S4agro

Soluções sustentáveis
para o setor agroindustrial

Factores críticos para a Cibersegurança

Produtividade, eficácia e eficiência ao nível da Indústria 4.0 e Economia Circular.

Cofinanciado por:

COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA
Fundo Europeu
de Desenvolvimento Regional

Factores críticos para a Cibersegurança

Pedro Dinis Gaspar

(coordenação)

Data

17-03-2022

Cofinanciado por:

COMPETE 2020
PROGRAMA OPERACIONAL COMPETITIVIDADE E INTERNACIONALIZAÇÃO

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu
de Desenvolvimento Regional

Ficha Técnica

Título:
Factores críticos para a Cibersegurança

Coordenação editorial:
Pedro Dinis Gaspar

Autores:
Mário Antunes
Carlos Rabadão

Data:
Março 2022

Projeto gráfico e design:
Catarina Laginha

Nota Explicativa:
Este estudo de factores críticos foi desenvolvido no âmbito do projeto S4Agro - Soluções Sustentáveis para o Setor Agroindustrial (Aviso 02/SIAC/2019 – Sistema de Apoio a Ações Coletivas – Qualificação, Projeto SIAC 46425), apoiado pelo COMPETE 2020.

O documento encontra-se disponível para download em www.s4agro.pt.

Agradecimentos:
O editor e autores agradecem ao "Programa Operacional Fatores de Competitividade" - COMPETE, pelo financiamento atribuído ao projeto S4Agro
O consórcio do Projeto S4Agro agradece a todas as instituições, entidades e organismos, governamentais, públicos e privados, que, de algum modo, quer pela disponibilização de dados, quer pelas indicações fornecidas, contribuíram para a elaboração do presente estudo.

Parceiros

Universidade da Beira Interior

Universidade de Évora

Instituto Politécnico de Castelo Branco

Instituto Politécnico de Coimbra

Instituto Politécnico da Guarda

Instituto Politécnico de Leiria

Instituto Politécnico de Viana do Castelo

InovCluster
Associação do Cluster Agro-Industrial do Centro

Enquadramento

O projeto S4AGRO - *Soluções Sustentáveis para o Setor Agroindustrial* visa qualificar as PME do setor agroindustrial, nomeadamente da fileira dos: produtos cárneos, produtos hortofrutícolas, produtos lácteos e, produtos de padaria/pastelaria, para a adoção de soluções inovadoras e sustentáveis, que permitam aumentar a sua produtividade, eficácia e eficiência ao nível da indústria 4.0 e economia circular.

O projeto S4AGRO pretende identificar e disseminar junto das PME do setor agroindustrial, boas práticas na utilização de embalagens primárias (ecológicas) e secundárias (recicláveis e/ou reutilizáveis) sustentáveis e os fatores críticos à aplicação destas e as práticas logísticas mais eficazes. Neste contexto, encontram-se também as tecnologias inovadoras e boas práticas em utilização de embalagens inteligentes e/ou ativas. Aborda igualmente a cibersegurança, visando identificar fatores críticos para a segurança de sistemas informáticos e qualificação para a aplicação de boas práticas. Destina-se também à identificação e caraterização de pontos geradores de desperdício e à definição de soluções inovadoras para o seu aproveitamento com vista à melhoria da eficiência produtiva e redução dos impactes ambientais. Visa ainda, permitir, divulgar e facilitar o acesso a processos de capacitação para a introdução de inovação de base científica e tecnológica com o intuito de capacitar PME para acelerar a adoção da Indústria 4.0.

Agradecimentos

O editor e autores agradecem ao Portugal 2020, COMPETE 2020 - Programa Operacional da Competitividade e Internacionalização (POCI) o financiamento do projeto S4AGRO - *Soluções Sustentáveis para o Setor Agroindustrial* (Aviso 02/SIAC/2019 – SIAC 46425), no âmbito do qual este manual foi produzido.

Agradece-se a todas as instituições, entidades e organismos, governamentais, públicos e privados, que, de algum modo, quer pela disponibilização dados, quer pelas indicações fornecidas, contribuíram para a elaboração do presente estudo "Factores críticos para a Cibersegurança".

Governance, Risk & Compliance

Pontos críticos no setor Agro Industrial

Versão 1.1, 30 Agosto 2021

Access Level: Client

Índex

1 INTRODUÇÃO

Este documento constitui o principal entregável da "Atividade 4 – Elaboração do estudo de fatores críticos para a cibersegurança em PME do setor agroindustrial" do projeto de serviços de consultoria especializada para apoio a estudo de boas práticas em cibersegurança no setor agroalimentar, contratado pelo Instituto Politécnico de Leiria à CIPHER.

O documento refere um conjunto de pontos críticos para a segurança do setor agroindustrial, conjunto esse que é baseado nas respostas de uma amostra de empresas do setor a questionários online, bem como a entrevistas via videoconferência.

1.1 ÂMBITO

O trabalho realizado pela CIPHER teve como base o feedback de uma amostra de 13 empresas do setor agroindustrial, base essa que serviu para uma extrapolação relativamente às necessidades generalizadas do setor no âmbito da segurança de informação e cibersegurança.

1.2 A CIPHER

A DOGNÆDIS/CIPHER é uma empresa focada em cibersegurança e segurança de informação com o lema "transformar a cibersegurança dos nossos clientes num valor acrescentado", e apresenta-se como prestadora de serviços especializados e focados na eficiência, sendo também produtora de tecnologias e de soluções inovadoras na área de segurança de informação e áreas subjacentes.

Em fins de 2018 o Grupo Prosegur iniciou a aquisição da CIPHER, uma empresa multinacional especializada em Segurança da Informação. Hoje a DOGNÆDIS/CIPHER, atualmente desenvolve atividade em 24 países distintos a partir dos seus escritórios em Portugal, Reino Unido, Estados Unidos da América, Brasil e Espanha. Contamos com aproximadamente 360 funcionários, dos quais 97 estão alocados aos serviços de SOC.

1.3 EQUIPA DE PROJETO

A equipa alocada ao presente projeto integra a *Service Line* de *Governance, Risk and Compliance* (GRC) da CIPHER, e é composta da seguinte forma:

- **Gestor de Projeto** (consultor de ligação) - Responsável pela gestão operacional do projeto, pela articulação com a equipa de controlo de qualidade e pela interlocução com o cliente:
  - Gustavo Neves (gneves@cipher.com)
- **Consultor Líder** - Responsável pela perspetiva técnica de todo o processo
  - Jorge de Carvalho (jcarvalho@cipher.com)

- **Consultor**:
    - João Damasceno (jdamasceno@cipher.com)

O projeto contou, do lado do Instituto Politécnico de Leiria, com os valiosos contributos de:

- Mário Antunes (mario.antunes@ipleiria.pt)
- Carlos Rabadão (carlos.rabadao@ipleiria.pt)

1.4 METODOLOGIA

As constatações enumeradas neste documento basearam-se nas respostas obtidas num questionário online junto de representantes de empresas do setor Agroindustrial. Participaram na resposta a este questionário 11 empresas, bem como 2 outras entrevistadas com recurso a videoconferência, dividindo-se pelos seguintes setores agroindustriais:

Setor	Nº de entidades
Cárneo	4
Hortofruticulturas	2
Lácteos	3
Padaria/Pastelaria	4

Os trabalhos da Atividade 1 iniciaram-se com o *kick-off* do projeto, a 25-03-2021, tendo o respetivo relatório sido concluído a 30-08-2021.

1.5 DIFICULDADES NA CONDUÇÃO DO PROJETO

O projeto teria beneficiado de uma participação mais numerosa das empresas do setor agroindustrial, no sentido de tornar a amostra mais significativa. A abordagem que se pretendia inicialmente para a recolha de informação seria baseada em entrevistas interativas com um conjunto de organizações, por forma a explorar os temas de segurança pertinentes, ajustando as questões às realidades específicas de cada caso. No entanto, poucas foram as organizações que demonstraram disponibilidade, o que obrigou a optar por um modelo de questionário fechado, e igual para todas as entidades, uma vez que se mostrou prioritário poupar o tempo dos intervenientes no processo.

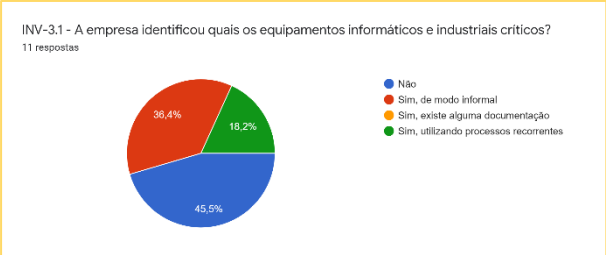
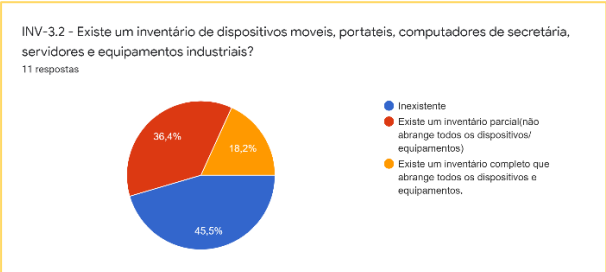
2 IDENTIFICAÇÃO DE PONTOS CRÍTICOS NO SETOR AGROINDUSTRIAL

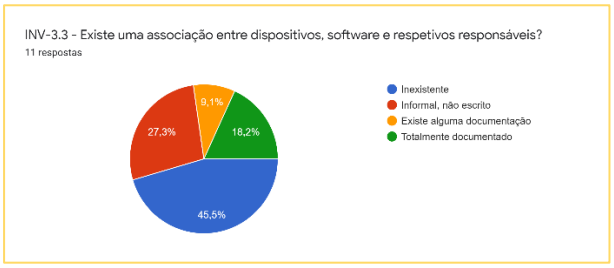
De acordo com o que ficou definido em caderno de encargos pelo Instituto Politécnico de Leiria, a CIPHER utilizou como referencial para a identificação dos pontos críticos para a segurança da informação nos setores agroindustriais o Quadro Nacional de Referência para a Cibersegurança (QNRCS), da autoria do Centro Nacional de Cibersegurança (CNCS). Assim sendo, os próximos capítulos percorrem um subconjunto dos controlos aí definidos, tendo o trabalho resultado numa avaliação por parte da CIPHER relativamente aos principais pontos de melhoria no estado de cumprimento de cada um, e que a seguir se detalham. Sublinhe-se mais uma vez que se trata de um subconjunto, tendo essa seleção sido feito pelos auditores externos da CIPHER, com base em critérios de aplicabilidade ou adequação à organização e ao âmbito definido para o presente trabalho.

