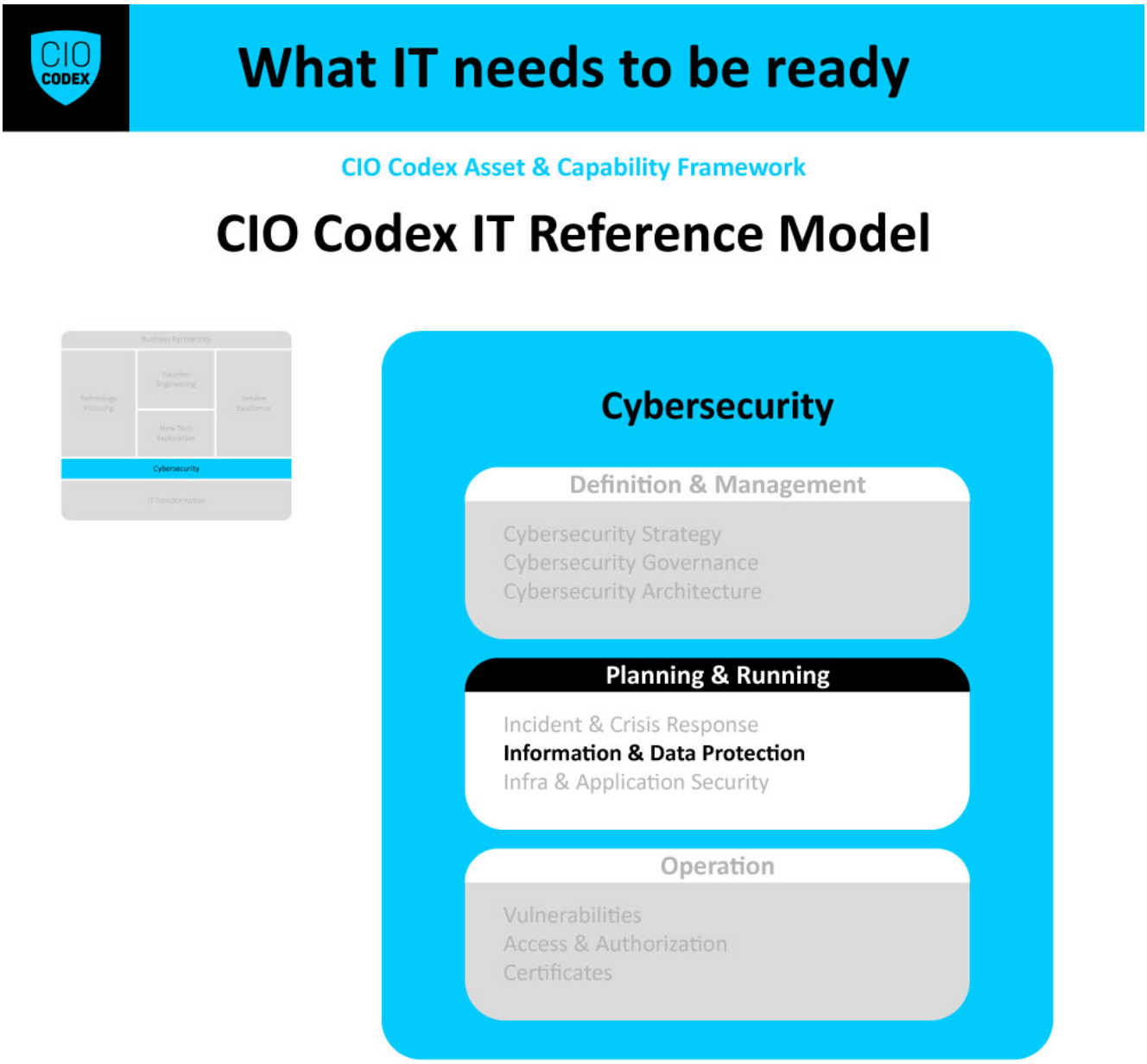

A capability de Information & Data Protection, integrada à macro capability Planning & Running e situada na camada Cybersecurity do CIO Codex Capability Framework, é fundamental no contexto atual, onde os dados são ativos críticos para as organizações.

Esta capability é responsável por garantir que as informações confidenciais permaneçam protegidas, preservando a integridade e a confidencialidade dos ativos de informação.

Os conceitos principais desta capability envolvem os Dados Críticos, que são informações vitais para o funcionamento e os objetivos da organização, e a Proteção de Dados, que abrange o conjunto de práticas, políticas e tecnologias destinadas a salvaguardar os dados contra acessos não autorizados, vazamentos ou perda.

A Criptografia surge como uma técnica essencial para transformar dados em um formato ilegível, protegendo-os durante armazenamento e transmissão.

Características notáveis desta capability incluem o Controle de Acesso, que impõe políticas e mecanismos rigorosos para garantir acesso restrito aos dados, e a Criptografia de Dados, que utiliza algoritmos avançados para garantir a segurança das informações sensíveis.

O Backup e Recuperação de Dados são cruciais para a disponibilidade contínua dos dados, enquanto a Prevenção de Perda de Dados e a Auditoria de Dados são fundamentais para evitar vazamentos de informações e monitorar atividades de acesso.

