores numa base de melhor esforço (não há garantia de que a mensagem seja recebida como pretendido ou a tempo).
- No mínimo, a organização comunica com a gestão, colaboradores e partes interessadas internas numa base de melhor esforço (não há garantia de que a mensagem seja recebida como pretendido ou a tempo).
- É estabelecida uma relação e coordenação básicas com os bombeiros, polícia e autoridades de segurança locais.
- A direção está envolvida na comunicação de crises.

## ML3

- Existe um plano de comunicação de crise que abrange, pelo menos, as partes abaixo:
- Os conceitos de comunicação de crise (incluindo partes interessadas, canais, momentos, processos, limiar) são definidos e implementados para toda a organização.
- A responsabilidade e a autoridade para o desempenho das atividades de comunicação de crises são atribuídas ao pessoal.
- O pessoal que executa as atividades de comunicação de crises possui as competências e os conhecimentos necessários para desempenhar as responsabilidades que lhe são atribuídas.
- As responsabilidades e diretrizes de comunicação interna são definidas e implementadas.
- As atividades de recuperação são comunicadas às partes interessadas internas e às equipas de gestão.
- As interfaces de comunicação com clientes, parceiros e fornecedores foram definidas e implementadas.
- As comunicações com as partes interessadas internas e externas são realizadas regularmente.

- A cooperação e as comunicações com os bombeiros, a polícia e as autoridades de segurança locais são exercidas.
- Foram elaborados projetos de declarações para cenários de crise importantes.

**ML4**

- São medidos os eventuais danos para a reputação da organização após um incidente (de segurança da informação).
- Durante os testes de recuperação de desastres, a eficácia das comunicações é medida através de uma análise colegial.

**ML5**

- Os conceitos de comunicação de crise são continuamente melhorados e as lições aprendidas com os incidentes são sistematicamente revistas e integradas.
- As vantagens estratégicas e competitivas obtidas com a estrutura da BCM são destacadas em comunicações periódicas internas e externas.
- São realizados exercícios de crise a intervalos regulares com a participação da direção. As conclusões são incorporadas no processo de melhoria contínua.

# Glossário

## (0) Ciclo de vida da informação / Gestão do ciclo de vida da informação

O ciclo de vida da informação começa quando a informação é criada pela primeira vez e continua até que a informação é eliminada ou destruída.

A gestão do ciclo de vida da informação (ILM) é o esforço de supervisionar os dados, desde a sua criação até à sua retirada, para os processar e armazenar da forma mais adequada e rentável, e para minimizar os riscos jurídicos e de conformidade que podem ser introduzidos por esses dados.

## (1) Sistema de Gestão da Segurança da Informação (SGSI)

Um SGSI rege as políticas, os procedimentos, os processos e os fluxos de trabalho escolhidos para ajudar a proteger a segurança da informação de uma organização. Após a organização definir as, estas devem ser implementadas e acionadas em toda a organização. É necessário realizar uma avaliação regular do funcionamento correto para poder ajustar o conteúdo do SGSI à evolução das necessidades da organização.

## (2) Responsabilidades documentadas dos colaboradores em matéria de segurança da informação

Os colaboradores devem saber claramente quais as suas responsabilidades no domínio da segurança da informação. É boa prática documentar essas responsabilidades e distribuí-las. Esta documentação deve ser revista regularmente e adaptada à situação atual da organização.

## (3) Gestão da conformidade

A identificação, a aplicação, o acompanhamento, etc., dos requisitos de conformidade (legislação nacional, contratos, RGPD, NIS, etc., mas também qualidade, saúde e segurança, ambiente, etc.) constituem a base para as escolhas políticas empresariais. A conformidade não é apenas um complemento ou um mal necessário, mas deve ser adotada pela organização como uma medida de responsabilidade empresarial integrada na atividade (diária).

## (4) Princípio da necessidade de saber

Este princípio estabelece que um utilizador só tem acesso à informação necessária para desempenhar as suas funções. O princípio da necessidade de saber pode ser aplicado através de controlos de acesso dos utilizadores e de procedimentos de autorização. Tem como objetivo garantir que apenas as pessoas identificadas como tendo necessidade de saber as informações sensíveis têm acesso a esses dados.

Enquanto a necessidade de saber diz respeito ao número de pessoas que podem ver determinadas informações, o princípio de privilégio mínimo (13) também abrange utilizadores não humanos, como contas de sistemas, aplicações, serviços e dispositivos.