2.1 IDENTIFICAR

2.1.1 ID.GA - GESTÃO DE ATIVOS

Neste domínio, o QNRCS visa os seguintes objetivos:
"A organização deve identificar os dados, colaboradores, equipamentos, sistemas e instalações que permitem cumprir os seus objetivos no decorrer da sua atividade. Devem ser identificados e geridos de forma consistente com aquela que é a sua relevância no cumprimento dos objetivos da organização e com a estratégia de gestão do risco."

Resultados relevantes do inquérito	***Pontos críticos***
 	• Há uma carência óbvia de sistematização de informação relativa a inventário de equipamentos; • Não parece haver uma correta caraterização da criticidade dos ativos; • Não existe formalização na atribuição de responsabilidades sobre ativos de informação.

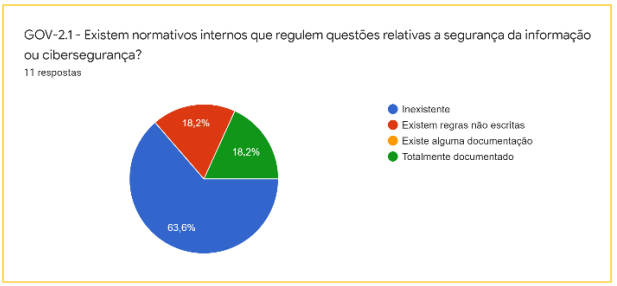


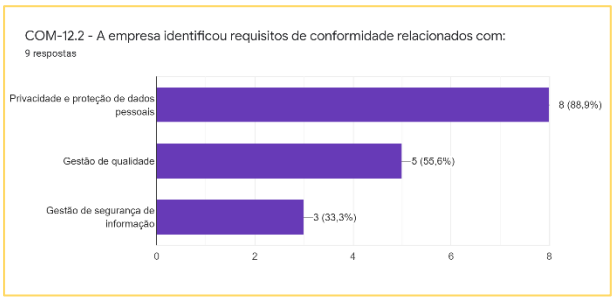
2.1.2 ID.GV – GOVERNAÇÃO

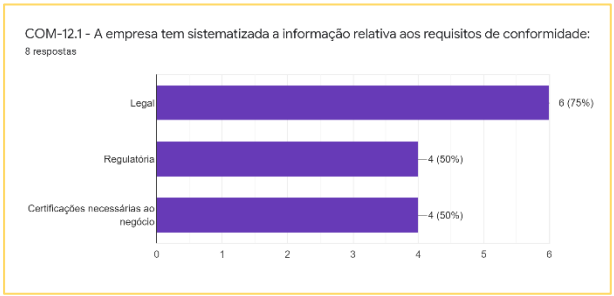
Neste domínio, o QNRCS visa os seguintes objetivos:

"A organização entende as políticas, processos e procedimentos para gerir e monitorizar as responsabilidades regulamentares, legais, de risco, ambientais e operacionais. Estas políticas, processos e procedimentos contribuem para a sensibilização e consolidação do conhecimento por parte dos órgãos de gestão, tendo em vista a identificação dos riscos no contexto da cibersegurança."

Resultados relevantes do inquérito







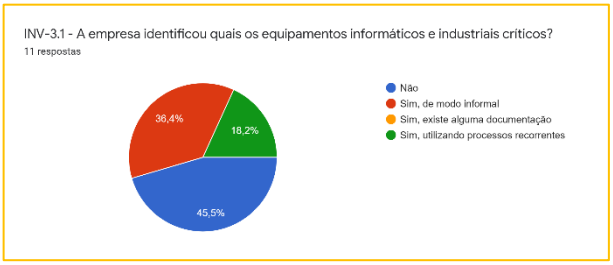
Pontos críticos

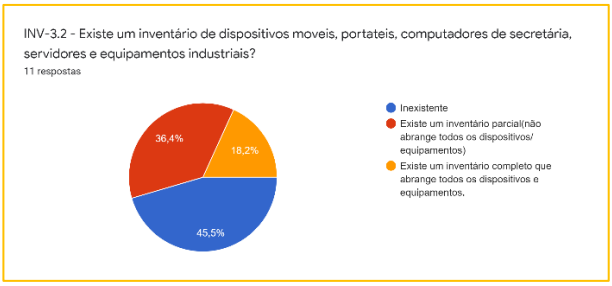
- No geral, as organizações concentram a sua documentação em processos e procedimentos operacionais diretamente relacionados com atividades de negócio. São raras as empresas que dedicam recursos à produção de políticas de cibersegurança ou segurança da informação.
- A governação de IT, e também da cibersegurança, são usualmente entregues a empresas externas, cujas atividades nem sempre são totalmente ou adequadamente monitorizadas pela organização.

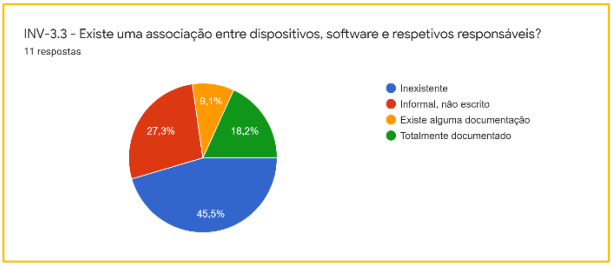
2.1.3 ID.AR - Avaliação de Risco

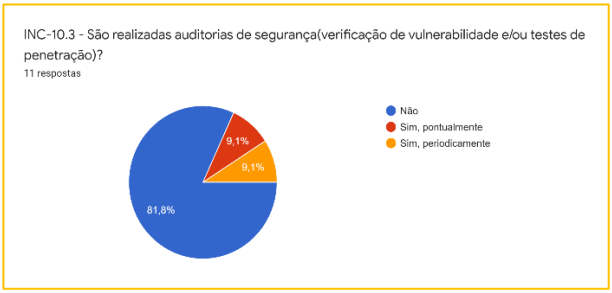
Neste domínio, o QNRCS visa os seguintes objetivos:
"A organização tem noção dos riscos de cibersegurança no âmbito da sua atividade (incluindo missão, funções, imagem ou reputação), ativos organizacionais e pessoas."

Resultados relevantes do inquérito









Pontos críticos

- Não existe uma correta caracterização do risco de cibersegurança, relacionado com os equipamentos industriais. Em boa parte, isto está relacionado com as deficiências na inventariação de gestão de ativos, que também não é adequadamente abrangente relativamente à componente industrial.
- Não são usualmente contempladas práticas de auditorias regulares à cibersegurança interna da organização.

2.1.4 ID.GR - Estratégia de gestão de risco

Neste domínio, o QNRCS visa os seguintes objetivos:

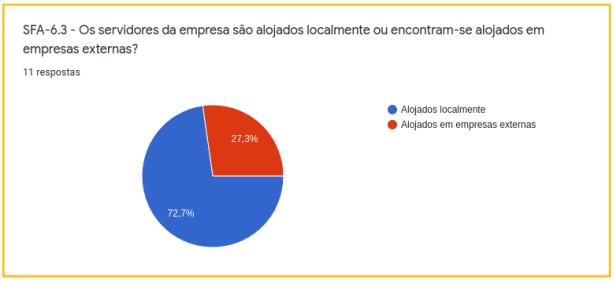
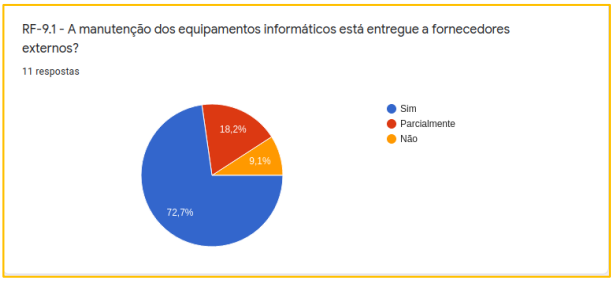
"Devem ser estabelecidas as prioridades, restrições, níveis de tolerância ao risco e assunções que são utilizadas para suportar a tomada de decisão, no âmbito da gestão do risco operacional."