O propósito central da Information & Data Protection é assegurar que informações sensíveis e estratégicas estejam protegidas contra ameaças internas e externas, desempenhando um papel vital na manutenção da confiança dos clientes, no cumprimento de regulamentações de privacidade e na preservação da reputação da organização.

Dentro do CIO Codex Capability Framework, os objetivos da Information & Data Protection incluem assegurar a eficiência operacional através da implementação de controles de proteção de dados, promover a inovação no desenvolvimento de soluções de proteção de dados e garantir uma vantagem competitiva, pois a proteção eficaz dos dados é um diferencial importante para clientes e parceiros de negócios.

No que diz respeito ao impacto tecnológico, a Information & Data Protection influencia diversas dimensões, como a Infraestrutura, com a implementação de medidas de segurança em servidores e redes, a Arquitetura, que define padrões de criptografia e autenticação, os Sistemas, desenvolvendo políticas de acesso a dados, a Cybersecurity, com foco na proteção de informações e dados confidenciais, e o Modelo Operacional, que estabelece procedimentos para a gestão de incidentes de segurança de dados.

Resumindo, a Information & Data Protection é uma capability essencial que fornece às organizações as ferramentas e processos necessários para a proteção eficaz de dados e informações.

Esta capability é crucial para garantir a segurança dos ativos de informação, contribuindo significativamente para a eficiência operacional, inovação e vantagem competitiva no cenário atual, onde a segurança dos dados é um fator crítico para o sucesso e a confiança no ambiente de negócios.

Conceitos e Características

A capability de Information & Data Protection é vital em um mundo onde dados são ativos críticos.

Ela garante que as informações confidenciais permaneçam confidenciais, protegendo a integridade e a confidencialidade dos ativos de informações da organização.

Conceitos

- Dados Críticos: Informações que são essenciais para o funcionamento e os objetivos da organização, frequentemente incluindo informações confidenciais, propriedade intelectual e dados de clientes.
- Proteção de Dados: O conjunto de práticas, políticas e tecnologias destinadas a garantir que os dados sejam preservados contra acessos não autorizados, vazamentos ou perda.
- Criptografia: A técnica de transformar dados em um formato ilegível para protegê-los durante o armazenamento e a transmissão, sendo decodificáveis apenas por aqueles com a chave de acesso.

Características

- Controle de Acesso: Implementação de políticas e mecanismos rigorosos para garantir que apenas indivíduos autorizados tenham acesso aos dados.
- Criptografia de Dados: Utilização de algoritmos robustos para criptografar informações sensíveis, garantindo que mesmo se os dados forem comprometidos, eles permanecerão ilegíveis.
- Backup e Recuperação de Dados: Desenvolvimento de estratégias de backup eficazes para garantir a disponibilidade contínua de dados, mesmo em situações de desastre.
- Prevenção de Perda de Dados: Implementação de ferramentas e políticas para evitar vazamentos de informações confidenciais.
- Auditoria de Dados: Monitoramento constante das atividades de acesso aos dados para identificar comportamentos suspeitos ou não autorizados.

Propósito e Objetivos

A Information & Data Protection é uma capability essencial para salvaguardar a integridade, confidencialidade e disponibilidade dos dados críticos de uma organização.

Seu propósito fundamental é assegurar que informações sensíveis e estratégicas estejam protegidas contra ameaças internas e externas.

Ela desempenha um papel vital na manutenção da confiança dos clientes, no cumprimento de regulamentações de privacidade e na preservação da reputação da organização.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos da Information & Data Protection são definidos de maneira clara:

- Eficiência Operacional: A capability busca a eficiência operacional, implementando controles e medidas de proteção de dados de forma que não prejudiquem a produtividade dos processos de negócios.
- Inovação: Incentiva a inovação ao desenvolver soluções de proteção de dados que permitam o uso seguro de novas tecnologias e modelos de negócios.
- Vantagem Competitiva: Garante que a organização tenha uma vantagem competitiva, pois a proteção adequada dos dados pode ser um diferencial importante para clientes e parceiros de negócios.

Impacto na Tecnologia

A Information & Data Protection influencia diversas dimensões da tecnologia:

- Infraestrutura: Implementa medidas de segurança em servidores, armazenamento e redes para proteger os dados em repouso e em trânsito.
- Arquitetura: Define padrões de criptografia, autenticação e autorização para garantir que os sistemas e aplicativos estejam protegidos contra

ameaças cibernéticas.
- Sistemas: Desenvolve políticas de acesso a dados, permitindo que apenas pessoal autorizado acesse informações sensíveis.
- Cybersecurity: A proteção de informações e dados confidenciais é fundamental para evitar vazamentos e violações de segurança.
- Modelo Operacional: Define procedimentos para a gestão de incidentes de segurança de dados, assegurando que a organização esteja preparada para responder a ameaças.

Roadmap de Implementação

A capability de Information & Data Protection desempenha um papel crítico na segurança cibernética e na proteção dos ativos de informações de uma organização.

Sua implementação requer uma abordagem estruturada e bem planejada para garantir que os dados críticos permaneçam confidenciais e íntegros.