## (5) Automação

A automação é um primeiro passo para a gestão da configuração, no qual ações repetitivas são automatizadas, entre outras coisas, para reduzir a possibilidade de erros humanos. Falamos de gestão da configuração como um método automatizado de manutenção de software, sistemas e redes num estado conhecido e consistente.

## (6) Elementos de configuração e linhas de base de configuração

Uma linha de base de configuração é uma coleção de uma ou mais verificações condicionais designadas por elementos de configuração. É formalmente acordada, documentada e gerida pelo processo de gestão das alterações.

## (7) Artefactos

Uma compilação de software contém não só o código do programador, mas também uma série de artefactos de software. Um artefacto DevOps é um subproduto produzido durante o processo de desenvolvimento de software. Pode consistir no código-fonte do projeto, dependências, binários ou recursos, e pode ser representado em diferentes formatos, conforme a tecnologia.

## (8) Informações sensíveis

Informações sensíveis refere-se a dados que devem ser protegidos contra o acesso não autorizado e a divulgação indesejada, a fim de manter a segurança da informação de uma pessoa ou organização. A exposição de dados sensíveis pode causar danos financeiros, reputacionais ou pessoais.

**Existem três tipos principais de informações sensíveis:**

- Informações pessoais (ou IPI; informações pessoais identificáveis)
- Informações empresariais
- Informações classificadas

## (9) Revisão do código

A revisão do código é uma atividade de garantia da qualidade do software na qual uma ou várias pessoas, que não o(s) autor(es) de um código, examinam esse código. Esta ação pode ser realizada por várias boas razões:

- Melhorar a qualidade do código
- Encontrar defeitos no código numa fase inicial do desenvolvimento
- Transferir conhecimentos
- ...

## (10) Testes de penetração

Os testes de penetração são uma forma de hacking ético, um método de avaliação da segurança de uma infraestrutura informática através da simulação de um ataque de pessoas externas e/ou internas mal-intencionadas. São feitas tentativas para explorar potenciais vulnerabilidades e/ou engenharia social para expor fragilidades de configuração ou de comportamento.

## (11) Entradas de aplicações

Monitorização dos registos das aplicações para detetar entradas inválidas ou inesperadas. Em ambientes de grande dimensão, este processo costuma faz parte da solução SIEM.

## (12) Bloqueio de acesso

Capacidade de desativar (temporariamente) as contas da rede. Por exemplo, durante a investigação de um evento de segurança. O bloqueio de acesso pode ser executado num modo automatizado (p. ex., parte da funcionalidade SIEM) ou manual.

## (13) Privilégio mínimo

O princípio de privilégio mínimo refere-se a um conceito de segurança da informação no qual um utilizador recebe os níveis de acesso mínimos ou as permissões necessárias mínimas para desempenhar as suas funções. O princípio de privilégio mínimo também pode ser aplicado aos sistemas de TIC, para garantir que estes apenas tenham acesso aos dados necessários para o processamento das suas tarefas.

## (14) Registo de eventos centralizado

O registo centralizado é um tipo de solução de registo que consolida os dados de registo e os envia para um local de armazenamento central e acessível. Ajuda a consolidar, analisar e visualizar as informações de forma rápida e clara. Quando configurado de forma correta,
pode ajudar a tornar os registos invioláveis.

## (15) Reforço da infraestrutura

O reforço da infraestrutura refere-se à redução da superfície de ataque - na qual a superfície de ataque é a combinação de todos os pontos onde um cibercriminoso pode atacar - para cada componente e cada camada dessa infraestrutura TIC.

## (16) Restrições a nível do sistema operativo

As restrições a nível do sistema operativo referem-se a etapas ou medidas específicas utilizadas para proteger o sistema operativo de ameaças, vírus, worms, malware ou intrusões remotas de piratas informáticos.
Concentra-se em:

- contas de utilizador do sistema operativo: limitar o número de utilizadores do sistema operativo para minimizar o risco de uma pessoa não autorizada obter acesso aos mesmos.
- permissões de ficheiros: utilizar as permissões de ficheiros do sistema operativo para restringir o acesso dos utilizadores aos ficheiros.