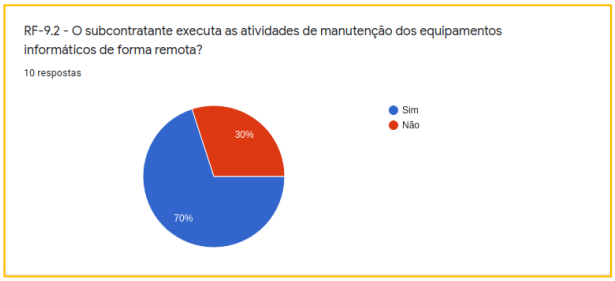
Resultados relevantes do inquérito	*Pontos críticos*
	• As empresas que efetuam gestão de risco como parte integrante dos seus processos de negócio, tipicamente não o fazem com algum enfoque na segurança de informação ou cibersegurança.

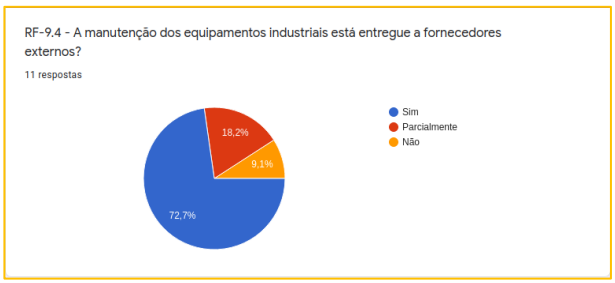
2.1.5 ID.GL - Gestão do risco da cadeia logística

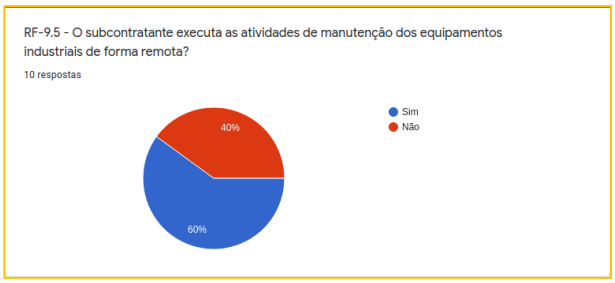
Neste domínio, o QNRCS visa os seguintes objetivos:

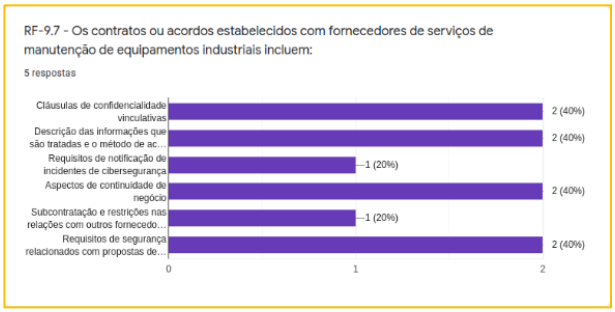
"Devem ser estabelecidas as prioridades, restrições, níveis de tolerância ao risco e assunções que são utilizadas para suportar a tomada de decisão, no âmbito da gestão do risco operacional da cadeia logística. A organização deve estabelecer e implementar os processos para identificar, avaliar e gerir os riscos inerentes à cadeia logística. "

Resultados relevantes do inquérito	*Pontos críticos*
  	• Existe um elevado nível de dependência destas empresas relativamente a prestadores de serviços externos, no que toca a manutenção de equipamentos industriais. Essa dependência é expectável, tendo em conta que se tratam de equipamentos com requisitos que envolvem tipicamente intervenções por parte do fabricante para proceder a reparações ou atualizações de firmware. • Acumulando com essa dependência, verifica-se que grande partes das ações de manutenção efetuadas por prestadores externos ocorrem remotamente, o que é um desafio do ponto de vista do controlo de acessos. • Existem lacunas apreciáveis no que toca à foralização de requisitos de segurança na relação contratual com prestadores de serviços de manutenção externos.





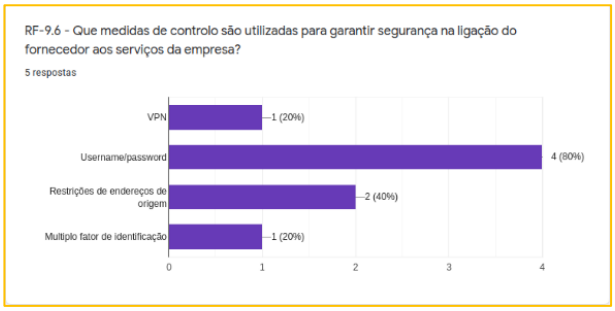




Designadamente, detetam-se tipicamente ausências de:

- Cláusulas de confidencialidades
- Restrições non acesso de subcontratantes à informação da empresa
- Aspetos de continuidade de negócio
- Requisitos de notificação de incidentes
- Restrições específicas de segurança na subcontratação

- Tendo em conta que a modalidade de acesso remoto é maioritariamente utilizada por terceiros em tarefas de manutenção, notam-se carências em controlos de segurança dos acessos remotos, designadamente na utilização de VPN ou MFA.

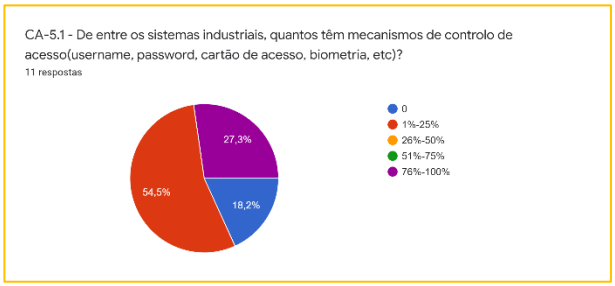


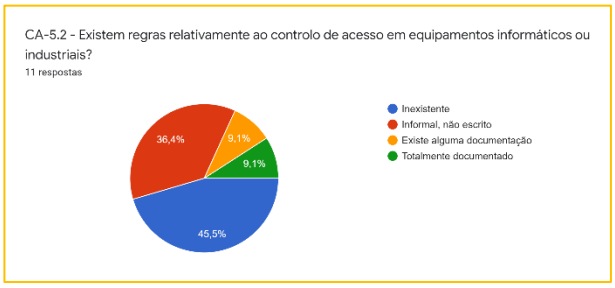
2.2 PROTEGER

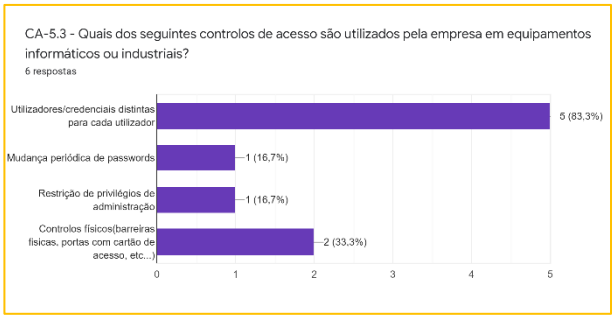
2.2.1 PR.GA – Gestão de identidades, autenticação e controlo de acessos

Neste domínio, o QNRCS visa os seguintes objetivos:
"Os acessos aos ativos físicos, lógicos e às instalações associadas, devem ser limitados às pessoas, processos e equipamentos autorizados. Estes devem ser geridos de acordo com a avaliação do risco de acesso não autorizado."

Resultados relevantes do inquérito

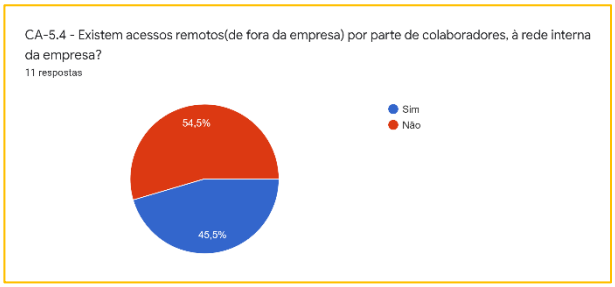


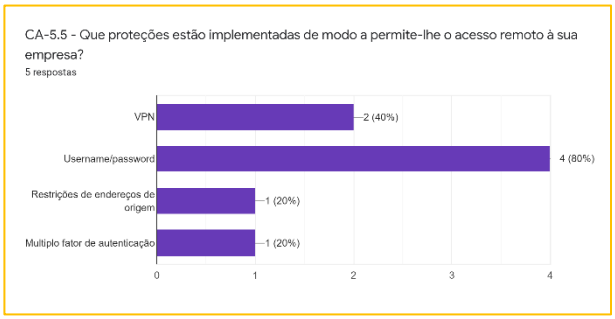


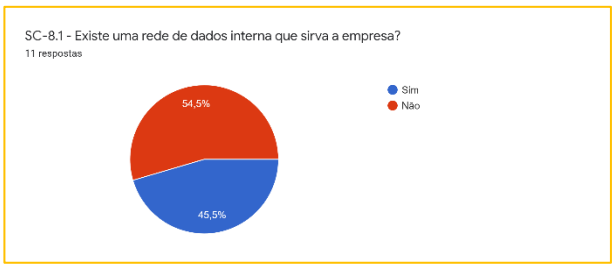


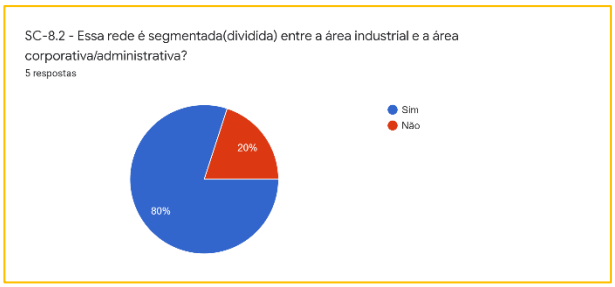
Pontos críticos

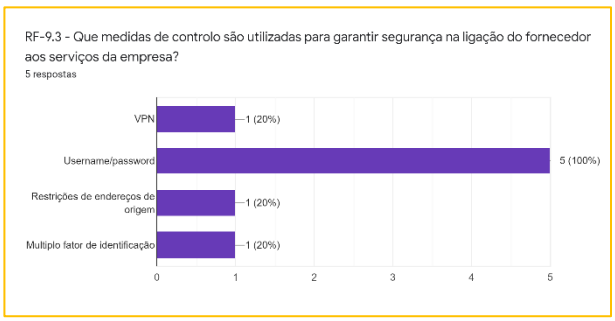
- O controlo de acessos nos equipamentos industriais é tipicamente básico, essencialmente limitando-se ao nível de username/password que nunca ou raramente são modificados.
- A falta de formalização (passagem a escrito) de regras ou requisitos no controlo de acessos é bastante frequente.
- Existe uma porção significativa de acessos que são efetuados remotamente pelos colaboradoes aos recursos informáticos das organizações. Isso torna preocupante o baixo nível de controlos de segurança aplicados tipicamente aos acessos remotos.
- Também nos acessos locais existe carência de controlo de acessos, no que toca a mudança de passwords, restrição de privilégios de administração e controlos físicos.