Neste contexto, um roadmap de implementação considerando os princípios do CIO Codex Capability Framework:

- Avaliação de Dados Críticos: O primeiro passo é identificar e classificar os dados críticos da organização, incluindo informações confidenciais, propriedade intelectual e dados de clientes. Isso permitirá um foco direcionado na proteção desses ativos essenciais.
- Definição de Políticas de Proteção de Dados: Desenvolva políticas de proteção de dados claras e abrangentes que estabeleçam as diretrizes para o acesso, armazenamento e uso de informações sensíveis. Essas políticas devem ser alinhadas com regulamentações relevantes de privacidade.
- Implementação de Controles de Acesso: Estabeleça mecanismos rigorosos de controle de acesso para garantir que apenas pessoal autorizado tenha permissão para acessar dados críticos. Isso pode incluir autenticação multifator e segregação de funções.
- Criptografia de Dados: Implemente a criptografia de dados em repouso e em trânsito. Isso garante que mesmo se os dados forem comprometidos, eles permaneçam ilegíveis para terceiros não autorizados.

- Desenvolvimento de Planos de Backup e Recuperação: Crie estratégias de backup e recuperação de dados sólidas para garantir a disponibilidade contínua de informações críticas, mesmo em caso de desastres ou incidentes.
- Prevenção de Perda de Dados: Implemente ferramentas e tecnologias para prevenir a perda de dados, evitando vazamentos acidentais ou intencionais de informações confidenciais.
- Auditoria de Dados e Monitoramento Contínuo: Estabeleça sistemas de auditoria de dados que monitorem continuamente as atividades de acesso aos dados. Isso ajuda a identificar comportamentos suspeitos ou não autorizados.
- Treinamento e Conscientização: Promova a conscientização sobre a importância da proteção de dados entre os funcionários e forneça treinamento regular sobre as políticas e procedimentos de proteção de dados.
- Teste de Incidentes de Segurança: Realize testes regulares de incidentes de segurança para avaliar a eficácia das medidas de proteção de dados e a capacidade de resposta a ameaças.
- Conformidade com Regulamentações: Garanta que todas as práticas de proteção de dados estejam em conformidade com regulamentações de privacidade relevantes, como o GDPR, LGPD e outras normas aplicáveis.
- Aprimoramento Contínuo: Estabeleça um ciclo de melhoria contínua, revisando periodicamente as políticas e procedimentos de proteção de dados e ajustando-os com base nas lições aprendidas e nas mudanças no cenário de ameaças.

A implementação eficaz da Information & Data Protection não apenas protegerá os ativos de informações da organização, mas também contribuirá para a eficiência operacional, inovação e vantagem competitiva.

Esta capability é um elemento essencial para preservar a integridade e a confidencialidade dos dados críticos e manter a confiança dos clientes e parceiros de negócios.

Melhores Práticas de Mercado

Dentro do contexto do CIO Codex Capability Framework, a capability de Information & Data Protection assume um papel crucial na preservação da integridade, confidencialidade e disponibilidade dos dados, que são ativos críticos em um mundo cada vez mais digitalizado.

Para garantir uma proteção eficaz dos dados, é fundamental adotar as melhores práticas de mercado.

A seguir, as principais melhores práticas amplamente reconhecidas neste campo:

- Classificação de Dados: Inicie com uma clara classificação de dados, identificando quais informações são críticas para a organização. Isso permite direcionar os recursos de proteção para os dados mais sensíveis e valiosos.
- Controle de Acesso: Implemente rigorosos controles de acesso, garantindo que apenas pessoas autorizadas tenham permissão para acessar dados sensíveis. A autenticação multifatorial e a gestão de identidade desempenham um papel fundamental nesse aspecto.
- Criptografia de Dados: Utilize criptografia robusta para proteger dados em repouso e em trânsito. A criptografia garante que mesmo se os dados forem comprometidos, eles permaneçam ilegíveis para qualquer pessoa sem a chave de acesso.
- Políticas de Retenção de Dados: Estabeleça políticas claras de retenção de dados que determinem por quanto tempo os dados devem ser armazenados e quando devem ser destruídos. Isso ajuda a reduzir o risco de retenção excessiva de informações.
- Backup e Recuperação de Dados: Desenvolva estratégias de backup eficazes para garantir a disponibilidade contínua de dados, mesmo em situações de desastre. Teste regularmente os procedimentos de recuperação para garantir sua eficácia.
- Prevenção de Perda de Dados: Implemente ferramentas e políticas para prevenir a perda acidental ou intencional de dados confidenciais. A monitorização constante das atividades de dados pode ajudar a identificar comportamentos suspeitos.
- Auditoria de Dados: Realize auditorias regulares de dados para monitorar quem acessou informações sensíveis e quando. Isso ajuda a identificar

atividades não autorizadas ou suspeitas e a garantir a conformidade com políticas de segurança.
- Conscientização e Treinamento: Invista na conscientização e treinamento da equipe para que todos compreendam a importância da proteção de dados e saibam como agir corretamente em relação a eles.
- Testes de Intrusão: Realize testes regulares de intrusão para identificar vulnerabilidades em sistemas e aplicativos que possam ser exploradas por atacantes. Isso ajuda a fortalecer a postura de segurança.
- Conformidade Regulatória: Mantenha-se atualizado com as regulamentações de privacidade e proteção de dados relevantes para sua indústria e região. Esteja em conformidade com essas regulamentações para evitar penalidades legais.
- Monitoramento Contínuo de Ameaças: Implemente um monitoramento contínuo de ameaças para identificar e responder a novos tipos de ameaças cibernéticas à medida que surgem.