## (17) Controlo de versão das alterações

Os sistemas de controlo de versões registam todas as alterações feitas num ficheiro ou num conjunto de ficheiros ao longo do tempo. As versões anteriores de uma configuração podem ser acedidas através do controlo de versões e, através do registo, todas as alterações podem ser determinadas.

## (18) Estratégia de recurso

A estratégia de recurso é um plano que contém um conjunto de ações alternativas necessárias caso o plano de lançamento tenha de ser abandonado devido a problemas imprevistos. A estratégia pode ser: recuar, avançar, eliminar e reiniciar a partir do código-fonte, etc.

## (19) Validação

A validação é realizada para verificar se os dados e os suportes de dados são efetivamente removidos e/ou destruídos em conformidade com os requisitos empresariais ou de conformidade documentados.

A política da própria organização, assim como os requisitos decorrentes do RGPD, etc., especificam quando é que os dados (registos de clientes, ficheiros de registo, etc.) devem ser removidos ou destruídos. A validação é necessária para verificar se esta remoção ou destruição está efetivamente a ser realizada a tempo e da forma indicada para todos os dados e suportes de dados abrangidos.

## (20) Política de controlos criptográficos

Política empresarial que especifica qual a encriptação (mínima) a utilizar (pelo menos para todos os dados confidenciais/sensíveis). Exemplos:

- Utilizar, pelo menos, TLS 1.2 (pelo que TLS 1.0 e 1.1 já não são permitidos)
- Nível mínimo de encriptação para a encriptação total do disco
- Utilização e gestão de chaves SSH
- Utilização e gestão de certificados digitais SSL

## (21) Monitorização em banda

A monitorização em banda é a capacidade de monitorizar a partir da(s) sua(s) própria(s) rede(s) através de um sistema que verifica constantemente a(s) rede(s) à procura de componentes lentos ou defeituosos e que envia notificações de forma (semi-)automática (por e-mail, SMS ou outros alarmes) em caso de avarias ou outros problemas.

## (22) Monitorização fora de banda

A monitorização de dispositivos fora de banda significa que se utiliza um caminho alternativo para monitorizar a rede, os sistemas e/ou os serviços de um ponto de vista externo. É frequentemente utilizada para monitorizar a experiência do utilizador (testes E2E) ou a disponibilidade externa dos serviços.

## (23) Monitorização ponta-a-ponta (E2E)

A monitorização E2E é o processo de análise de dados entre infraestruturas (redes, dispositivos, aplicações e serviços) para medir a experiência digital do utilizador final. A monitorização E2E tenta olhar para o todo e não para a soma das diferentes partes de que algo é feito. Exemplo:  um objeto de monitorização E2E que mede o tempo que demora desde o pedido de um cliente até este receber a resposta (correta).

## (24) Perfil de ameaça

O desenvolvimento de um perfil de ameaça pormenorizado fornece a uma organização uma ilustração clara das ameaças que enfrenta, permitindo que esta implemente um programa proativo de gestão de incidentes que se

concentra na componente de ameaça do risco. Permite à organização antecipar e atenuar futuros ataques com base neste conhecimento pormenorizado das ameaças.

## (25) Planos de continuidade pró-ativos

Para a maioria das empresas, o planeamento da continuidade de negócios é/era imediatamente equiparado à recuperação de desastres (= capacidade reativa de uma empresa para continuar as suas operações após uma perturbação não planeada). A mentalidade reativa em torno da continuidade de negócios evoluiu para incluir um planeamento proativo e preventivo, principalmente para otimizar a eficiência das atividades (= proativo).

## (26) Ciclo de vida da informação

Na gestão da segurança da informação, o ciclo de vida da informação refere-se às fases que a informação atravessa desde a sua criação até à sua eventual destruição ou eliminação. Este ciclo de vida é crucial para a aplicação de medidas de segurança eficazes para proteger a confidencialidade, a integridade e a disponibilidade de informações sensíveis.

## (27) Universo de auditoria

Mapa de auditoria que inclui e define todos os objetos de uma auditoria. O universo de auditoria inclui, assim, todos os temas, unidades organizacionais, sistemas, etc., relevantes para o planeamento e a realização de atividades de auditoria num período definido.

EUROPEAN
TLD ISAC

Belliardstraat 20 (6th floor) 1040 Brussels, Bélgica

+32 2 627 5550

secretariat@tld-isac.eu

www.tld-isac.eu