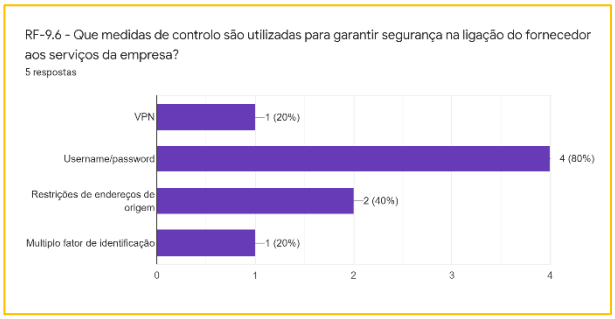






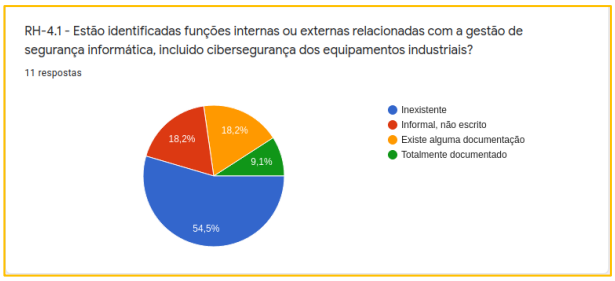
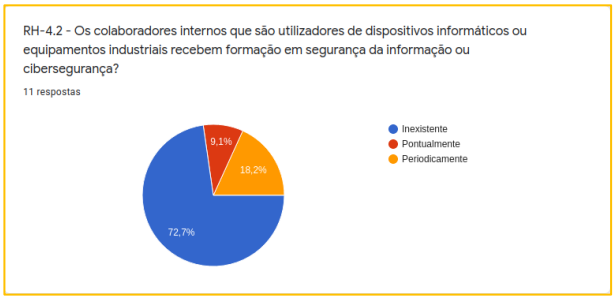


- Como referido anteriormente, as medidas de controlo de acessos remotos de fornecedores apresentam lacunas apreciáveis.



2.2.2 PR.FC – Formação e sensibilização

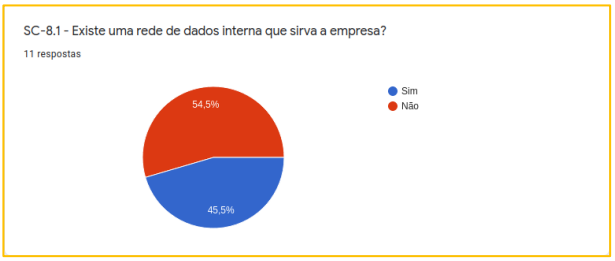
Neste domínio, o QNRCS visa os seguintes objetivos:
"Devem ser ministradas sessões de sensibilização em cibersegurança a colaboradores e fornecedores. Estes, devem ser formados para cumprirem as suas responsabilidades e os seus deveres relacionados com a cibersegurança, em concordância com as políticas, processos, procedimentos e acordos relevantes."

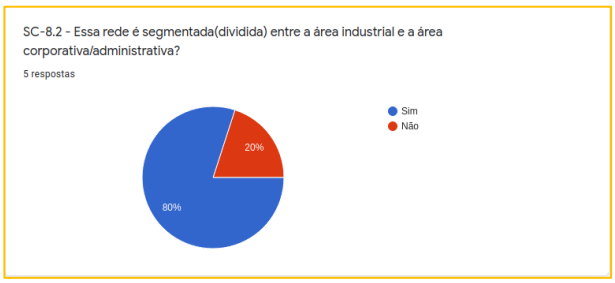
Resultados relevantes do inquérito	***Pontos críticos***
 	• Tipicamente não estão identificadas funções relacionadas com gestão de segurança de informação ou cibersegurança. • Existem óbvias carências de sensibilização e formação dos colaboradores das empresas para questões de cibersegurança.

2.2.3 PR.SD – Segurança de dados

Neste domínio, o QNRCS visa os seguintes objetivos:
"As informações e os dados devem ser geridos de acordo com a estratégia de gestão do risco organizacional, por forma a proteger a confidencialidade, integridade e disponibilidade da informação."

Resultados relevantes do inquérito	*Pontos críticos*



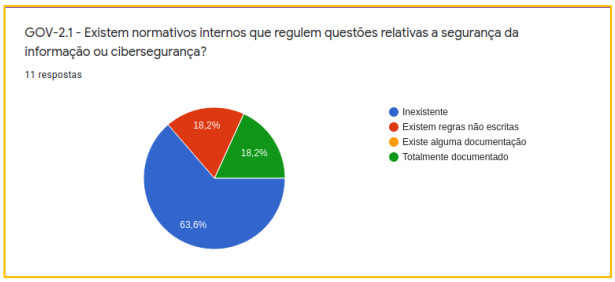


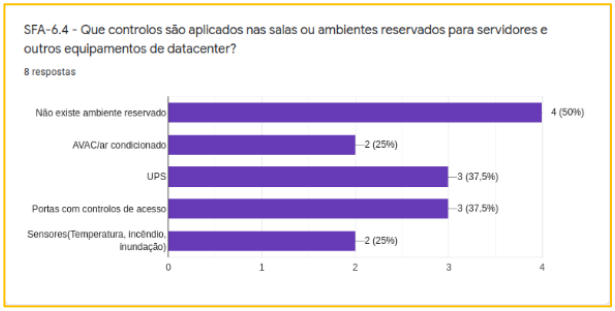
- O foco das empresas resume-se à continuidade das operações, e não existe um foco na confidencialidade dos dados. É extremamente raro haver cuidados relativamente à segurança da informação em trânsito ou em repouso.

2.2.4 PR.PI – Procedimentos e processos de proteção da informação

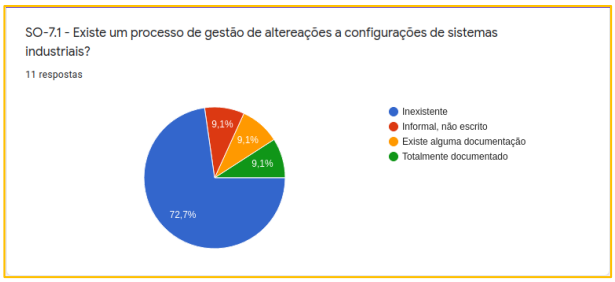
Neste domínio, o QNRCS visa os seguintes objetivos:
"As políticas de segurança, processos e procedimentos devem ser mantidas e utilizadas por forma a permitir gerir a proteção das redes e sistemas de informação."

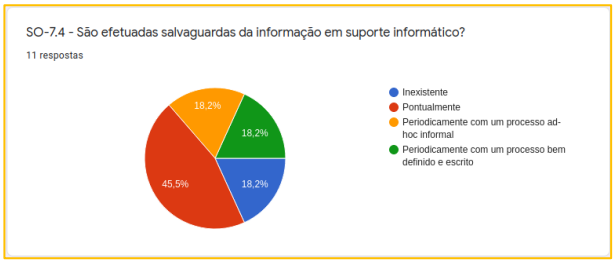
Resultados relevantes do inquérito	*Pontos críticos*

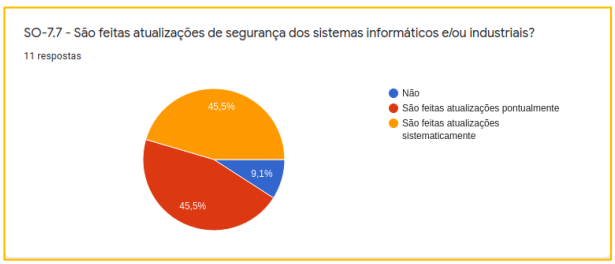


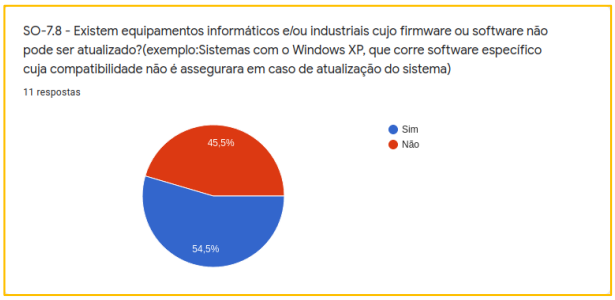


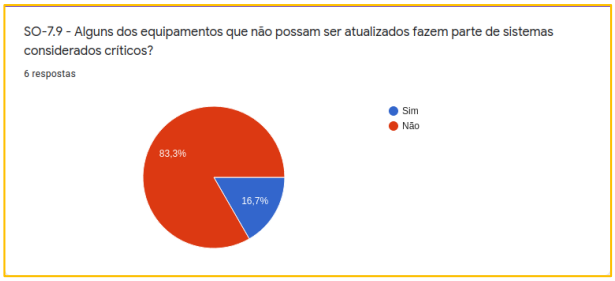
- Existe muito pouca sistematização (processos documentados) relativamente à manutenção de processos de proteção, como backups. Tipicamente, estes processos são pontuais com baixo grau de automação ou controlo de qualidade.
- Os processos de gestão de alterações são inexistentes ou não documentados.
- A atualização de sistemas informáticos é também um problema premente em duas frentes:





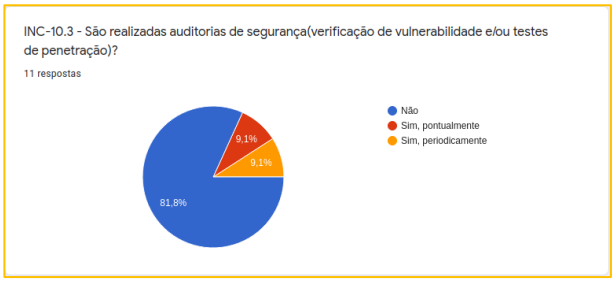


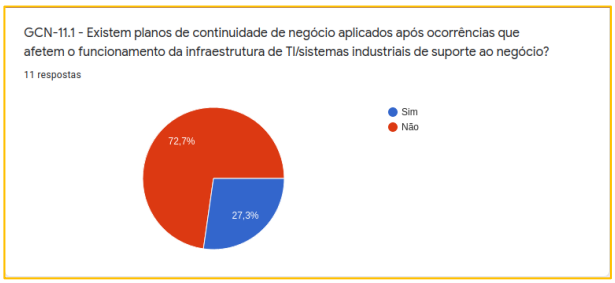


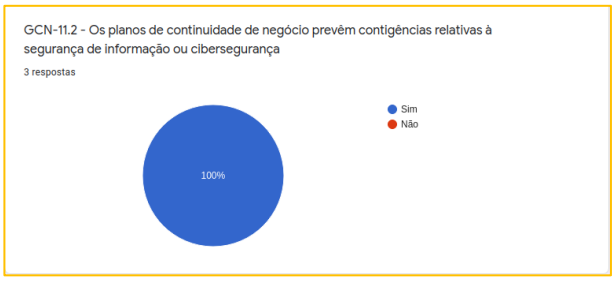


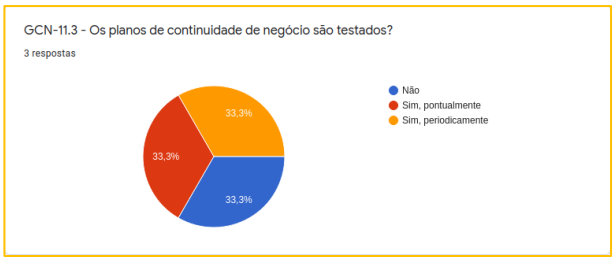
- Os serviços informáticos de suporte são tipicamente atualizados sem recursos a automação ou sistematização;
- Existe uma componente de *legacy* apreciável relacionada com os equipamentos industriais, que tornam determinados sistemas "não atualizáveis", por forma a manter a conformidade com as funcionalidades previstas pelo fabricante.

- A falta de auditorias ou testes de penetração (principalmente tendo em conta a componente *legacy*) é também preocupante, limitando a visibilidade da organização sobre a exposição a vulnerabilidades e exploits que levarão a problemas de segurança.
- Dada esta propensão para a "estanquicidade" dos sistemas de controlo industriais, é previsível a ocorrência de credenciais por *default*. Em várias situações, estas credenciais nem podem ser modificadas, por fazerem parte de *scripts* ou programas *hardcoded* com essa informação.
- A gestão de credenciais, tal como no restante do controlo de acessos, necessita de melhorias. Não existem requisitos sobre complexidade ou proazos de modificação de *passwords*.





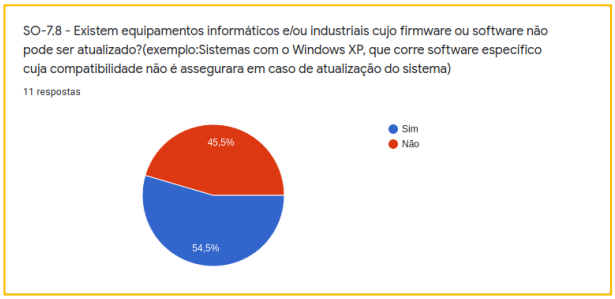


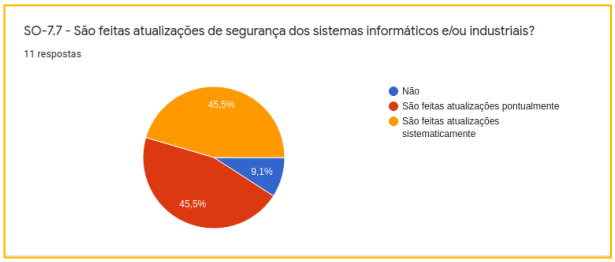


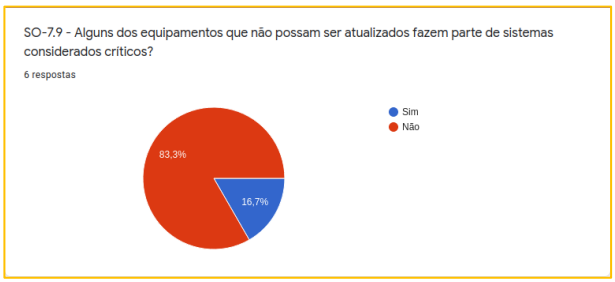
2.2.5 PR.MA – Manutenção

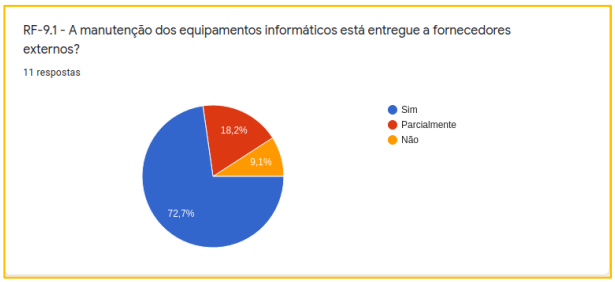
Neste domínio, o QNRCS visa os seguintes objetivos:
"A manutenção e reparação das redes e sistemas de informação deve ser realizada em concordância com as políticas, processos e procedimentos instituídos."

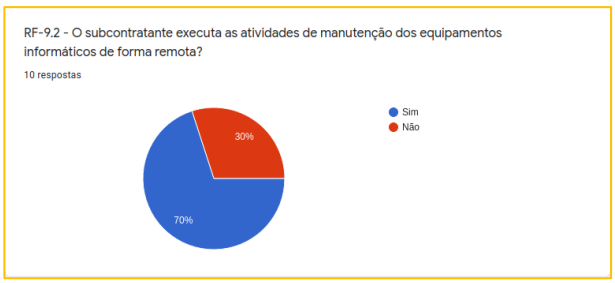
Resultados relevantes do inquérito	***Pontos críticos***



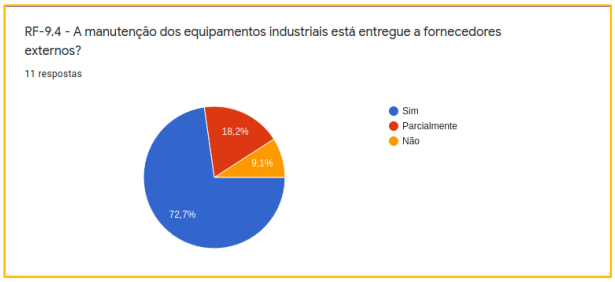


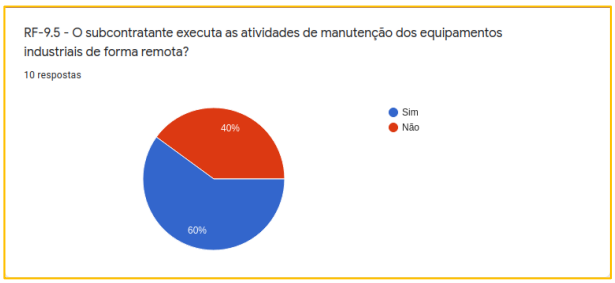


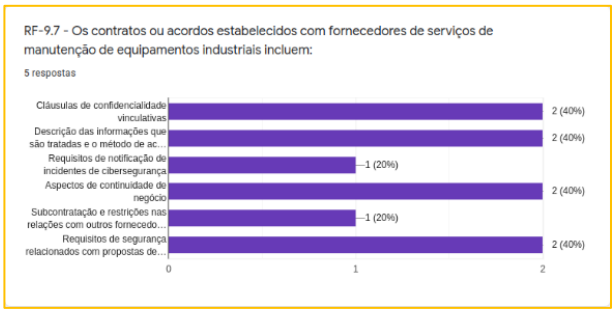


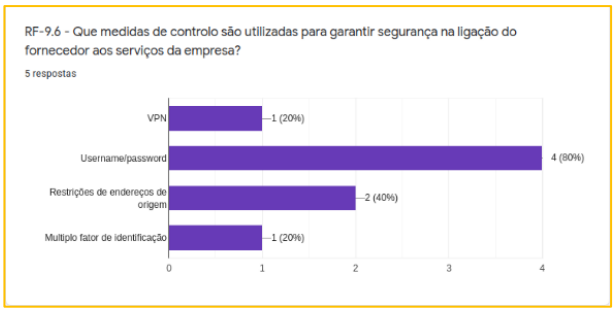


- Neste domínio, reiteram-se as consideração relativamente referidas relativamente a:
    - Dependência de fornecedores externos
    - Frequência de recursos ao acesso em modo remoto
    - Lacunas de controlos de segurança no acesso remoto
    - Lacunas de formalização contratual dos requisitos de segurança aplicáveis às tarefas de manutenção