Adotar essas melhores práticas de mercado na capability de Information & Data Protection é fundamental para garantir que os dados confidenciais permaneçam seguros, preservando a confiança dos clientes, cumprindo regulamentações e protegendo a reputação da organização.

Desafios Atuais

A Capability de Information & Data Protection é de suma importância em um cenário em que os dados são ativos críticos para as organizações.

No entanto, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações enfrentam diversos desafios atuais de mercado, alinhados com as melhores práticas do setor.

A seguir, os principais desafios enfrentados pelas organizações:

- Proteção de Dados Sensíveis: O aumento exponencial no volume de dados tornou a proteção de informações sensíveis mais complexa. As organizações enfrentam o desafio de identificar e proteger adequadamente dados críticos.

- Regulamentações em Evolução: As regulamentações de privacidade e segurança de dados estão em constante evolução, criando desafios de conformidade para as organizações, especialmente em âmbito global.
- Ameaças Cibernéticas Avançadas: As ameaças cibernéticas estão se tornando mais sofisticadas, exigindo soluções de proteção igualmente avançadas para evitar violações de dados.
- Nuvem e Mobilidade: A adoção da nuvem e a mobilidade dos funcionários criam desafios adicionais na proteção de dados, especialmente quando os dados são acessados de dispositivos não gerenciados.
- Gerenciamento de Chaves de Criptografia: A implementação eficaz da criptografia requer um gerenciamento rigoroso das chaves de criptografia, o que pode ser complexo.
- Conscientização da Equipe: Educar a equipe sobre práticas de segurança de dados é um desafio constante, pois a conscientização deve ser mantida em todos os níveis da organização.
- Resposta a Incidentes: Ter um plano eficaz de resposta a incidentes é crucial. As organizações enfrentam o desafio de desenvolver e manter processos de resposta ágeis.
- Terceirização de Serviços: Quando serviços são terceirizados, garantir a proteção de dados em toda a cadeia de fornecimento é um desafio, pois a organização pode ter menos controle sobre esses processos.
- Cultura de Privacidade: Estabelecer uma cultura de privacidade e segurança de dados é um desafio, pois requer a adoção de práticas e comportamentos consistentes em toda a organização.
- Gestão de Vulnerabilidades: Identificar e remediar vulnerabilidades de segurança em tempo hábil é um desafio, pois as ameaças evoluem rapidamente.

Esses desafios refletem a crescente importância da Capability de Information & Data Protection no cenário atual de negócios, onde a proteção de dados se tornou uma prioridade crítica.

Superar esses obstáculos é fundamental para garantir que as informações confidenciais permaneçam protegidas e que a organização esteja em conformidade com as regulamentações em constante mudança.

A capability de implementar medidas de proteção de dados eficazes, incluindo criptografia, controle de acesso e políticas de conscientização, é fundamental para

enfrentar esses desafios e manter a integridade e a confidencialidade dos ativos de informações da organização.

Além disso, investir na educação da equipe e na adaptação às mudanças regulatórias é essencial para mitigar os riscos associados à proteção de dados no ambiente empresarial atual.

Tendências para o Futuro

A Capability de Information & Data Protection é de suma importância em um cenário onde os dados se tornaram ativos críticos para as organizações.

Ela desempenha um papel fundamental na garantia da confidencialidade, integridade e disponibilidade dos dados, protegendo-os contra ameaças internas e externas.

À medida que o ambiente de segurança cibernética continua a evoluir, é essencial antecipar as tendências que moldarão o futuro dessa capability.

Portanto, as principais tendências futuras dentro do contexto do CIO Codex Capability Framework:

- Privacidade de Dados Reforçada: Com a crescente preocupação com a privacidade dos dados, as regulamentações se tornarão mais rígidas. As organizações investirão em tecnologias e práticas para garantir a conformidade e proteger os dados dos usuários.
- Proteção de Dados em Multiplataforma: Com a proliferação de dispositivos e ambientes de computação em nuvem, a capacidade de proteger dados em várias plataformas se tornará crucial. Soluções integradas de proteção de dados serão cada vez mais adotadas.
- Inteligência Artificial na Detecção de Ameaças: A IA será amplamente utilizada na detecção de ameaças cibernéticas. Algoritmos de aprendizado de máquina identificarão padrões de comportamento suspeito e ameaças em tempo real.
- Criptografia Quântica: Com o avanço da computação quântica, a criptografia tradicional pode se tornar vulnerável. A criptografia quântica, que oferece segurança inquebrável, será explorada para proteger dados críticos.
- Gestão de Identidade Digital Avançada: O gerenciamento de identidade

digital evoluirá com autenticação biométrica, autenticação de dois fatores e sistemas de gerenciamento de identidade mais robustos para garantir que apenas usuários autorizados acessem dados sensíveis.
- Zero Trust Security: A abordagem Zero Trust ganhará destaque, onde a confiança não é concedida com base na localização ou na rede do usuário, mas em sua autenticação e validação contínuas.
- Proteção de Dados em Tempo Real: A capacidade de proteger dados em tempo real se tornará crucial à medida que as organizações buscam prevenir vazamentos e ataques em tempo hábil.
- Resposta a Incidentes Automatizada: A automação desempenhará um papel importante na resposta a incidentes de segurança de dados, permitindo ação imediata para conter ameaças.
- Blockchain para Integridade de Dados: A tecnologia blockchain será adotada para garantir a integridade dos dados, tornando os registros imutáveis e à prova de adulteração.
- Treinamento de Conscientização em Segurança: Investimentos contínuos em treinamento de conscientização em segurança cibernética se tornarão essenciais, capacitando os colaboradores a reconhecerem e responder a ameaças.