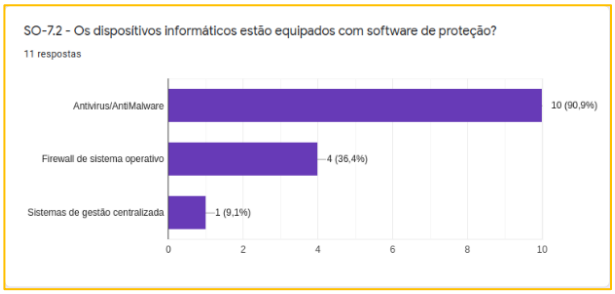


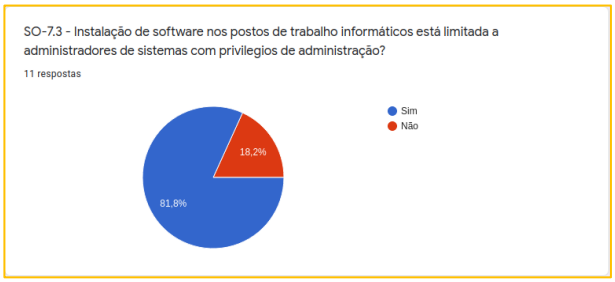


2.2.6 PR.TP – Tecnologia de proteção

Neste domínio, o QNRCS visa os seguintes objetivos:
"As soluções técnicas de segurança devem ser geridas por forma a garantir a confidencialidade, integridade e disponibilidade das redes e sistemas de informação, em concordância com as políticas relacionadas, processos, procedimentos e acordos relevantes."

Resultados relevantes do inquérito	***Pontos críticos***





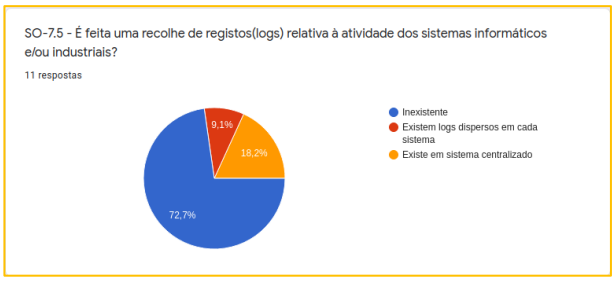
- A tecnologia de proteção está tipicamente limitada ao mínimo, o que significa apenas anti-vírus individuais, sem gestão centralizada.

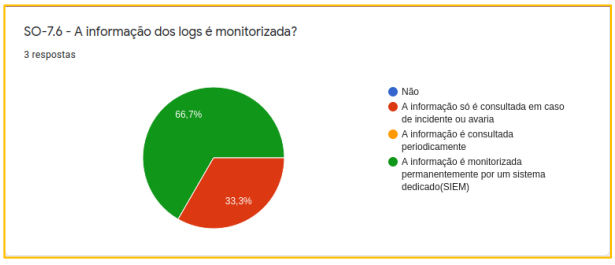
2.3 DETETAR

2.3.1 DE.AE – Anomalias e eventos

Neste domínio, o QNRCS visa os seguintes objetivos:
"Devem ser detetadas as atividades anómalas em tempo útil, bem como deve ser assegurada a compreensão do impacto potencial dos eventos."

Resultados relevantes do inquérito	***Pontos críticos***



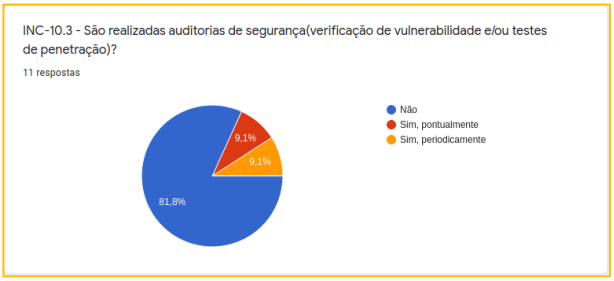


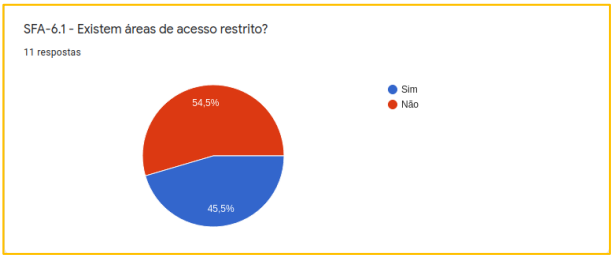
- A informação de *logging* é, no geral, inexistente, insuficiente ou armazenada por períodos de tempo que não são controlados.

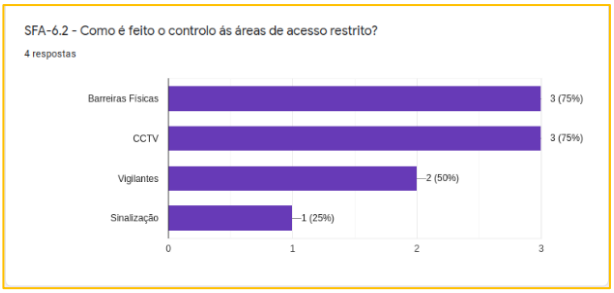
2.3.2 DE.MC – Monitorização Contínua de Segurança

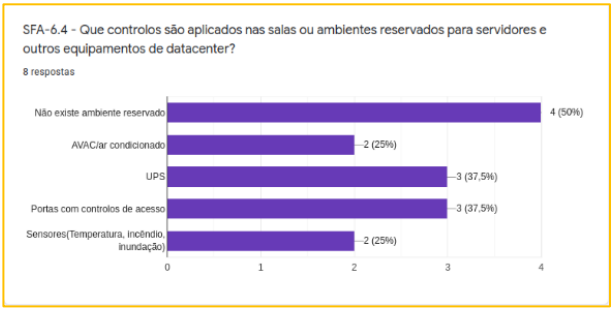
Neste domínio, o QNRCS visa os seguintes objetivos:
"As redes e sistemas de informação devem ser monitorizadas para identificação de eventos de cibersegurança e verificação da eficácia das medidas de proteção aplicadas."

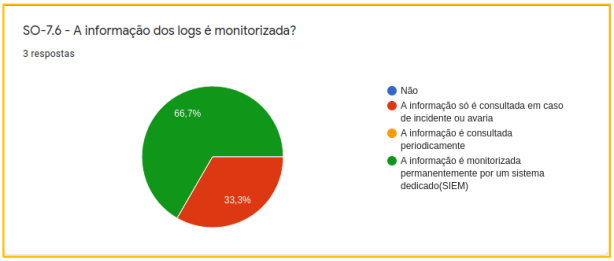
Resultados relevantes do inquérito











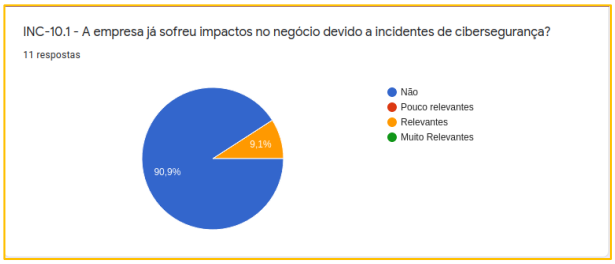
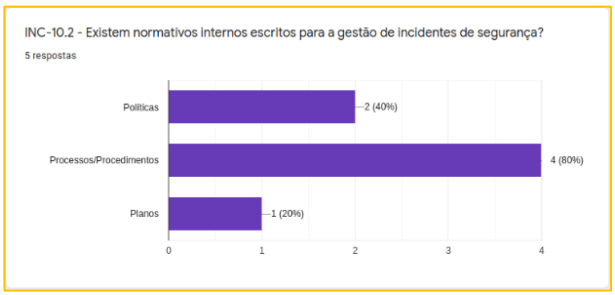
Pontos críticos

- É invulgar encontrar empresas do setor que dediquem recursos a monitorização de cibersegurança. Quando essa função existe, normalmente é sub-contratada e não em regime contínuo. Na realidade, poucas empresas têm uma infraestrutura de IT que o justifique.
- A falta de informação de registos de auditoria (*logging*) é um componente essencial que deixa muito espaço de melhoria no domínio da monitorização.

2.4 RESPONDER

2.4.1 RS.PR – Planeamento de resposta

Neste domínio, o QNRCS visa os seguintes objetivos:
"Os processos de resposta e respetivos procedimentos devem ser executados e mantidos para garantir resposta aos incidentes detetados."

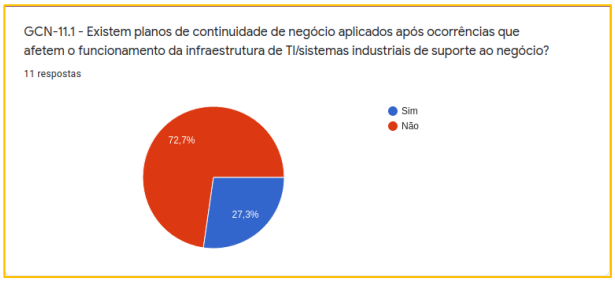
Resultados relevantes do inquérito	***Pontos críticos***
 	• Apesar de existirem normativos relativos à gestão de incidentes, é dúbio se esta documentação cobrirá adequadamente incidentes de cibersegurança. Isto poderá, em parte pelo menos, estar relacionado com a perceção generalizada dos inquiridos de que não existe um histórico de impacto relacionado com tais incidentes.

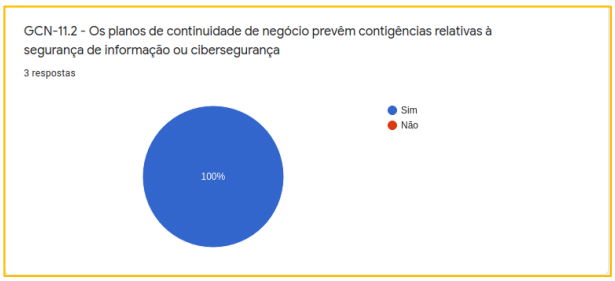
2.5 RECUPERAR

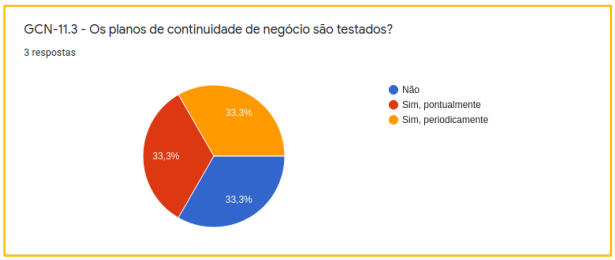
2.5.1 RC.PR – Plano de recuperação

Neste domínio, o QNRCS visa os seguintes objetivos:
"Os processos e procedimentos de recuperação devem ser executados e mantidos para garantir a recuperação das redes e sistemas de informação afetados pelos incidentes."

Resultados relevantes do inquérito	***Pontos críticos***







- Como dito anteriormente, não parece haver uma devida automação e sistematização dos processos de salvaguarda e restauro, com adequado controlo de qualidade.
- Os planos de continuidade de negócio não abrangem adequadamente a componente de segurança de informação, mas apenas as estritas necessidades operacionais.
- Os planos de continuidade de negócio e recuperação de desastre necessitam de processos de revisão periódicos e de testes específicos.

3 PRINCIPAIS CONCLUSÕES

Do estudo realizado, embora com uma amostra reduzida, foi possível tirar as seguintes conclusões principais:

1. A generalidade das empresas participantes neste projeto enquadra-se na definição de PME, pelo que existem poucos recursos humanos e técnicos associados à componente de segurança. É também relevante considerar, a este respeito, que muitas das empresas inquiridas parece não contar com infraestruturas de IT ou OT que justifiquem cuidados a este nível, que seriam sem dúvida enquadráveis em empresas de maior complexidade ou dimensão. Ressalva-se que, no âmbito do estudo, participou uma empresa de maior dimensão em que o cenário analisado foi bastante díspar relativamente às suas congéneres, com bons níveis de maturidade observados na generalidade dos indicadores de segurança contemplados.
2. Os cuidados com a segurança, no âmbito das empresas da amostra analisada, concentram-se em segurança operacional, com relevância para o respeito por normas de higiene, salubridade, preservação ambiental, e outras considerações normativas ou regulamentares diretamente aplicáveis aos respetivos setores. A cibersegurança não está na lista de principais preocupações da generalidade destas organizações.

3. É fácil de constatar um baixo grau de consciencialização por parte dos responsáveis das empresas em âmbito deste estudo relativamente a aspetos de cibersegurança. Essencialmente, o desconhecimento parece dever-se à perceção generalizada de que é uma matéria com pouca relevância no contexto das respetivas operações, sendo que, em muitos casos, isso se justificará pela ausência de dispositivos ou infraestruturas que, de alguma forma, estejam ligadas à Internet, ou sequer em rede local.
4. Ainda no domínio da consciencialização, nota-se um défice na perceção dos inquiridos no que respeita à necessidade de manter certos níveis de segurança e privacidade em dados que poderão não estar diretamente ligados ao negócio (e.g. sistemas de email, documentação de recursos humanos). Esta é uma justificação típica para o relaxamento de medidas de segurança protetivas em torno dos dispositivos de IT que processam esses tipos de informação.
5. Os conceitos de "gestão de ativos" e "gestão de risco" estão, tipicamente, ligados unicamente a simples inventários e considerações de risco operacional. Esta é uma carência fundamental, na medida em que a implantação de uma cultura de cibersegurança nas organizações deve assentar no aspeto central, que é a metodologia de gestão de risco – incluindo o risco de segurança de informação – como base estratégica para a tomada de decisões.
6. Foram observadas sérias carências no capítulo de governação da segurança, especificamente no que toca a sistematização e formalização de normativos internos. Não se encontram muito exemplos de políticas, processos e procedimentos adequadamente estabelecidos e aprovados que regulem nem que seja aspetos básicos de utilização aceitável de recursos informáticos.
7. A dependência de fornecedores externos é uma constante no que toca à manutenção de determinados equipamentos, com destaque para os de índole industrial, o que é compreensível dados os requisitos necessários às operações envolvidas, tipicamente restritas a fabricantes. É também relevante referir que, para a típica PME, uma solução de serviço subcontratado, inclusive no capítulo da segurança (e.g. *Managed Security Services*), será quase sempre mais eficaz a nível custos do que uma solução totalmente internalizada, se não falamos de funções nucleares do negócio. No entanto, é importante considerar que isto leva ao surgimento de vulnerabilidades na gestão da cadeia logística, se não forem devidamente monitorizados e controlados os acessos remotos ou locais desses fornecedores aos recursos tecnológicos da organização. Designadamente, podem surgir portas de entrada pouco vigiadas ou protegidas para ameaças externas, sendo que também não é de excluir a possibilidade de ameaça interna (do próprio

fornecedor), se não forem acionadas salvaguardas contratuais e técnicas que mitiguem esses riscos.

8. Existe um risco tipicamente ligado a sistemas industriais, que são usualmente desenhados para serem estanques. Essa caraterística "monolítica" costuma implicar sérias restrições à atualização dos sistemas informáticos de suporte, pelo perigo de provocar incompatibilidades que interfiram com a funcionalidade. Tais casos foram observados na amostra de empresas em âmbito deste estudo. Temos, por isso, a certo prazo no ciclo de vida destas soluções, risco de um *legacy* de *hardware* e *software* que, em virtude de não ser passível de atualizações de segurança regulares, deve ser objeto de análise de risco e consequente mitigação, através de camadas adicionais de segurança.
9. Constatam-se debilidades na capacidade da generalidade das organizações em âmbito de fazerem face a incidentes de segurança, com ênfase para incidentes de proporção que possam afetar a continuidade de negócio. É importante incutir na cultura destas empresas que existem, até a nível legal (e.g. RGPD, Diretiva NIS, etc.), requisitos de resposta a *data breaches* que pressupõem meios adequados, no que toca a *logging*, monitorização, gestão de incidentes e gestão de vulnerabilidades. Estas capacidades devem ser reforçadas no setor, sempre tendo em conta a relação custo/benefício aferida em sede de análise de risco. Também devem ser reforçadas as capacidades e processos que suportam *disaster recovery*, designadamente no que toca a *backup* e *recovery*.

ANEXO A – QUESTIONÁRIO

A tabela seguinte apresenta as questões que fizeram parte do questionário online disponibilizado as entidades.