Essas tendências representam as expectativas do mercado e apontam para um futuro em que a proteção de informações e dados será ainda mais crítica.

A Capability de Information & Data Protection desempenhará um papel vital na salvaguarda dos ativos de informações das organizações, garantindo sua integridade e confidencialidade em um ambiente de ameaças em constante evolução.

KPIs Usuais

A capacidade de Information & Data Protection desempenha um papel fundamental na preservação da confidencialidade e integridade dos ativos de informações críticas de uma organização.

Medir o desempenho dessa capability é essencial para garantir a segurança dos dados em um ambiente cada vez mais digital e interconectado.

Abaixo, uma lista dos principais KPIs usuais no contexto do CIO Codex Capability

Framework, que ajudam a avaliar o desempenho da Information & Data Protection:

- Taxa de Conformidade com Regulamentações de Privacidade (Privacy Regulations Compliance Rate): Mede o grau de conformidade da organização com regulamentações de privacidade de dados, como GDPR e LGPD.
- Taxa de Incidentes de Vazamento de Dados (Data Breach Incident Rate): Avalia a frequência com que ocorrem incidentes de vazamento de dados e a eficácia das medidas de prevenção.
- Tempo Médio de Detecção de Vazamentos de Dados (Mean Time to Detect Data Breaches): Calcula o tempo médio necessário para identificar um vazamento de dados desde o momento em que ocorre.
- Taxa de Recuperação de Dados (Data Recovery Rate): Indica a eficácia das estratégias de backup e recuperação de dados, medida pela capacidade de restaurar informações após um incidente.
- Taxa de Criptografia de Dados (Data Encryption Rate): Avalia o percentual de dados confidenciais que são criptografados para proteção contra acessos não autorizados.
- Taxa de Acesso Não Autorizado (Unauthorized Access Rate): Mede a frequência com que ocorrem tentativas de acesso não autorizado aos dados protegidos.
- Tempo Médio de Resposta a Incidentes de Segurança de Dados (Mean Time to Respond to Data Security Incidents): Calcula o tempo médio que a equipe leva para iniciar a resposta a um incidente de segurança de dados após sua detecção.
- Taxa de Auditorias de Dados Concluídas (Completed Data Audits Rate): Avalia a regularidade das auditorias de dados para garantir o cumprimento das políticas de proteção.
- Taxa de Uso de Autenticação Multifatorial (Multifactor Authentication Usage Rate): Indica o percentual de usuários que utilizam autenticação multifatorial para acesso a sistemas e dados sensíveis.
- Taxa de Treinamento em Segurança de Dados (Data Security Training Rate): Avalia a porcentagem de funcionários que receberam treinamento em segurança de dados.
- Taxa de Remediação de Vulnerabilidades (Vulnerability Remediation Rate): Mede a eficácia na correção de vulnerabilidades de segurança de dados identificadas.

- Taxa de Backup de Dados Críticos (Critical Data Backup Rate): Avalia a frequência com que os dados críticos são copiados e armazenados em locais seguros.
- Taxa de Testes de Recuperação de Desastres (Disaster Recovery Testing Rate): Indica a periodicidade com que são realizados testes de recuperação de desastres para garantir a disponibilidade contínua de dados.
- Taxa de Classificação de Dados (Data Classification Rate): Mede o percentual de dados que são classificados de acordo com seu nível de confidencialidade e importância.
- Taxa de Resposta a Solicitações de Acesso a Dados (Data Access Request Response Rate): Avalia a rapidez e eficácia na resposta a solicitações de acesso a dados por partes autorizadas.

Esses KPIs são cruciais para garantir que a Information & Data Protection atue como um escudo eficaz contra ameaças internas e externas, protegendo os dados críticos da organização.

A medição constante desses indicadores permite aprimorar continuamente as práticas de proteção de dados e manter a confiança dos clientes, o cumprimento regulatório e a reputação da organização.

Exemplos de OKRs

A capability de Information & Data Protection na macro capability Planning & Running da camada Cybersecurity desempenha um papel crítico na garantia da segurança e privacidade dos dados críticos da organização.

Essa capability é essencial para proteger informações sensíveis contra acessos não autorizados, vazamentos e outras formas de comprometimento.

Ela envolve o desenvolvimento e implementação de estratégias abrangentes para garantir a integridade e confidencialidade das informações.

A seguir, são apresentados exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a esta capability:

Controle Rigoroso de Acesso aos Dados

Objetivo: Garantir que apenas pessoas autorizadas tenham acesso a dados sensíveis.

- KR1: Implementar autenticação de dois fatores para acesso a sistemas críticos.
- KR2: Estabelecer políticas de acesso baseadas em funções e necessidade de conhecimento.
- KR3: Monitorar e auditar regularmente os acessos aos dados.

Criptografia de Dados Sensíveis

Objetivo: Proteger dados sensíveis por meio de criptografia.

- KR1: Implementar criptografia de ponta a ponta para comunicações de dados sensíveis.
- KR2: Criptografar dados armazenados em sistemas de armazenamento de dados sensíveis.
- KR3: Manter chaves de criptografia em ambientes seguros e de acesso restrito.

Realização de Backup Seguro

Objetivo: Garantir a disponibilidade de dados críticos por meio de backups seguros.

- KR1: Estabelecer políticas de backup regulares e automatizadas.
- KR2: Testar a restauração de dados de backup para garantir a eficácia.
- KR3: Armazenar cópias de backup em locais geograficamente dispersos.

Prevenção de Perda de Dados (DLP)

Objetivo: Implementar medidas para prevenir a perda de dados sensíveis.

- KR1: Configurar sistemas de Prevenção de Perda de Dados para monitorar e bloquear atividades suspeitas.
- KR2: Definir políticas de DLP que incluam a identificação de dados confidenciais.

- KR3: Educar os colaboradores sobre as práticas seguras de manuseio de dados.

Integridade e Confidencialidade das Informações

Objetivo: Assegurar que as informações permaneçam íntegras e confidenciais.

- KR1: Implementar sistemas de detecção de alterações não autorizadas nos dados.
- KR2: Criar trilhas de auditoria detalhadas para todas as atividades relacionadas a dados sensíveis.
- KR3: Realizar avaliações regulares de vulnerabilidades para identificar ameaças potenciais.

Através desses OKRs, a capability de Information & Data Protection desempenha um papel fundamental na proteção dos dados críticos da organização, garantindo que eles permaneçam seguros e confidenciais.

Isso é essencial para cumprir regulamentações de privacidade, manter a confiança dos clientes e evitar danos à reputação da organização.

Critérios para Avaliação de Maturidade

A capability Information & Data Protection, inserida na macro capability Planning & Running e na camada Cybersecurity, desempenha um papel fundamental na preservação da segurança e privacidade dos dados críticos de uma organização.

Para avaliar sua maturidade, seguem critérios inspirados no modelo CMMI, considerando cinco níveis de maturidade: Inexistente, Inicial, Definido, Gerenciado e Otimizado.

Nível de Maturidade Inexistente

- Não há procedimentos formais para proteção de dados.
- Conscientização limitada sobre a importância da proteção de informações sensíveis.

- Ausência de controle de acesso a dados confidenciais.
- Falta de criptografia de dados sensíveis.
- Ausência de backups regulares e políticas de recuperação de dados.

Nível de Maturidade Inicial

- Processos iniciais de proteção de dados, mas não são abrangentes.
- Alguma conscientização sobre a importância da proteção de informações sensíveis.
- Início da implementação de controles de acesso.
- Uso limitado de criptografia para dados confidenciais.
- Início da realização de backups regulares e políticas de recuperação de dados.

Nível de Maturidade Definido

- Processos formalizados e documentados para proteção de dados.
- Conscientização crescente sobre a importância da proteção de informações sensíveis.
- Controles de acesso bem definidos e aplicados.
- Uso consistente de criptografia para dados sensíveis.
- Políticas estabelecidas para backups regulares e recuperação de dados.

Nível de Maturidade Gerenciado

- Processos de proteção de dados são eficazes e adaptáveis.
- Conscientização disseminada sobre a importância da proteção de informações sensíveis.
- Controles de acesso são monitorados e atualizados proativamente.
- Criptografia avançada e medidas de prevenção de perda de dados em vigor.
- Backups regulares e políticas de recuperação de dados são altamente eficazes.

Nível de Maturidade Otimizado

- Processos de proteção de dados são altamente otimizados e inovadores.
- Conscientização e treinamento contínuos sobre proteção de informações sensíveis.
- Controles de acesso avançados com monitoramento em tempo real.
- Criptografia de ponta e medidas avançadas de prevenção de perda de dados.
- Backups automatizados e recuperação de dados instantânea e eficaz.

A avaliação de maturidade da capability Information & Data Protection é crucial para garantir a integridade, confidencialidade e disponibilidade dos dados críticos da organização.

À medida que a maturidade aumenta, a organização está mais preparada para proteger suas informações sensíveis contra ameaças e riscos de segurança cibernética.

Convergência com Frameworks de Mercado

A capability Information & Data Protection, integrante da macro capability Planning & Running e localizada na camada Cybersecurity, é fundamental para a segurança e privacidade dos dados críticos de uma organização.

Esta capability abarca o desenvolvimento e implementação de estratégias para proteger informações sensíveis contra acessos não autorizados, vazamentos e outras formas de comprometimento, aplicando controles de acesso rigorosos, criptografia, backup e medidas de prevenção de perda de dados.

A seguir, é analisada a convergência desta capability em relação a um conjunto dez frameworks de mercado reconhecidos e bem estabelecidos em suas respectivas áreas de expertise:

COBIT

- Nível de Convergência: Alto

- Racional: O COBIT fornece um framework estruturado para governança de TI, incluindo a gestão de riscos e segurança da informação. A Information & Data Protection se alinha com os princípios do COBIT no que diz respeito à proteção de informações e gerenciamento de riscos, garantindo a segurança dos dados e a conformidade com as políticas organizacionais.