Ref. Categoria QNRCS	ID questão	Questões	Respostas possiveis				
	CE-1	**Caraterização da empresa**					
	CE-1.1	Designação da empresa	TEXTO LIVRE				
	CE-1.2	Setor de atividade	CARNEO	HORTOFRUTICOLAS	LÁCTEOS	PADARIA/ PASTELARIA	
	CE-1.3	Numero de trabalhadores	[0-10]	[11-50]	[51-100]	mais de 100	
	CE-1.4	Percentagem trabalhadores na área fabril/industrial	[0-25]	[26-50]	[51-75]	[76-100]	
	CE-1.5	Número de computadores para utilização individual (portateis/computadores de secretária)?	0	[1-10]	[11-50]	[51-100]	mais de 100
	CE-1.6	Número de servidores (fisico ou/e virtuais)	0	[1-5]	[6-20]	mais de 20	
	CE-1.7	Quantos sistemas industriais distintos têm uma consola/ecrã de controlo informatizada ou têm ligação a sistemas informáticos?	0	[1-5]	[6-10]	[11-20]	mais de 20
	CE-1.8	Quantos sistemas de monitorização, sensores, alarmistica têm uma consola/ecrã de controlo informatizada ou têm ligação a sistemas informáticos?	0	[1-5]	[6-10]	[11-20]	mais de 20
	CE-1.09	Tem equipa de IT interna?	Sim	Não			
	CE-1.10	Quantos elementos tem a sua equipa de IT	TEXTO LIVRE				
	GOV-2	**Governação**					
ID.GV, PR.PI	GOV-2.1	Existem normativos internos que regulem questões relativas a segurança da informação ou cibersegurança?	Inexistentes	Existem regras não escritas	Existe alguma documentação	Totalmente documentado	
	INV-3	**Gestão de risco**					
ID.GA, ID.AR	INV-3.1	A empresa identificou quais os equipamentos informáticos e industriais críticos?	Não	Sim, de modo informal	Sim, existe alguma documentação	Sim, utilizando processos recorrentes	
ID.GA, ID.AR	INV-3.2	Existe um inventário de dispositivos moveis, portáteis, computadores de secretária, servidores e equipamentos industriais?	Inexistente	Existe um inventario parcial (não abrange todos os dispositivos/equipamentos)	Existe um inventário completo que abrange todos os dispositivos e equipamentos.		
ID.GA, ID.AR	INV-3.3	Existe uma associação entre dispositivos, software e respetivos responsáveis?	Inexistente	Informal, não escrito	Existe alguma documentação	Totalmente documentado	
ID.GR, ID.GL	INV-3.4	A empresa efetua uma gestão de riscos relacionados com a cibersegurança?	Não	Sim, com uma metodologia própria	Sim, com uma metodologia reconhecida		
	RH-4	**Recursos humanos**					
PR.FC	RH-4.1	Estão identificadas funções internas ou externas relacionadas com a gestão de segurança informática, incluindo cibersegurança dos equipamentos industriais?	Inexistente	Informal, não escrito	Existe alguma documentação	Totalmente documentado	
PR.FC	RH-4.2	Os colaboradores internos que são utilizadores de dispositivos informaticos ou equipamentos industriais recebem formação em segurança da informação ou cibersegurança?	Inexistente	Pontualmente	Periodicamente		
	CA-5	**Controlo de acessos**					
PR.GA	CA-5.1	De entre os sistemas industriais, quantos têm mecanismos de controlo de acesso (username, password, cartão de acesso, biometria, etc)?	0	[1%-25%]	[26%-50%]	[51%-75%]	[76%-100%]
PR.GA	CA-5.2	Existem regras relativamente ao controlo de acesso em equipamentos informáticos ou industriais?	Inexistente	Informal, não escrito	Existe alguma documentação	Totalmente documentado	
PR.GA	CA-5.3	Quais dos seguintes controlos de acesso são utilizados pela empresa em equipamentos informáticos ou industriais? (escolha multipla)	Utilizadores/Credenciais distintas para cada utilizador	Mudança periódica de passwords	Restrição de privilégios de administração	Controlos físicos (barreiras fisicas, portas com cartão de acesso, etc..)	
PR.GA	CA-5.4	Existem acessos remotos (de fora da empresa) por parte de colaboradores, à rede interna da empresa?	Sim	Não			
PR.GA	CA-5.5	Que proteções estão implementadas de modo a permite-lhe o acesso remoto à sua empresa? (escolha multípla)	VPN	Username/ password	Restrição de endereços de origem	Multiplo fator de autenticação	Outros
	SFA-6	**Perímetro de segurança física**					
DE.MC	SFA-6.1	Existem áreas de acesso restrito?	Sim	Não			
DE.MC	SFA-6.2	Como é feito o controlo ás áreas de acesso restrito?	Barreiras fisicas	CCTV	Vigilantes	Sinalização	Outros
ID.GL	SFA-6.3	Os servidores da empresa são alojados localmente ou encontram-se alojados em empresas externas?	Alojados localmente	Alojados em empresas			
DE.MC, PR.PI	SFA-6.4	Que controlos são aplicados nas salas ou ambientes reservados para servidores e outros equipamentos de datacenter? (escolha multipla)	Não existe ambiente reservado	AVAC/ Ar condicionado	UPS	Portas com controlo de acesso	Sensores (Temperatura, incendio, inundação)

	SO-7	**Segurança de operações**				
PR.PI	SO-7.1	Existe um processo de gestão de alterações a configurações de sistemas industriais?	Inexistente	Informal, não escrito	Existe alguma documentação	Totalmente documentado
PR.TP	SO-7.2	Os dispositivos informaticos estão equipados com software de proteção? (escolha multipla)	Antivirus/AntiMalware	Firewall de sistema operativo	Outros	
PR.TP	SO-7.3	Instalação de software nos postos de trabalho informáticos está limitada a administradores de sistemas com privilégios de administração?	Sim	Não		
PR.PI	SO-7.4	São efetuadas salvaguardas da informação em suporte informático?	Inexistente	Pontualmente	Periodicamente com processo ad-hoc informal	Periodicamente com processo bem definido e escrito.
DE.AE	SO-7.5	É feita uma recolha de registos (logs) relativa à atividade dos sistemas informáticos e/ou industriais?	Inexistente	Existem logs dispersos em cada sistema	Existem em sistema centralizado	
DE.AE, DE.MC	SO-7.6	A informação dos logs é monitorizada?	Não	A informação só é consultada em caso de incidente ou avaria	A informação é consultada periodicamente	A informação é monitorizada permanentemente por um sistema dedicado (SIEM)
PR.MA, PR.PI	SO-7.7	São feitas atualizações de segurança aos sistemas informaticos e/ou industriais?	Não	São feitas atualizações pontualmente	São feitas atualizações sistematicamente	
PR.MA, PR.PI	SO-7.8	Existem equipamentos informáticos e/ou industriais cujo firmware ou software não pode ser atualizado? (Exemplo: sistemas com Windows XP, que corre software específico cuja compatibilidade não é assegurada em caso de atualização de sistema)	Sim	Não		
PR.MA, PR.PI	SO-7.9	Alguns dos equipamentos que não possam ser atualizados fazem parte de sistemas considerados críticos?	Sim	Não		
	SC-8	**Segurança das comunicaçoes**				
PR.SD, PR.GA	SC-8.1	Existe uma rede de dados interna que sirva a empresa?	Sim	Não		
PR.SD, PR.GA	SC-8.2	Essa rede é segmentada (dividida) entre área industrial e área corporativa/administrativa?	Sim	Não		
	RF-9	**Relações com fornecedores**				
PR.MA, ID.GL	RF-9.1	A manutenção dos equipamentos informáticos está entregue a fornecedores externos?	Sim	Parcialmente	Não	
PR.MA, ID.GL	RF-9.2	O subcontratante executa as atividades de manutenção dos equipamentos informáticos de forma remota?	Sim	Não		
PR.MA, ID.GL	RF-9.7	Os contratos ou acordos estabelecidos com fornecedores de serviços de manutenção de equipamentos informáticos incluem:	Cláusulas de confidencialidade vinculativas	Descrição das informações que são tratadas e o método de aceder essas informações	Requisitos de notificação de incidentes de cibersegurança	Aspectos de continuidade de negócios	Subcontratação e restrições nas relações com outros fornecedores
PR.MA, ID.GL, PR.GA	RF-9.3	Que medidas de controlo são utilizadas para garantir segurança na ligação do fornecedor aos dispositivos da empresa?	VPN	Username/ password	Restrição de endereços de origem	Multiplo fator de autenticação	
PR.MA, ID.GL	RF-9.4	A manutenção dos equipamentos industriais está entregue a fornecedores externos?	Sim	Não			
PR.MA, ID.GL	RF-9.5	O subcontratante executa as atividades de manutenção dos equipamentos industriais de forma remota?	Sim	Não			
PR.MA, ID.GL	RF-9.7	Os contratos ou acordos estabelecidos com fornecedores de serviços de manutenção de equipamentos industriais incluem:	Cláusulas de confidencialidade vinculativas	Descrição das informações que são tratadas e o método de aceder essas informações	Requisitos de notificação de incidentes de cibersegurança	Aspectos de continuidade de negócios	Subcontratação e restrições nas relações com outros fornecedores
PR.MA, ID.GL, PR.GA	RF-9.6	Que medidas de controlo são utilizadas para garantir segurança na ligação do fornecedor aos dispositivos da empresa?	VPN	Username/ password	Restrição de endereços de origem	Multiplo fator de autenticação	
	INC-10	**Gestão de incidentes de segurança da informação e vulnerabilidades**				
RS.PR	INC-10.1	A empresa já sofreu impactos no negócio devido a incidentes de cibersegurança?	Não	Pouco relevantes	Relevantes	Muito relevantes
RS.PR	INC-10.2	Existem normativos internos escritos para gestão de incidentes de segurança? (escolha multipla)	Políticas	Processos/ procedimentos	Planos	
ID.AR, PR.PI, DE.MC	INC-10.3	São realizadas auditorias de segurança (verificação de vulnerabilidades e/ou testes de penetração)?	Não	Sim, pontualmente	Sim, periodicamente	
	GCN-11	**Gestão da continuidade do negócio**				
RC.PR, PR.PI	GCN-11.1	Existem planos de continuidade de negócios aplicados após ocorrências que afetem o funcionamento da infraestrutura de TI/Sistemas industrias de suporte ao negócio?	Não	Sim		
RC.PR, PR.PI	GCN-11.2	Os planos de continuidade de negócio prevêm contigências relativas à segurança de informação ou cibersegurança?	Não	Sim		
RC.PR, PR.PI	GCN-11.3	Os planos de continuidade de negócio são testados?	Não	Sim, pontualmente	Sim, periodicamente	
	COM-12	**Conformidade**				
ID.GV	COM-12.1	A empresa tem sistematizada a informação relativa aos requisitos de conformidade: (escolha multipla)	Legal	Regulatória	Certificações necessárias ao negócio	
ID.GV	COM-12.2	A empresa identificou requisitos de conformidade relacionados com: (escolha multipla)	Privacidade e proteção de dados pessoais	Gestão da qualidade	Gestão da segurança da informação	