ITIL

- Nível de Convergência: Médio
- Racional: O ITIL, focado na gestão de serviços de TI, oferece um contexto relevante para a Information & Data Protection, especialmente no que se refere à gestão de incidentes e problemas relacionados à segurança da informação.

SAFe

- Nível de Convergência: Médio
- Racional: Embora o SAFe seja um framework de desenvolvimento ágil, a integração da Information & Data Protection é vital para garantir a segurança nos processos de desenvolvimento e entrega contínua.

PMI

- Nível de Convergência: Médio
- Racional: A metodologia do PMI, aplicada na gestão de projetos, pode se beneficiar da Information & Data Protection para assegurar a segurança dos dados em todas as fases do projeto.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI foca na maturidade dos processos organizacionais. A Information & Data Protection colabora com o aprimoramento dos

processos, garantindo a segurança e proteção dos dados.

TOGAF

- Nível de Convergência: Médio
- Racional: No TOGAF, que trata de arquitetura empresarial, a Information & Data Protection contribui para a incorporação de práticas de segurança na arquitetura de TI, assegurando a proteção de dados em toda a organização.

DevOps SRE

- Nível de Convergência: Médio
- Racional: Em ambientes DevOps SRE, a rápida inovação e entrega contínua exigem práticas robustas de segurança de dados. A Information & Data Protection é essencial para manter a segurança e a integridade dos dados em tais ambientes.

NIST

- Nível de Convergência: Alto
- Racional: O NIST oferece diretrizes abrangentes para a segurança cibernética. A Information & Data Protection está em conformidade com essas diretrizes, focando na proteção de dados e na prevenção de ameaças cibernéticas.

Six Sigma

- Nível de Convergência: Baixo
- Racional: O Six Sigma, voltado para a melhoria da qualidade e eficiência dos processos, tem uma convergência menor com a Information & Data Protection, mas ainda assim pode beneficiar-se de práticas de proteção de dados para reduzir riscos e erros.

Lean IT

- Nível de Convergência: Baixo
- Racional: O Lean IT, focado na eficiência operacional, tem uma convergência indireta com a Information & Data Protection, pois a segurança de dados contribui para a redução de desperdícios e melhoria da eficiência operacional.

A capability Information & Data Protection desempenha um papel crítico na proteção de ativos de informação, sendo um componente vital para a manutenção da confidencialidade, integridade e disponibilidade dos dados.

Os KPIs relevantes incluem a taxa de incidentes de segurança resolvidos, o tempo médio para detecção de violações de dados e a eficácia das medidas de proteção de dados.

Esta capability é essencial para a resiliência organizacional em um cenário de ameaças cibernéticas em constante evolução.

Processos e Atividades

Develop Data Protection Plans

O desenvolvimento de planos detalhados para proteção de informações e dados é um passo essencial para assegurar que a organização esteja preparada para proteger seus ativos de informação contra ameaças internas e externas.

Este processo envolve a criação de planos que detalham as medidas de segurança a serem implementadas para garantir a confidencialidade, integridade e disponibilidade dos dados.

Os planos devem incluir políticas de acesso, criptografia, backup e recuperação de dados, bem como procedimentos para resposta a incidentes de segurança.

A elaboração desses planos requer uma análise minuciosa dos requisitos regulatórios e das melhores práticas do setor.

É fundamental envolver várias áreas da organização para assegurar que todos os

aspectos de segurança, operacionais e de negócios sejam considerados.

A documentação clara dos papéis e responsabilidades, bem como a comunicação eficaz dos planos a todos os colaboradores, é crucial para a eficácia da implementação.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Risk Assessment	Realizar uma avaliação de riscos para identificar ameaças e vulnerabilidades.	Dados de risco, análise de ameaças	Relatório de avaliação de riscos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Define Protection Policies	Definir políticas de proteção de dados que atendam aos requisitos de segurança e compliance.	Relatório de avaliação de riscos	Políticas de proteção de dados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Develop Protection Procedures	Desenvolver procedimentos detalhados para a implementação das políticas de proteção de dados.	Políticas de proteção de dados	Procedimentos de proteção	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

4	Assign Roles and Responsibilities	Atribuir papéis e responsabilidades para a equipe de proteção de dados.	Procedimentos de proteção	Documento de papéis e responsabilidades	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Document Data Protection Plan	Documentar o plano de proteção de dados de forma detalhada e acessível.	Documento de papéis e responsabilidades	Plano de proteção de dados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Identify Data Protection Requirements

A identificação dos requisitos para proteção de informações e dados é fundamental para assegurar que todas as necessidades de segurança e conformidade sejam atendidas.

Este processo envolve a análise de regulamentos, políticas internas e melhores práticas do setor para determinar as medidas de proteção necessárias.

Os requisitos devem abranger aspectos como controle de acesso, criptografia, backup, prevenção de perda de dados e auditoria.

A identificação precisa desses requisitos permite à organização desenvolver e implementar soluções de proteção de dados eficazes.

A colaboração entre diferentes áreas da TI e do negócio é essencial para garantir que todos os aspectos sejam considerados e que os requisitos sejam adequadamente incorporados aos planos de proteção.

- PDCA focus: Plan
- Periodicidade: Semestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Analyze Regulatory Requirements	Analisar requisitos regulatórios e de compliance para proteção de dados.	Regulamentos, políticas internas	Relatório de requisitos regulatórios	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Identify Business Needs	Identificar as necessidades de negócios relacionadas à proteção de dados.	Relatório de requisitos regulatórios	Relatório de necessidades de negócios	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Define Security Controls	Definir os controles de segurança necessários para atender aos requisitos identificados.	Relatório de necessidades de negócios	Lista de controles de segurança	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Develop Compliance Procedures	Desenvolver procedimentos de compliance para garantir a conformidade com os requisitos.	Lista de controles de segurança	Procedimentos de compliance	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Document Requirements	Documentar todos os requisitos de proteção de dados de forma clara e acessível.	Procedimentos de compliance	Documentação de requisitos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

Implement Data Protection Solutions

A implementação das soluções de proteção de dados conforme planejado é crucial para garantir que as medidas de segurança sejam efetivamente aplicadas e mantidas.

Este processo envolve a execução dos procedimentos definidos nos planos de proteção de dados, incluindo a configuração de controles de acesso, a implantação de criptografia, a implementação de backups regulares e a utilização de ferramentas de prevenção de perda de dados.

A coordenação entre as várias áreas de TI é fundamental para assegurar que as soluções sejam integradas de forma eficaz e que os dados estejam protegidos em todos os níveis.

A formação contínua da equipe e a validação das soluções implementadas através de testes regulares garantem a eficácia das medidas de proteção.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Configure Access Controls	Configurar controles de acesso para garantir que apenas usuários autorizados acessem os dados.	Lista de controles de segurança	Controles de acesso configurados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Implement Encryption	Implementar criptografia para proteger dados sensíveis durante o armazenamento e a transmissão.	Lista de controles de segurança	Dados criptografados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Setup Backup Procedures	Configurar procedimentos de backup para garantir a disponibilidade dos dados.	Lista de controles de segurança	Procedimentos de backup configurados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Deploy DLP Tools	Implementar ferramentas de prevenção de perda de dados para proteger informações confidenciais.	Lista de controles de segurança	Ferramentas DLP implementadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Validate Implementation	Validar a implementação das soluções de proteção através de testes e auditorias.	Ferramentas DLP implementadas	Implementação validada	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Monitor Data Protection Performance

O monitoramento contínuo do desempenho das soluções de proteção de dados é vital para garantir a eficácia das medidas de segurança e identificar áreas que necessitam de melhoria.

Este processo envolve a coleta e análise de dados sobre a performance dos controles de segurança implementados, incluindo a eficácia da criptografia, a confiabilidade dos backups e a eficiência das ferramentas de prevenção de perda de dados.

A auditoria regular e a análise de logs de acesso são componentes chave deste processo.

O feedback obtido através do monitoramento é utilizado para ajustar e melhorar continuamente as soluções de proteção de dados, assegurando que a organização esteja sempre protegida contra novas ameaças.

- PDCA focus: Check
- Periodicidade: Mensal

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Collect Performance Data	Coletar dados de desempenho das soluções de proteção de dados implementadas.	Logs de acesso, relatórios de auditoria	Dados de desempenho coletados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Analyze Data Protection Metrics	Analisar as métricas de proteção de dados para avaliar a eficácia das soluções implementadas.	Dados de desempenho coletados	Relatórios de análise de métricas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Conduct Security Audits	Realizar auditorias de segurança para identificar possíveis vulnerabilidades e não conformidades.	Relatórios de análise de métricas	Relatórios de auditoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

4	Generate Improvement Reports	Gerar relatórios de melhoria com base na análise de desempenho e auditorias realizadas.	Relatórios de auditoria	Relatórios de melhoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Report Findings	Relatar as descobertas e recomendações de melhoria para a alta gestão e partes interessadas.	Relatórios de melhoria	Relatórios de descobertas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Review and Improve Data Protection Practices

A revisão e melhoria contínua das práticas de proteção de dados é essencial para manter a eficácia das medidas de segurança e adaptar-se às novas ameaças.

Este processo envolve a análise dos resultados do monitoramento e auditorias para identificar áreas de melhoria.

As lições aprendidas são integradas aos procedimentos existentes, e novos controles de segurança são desenvolvidos conforme necessário.

O processo também inclui a atualização das políticas e procedimentos de proteção de dados, a realização de treinamentos regulares e a validação das práticas de segurança através de testes contínuos.

A melhoria contínua assegura que a organização esteja sempre pronta para proteger seus dados contra ameaças emergentes.

- PDCA focus: Act
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Analyze Audit Findings	Analisar as descobertas das auditorias e monitoramento de desempenho.	Relatórios de auditoria	Análise de descobertas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Identify Improvement Areas	Identificar áreas de melhoria nas práticas de proteção de dados com base na análise.	Análise de descobertas	Lista de áreas de melhoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Update Protection Procedures	Atualizar os procedimentos de proteção de dados para incorporar as melhorias identificadas.	Lista de áreas de melhoria	Procedimentos atualizados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Conduct Training Sessions	Realizar sessões de treinamento para assegurar que a equipe esteja familiarizada com os procedimentos atualizados.	Procedimentos atualizados	Sessões de treinamento realizadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Validate Protection Practices	Validar as práticas de proteção através de testes e auditorias contínuas.	Procedimentos atualizados	Práticas validadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity