Indústria 4.0
CIBERSEGURANÇA

gmv
INNOVATING SOLUTIONS

QUEM SOMOS

UM GRUPO TECNOLÓGICO GLOBAL

Grupo multinacional tecnológico

Há cerca de 20 anos em Portugal

Mais de 2100 empregados

Aeronáutica, Espaço, Defesa e Segurança, Cibersegurança, Saúde, Sistemas Inteligentes de Transporte , Banca e Finanças, Tecnologias da Informação e Comunicação

Capital privado

Escritórios em 10 países

Origem vinculada ao sectores do Espaço e da Defesa

Engenharia, desenvolvimento e integração de sistemas, software, hardware, serviços e produtos especializados

Fundado em

1984

COMPROMISSO COM A QUALIDADE

Existe um compromisso contínuo com os clientes, a **excelência**, a **inovação** e a melhoria contínua dos processos de gestão da **qualidade**.

As diferentes empresas do grupo **GMV** possuem **certificações** de qualidade ajustadas às suas áreas de atividade e especialização.

Aeroespacial e Defesa

CMMI Level 5
ISO 9001:2008
ISO 9100:2010
AQAP/PECAL 2110
AQAP/PECAL 2210

Segurança e TIC

ISO 27001:2013
ISO 20000:2007
BS 25999:2007
ISO 22301:2012

Ambiental

ISO 14001:2004

Saúde

ISO 13485:2003

Indústria 4.0

O que é?

Ameaças Físicas

CiberAmeaças


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

GMV: O que fazemos?

Ciber-segurança	Consultoria	Inteligência de Negócio	Integração de Sistemas	(I)IoT
Red Team Blue Team Products	Análise, definição e implementação de estratégias e casos de uso de máximo valor agregado	Medição e monitorização de KPIs críticos para os processos de negócio I+D	Integração de dados em sistemas de gestão de processos Definição de novas estratégias de gestão automáticas Engenharia de Software	Integração e desenvolvimento de ativos conectados Computação na Nuvem

Data breaches (1 / 2)

YAHOO!

- Maior *data breach* da história
- 3 biliões de contas de utilizadores afetadas
- Quebrado 2 vezes, em 2013 e em 2014

- 60 gigabytes de dados de empresa de encontros on-line
- Dados tornados públicos: emails, nomes, endereços, números de cartões de crédito, fantasias sexuais

EQUIFAX

- 40% dos americanos tiveram seus dados pessoais expostos
- Quebrado 2 vezes em 2017
- Dados tornados públicos: nomes, datas de nascimento, números de seguridade social, endereços e números de cartão de crédito de 147 milhões de pessoas.

Marriott

- 383 milhões de registros de clientes roubados (nomes, números de cartão de crédito, números de telefone, endereços)
- No final de 2018, 25,5 milhões de números de passaporte comprometidos. 5,25 milhões foram armazenados em texto simples

Data breaches (2 / 2)

- De acordo com o grupo “Guardians of Peace”, 100 terabytes de dados da Sony foram recolhidos
- E-mails embaraçosos e detalhes pessoais sobre estrelas de cinema publicados
- Filmes ainda não lançados publicados em sites de partilha de arquivos
- Salários dos patrões publicados
- De acordo com o FBI, o agressor foi a Coreia do Norte

Leaked in

- Maior violação de 2012, quando 6,5 milhões de senhas criptografadas foram publicadas num site.
- Em 2016, 167 milhões de credenciais do LinkedIn foram colocadas à venda na dark web.

RSA

- 40 milhões de tokens de segurança RSA SecurID comprometidos
- Tokens reemitidos para clientes
- Ataque lançado no cliente da RSA e empreiteiro de defesa dos EUA Lockheed Martin

…e Portugal também!

CRIME

Ataque informático expõe documentos da PLMJ sobre casos mediáticos

Ficheiros internos da sociedade de advogados PLMJ foram acedidos ilicitamente e divulgados num blogue. Entre os processos visados estão os casos *E-Toupeira* e a *Operação Marquês*.

Francisco Correia · 7 de Janeiro de 2019, 20:02

249 PARTILHAS

Hospitais da CUF sofrem ataque informático com Ransomware SamSam

04 AGO 2018 · NOTÍCIAS 61 COMENTÁRIOS

Não é a primeira vez que os Hospitais portugueses são vítimas de ataques informáticos.

No final de 2016 o Hospital Garcia de Orta foi vítima de um ataque informático que incidiu no sistema onde são guardados imagens obtidas em exames médicos como radiografias ou TAC e agora há informações que o grupo de Hospitais CUF também foi alvo de um ataque informático.

Reading Time: 2 minutes

Os sistemas da multinacional Altran foram paralizados devido a um ataque informático com origem ainda desconhecida.

A empresa de engenharia sofreu um ataque informático e os criminosos acederam aos dados dos colaboradores.

A Altran foi atacada por hackers a nível internacional e nacional, com os responsáveis a terem conseguido infiltrar-se no sistema de segurança na madrugada de quinta-feira, dia 24.

CIBERSEGURANÇA & PROTECÇÃO DE INFRA-ESTRUTURAS CRITICAS (PIC)

NIST CYBERSECURITY FRAMEWORK

CIBERSEGURANÇA & PROTECÇÃO DE INFRA-ESTRUTURAS CRITICAS (PIC)

Identify

- Desenvolvimento Normativo, Planos Diretores e SGSI
- Definição de Controlos, Indicadores e Dashboards
- Auditorias de Cumprimento (27000, NIS,...)
- Análise e Gestão de Risco

Protect

- Assessoria na adoção e incorporação de novas tecnologias
- Implantação de soluções tecnológicas de ciber-segurança
- Desenvolvimento de soluções e serviços próprios

Detect

- Ciberavaliações personalizadas (pentest, secdevops, apps...)
- Gestão de vulnerabilidades
- Red Team
- Infraestruturas de monitorização contínua

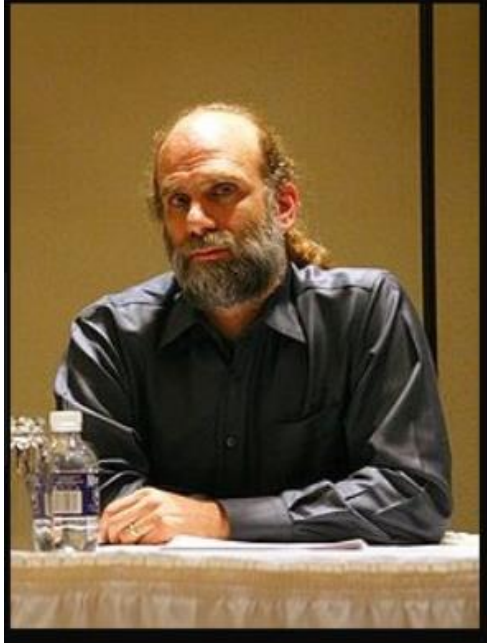
Respond

- Diagnósticos especializados (hackings, código fonte, ...)
- Blue Team
- GMV SOCs

Recover

- GMV-CERT
- Serviços proativos: Assessments, Gestão da configuração, Serviços de Inteligência
- Serviços reativos: Gestão de incidências, Análise forense

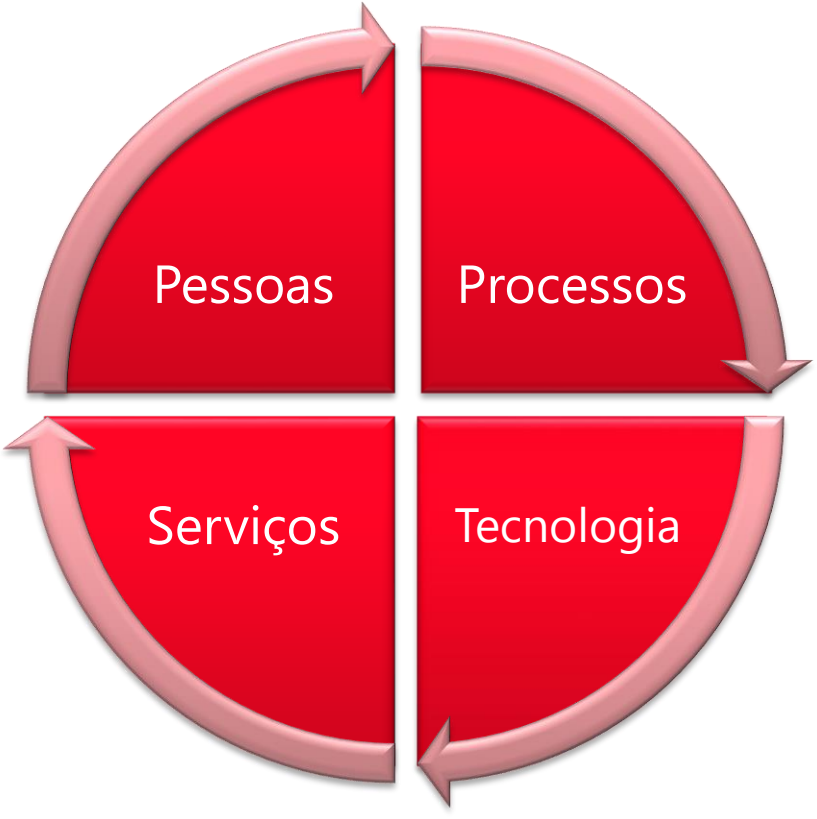
gmv



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

(Bruce Schneier)

Cibersegurança: Abordagem GMV



COMPETÊNCIAS & EXPERIÊNCIA

PESSOAS

- Auditorias de Engenharia Social
- Formação e *Awareness* para a cibersegurança
- Prevenção Hacking (“hacktivism prevention”)
- Prevenção Fraude
- Capacitação em Desenvolvimento de Código Seguro
- Preparação de resposta a incidentes

COMPETÊNCIAS & EXPERIÊNCIA

PROCESSOS

- Gestão de Risco:
  - Avaliação do Nível Segurança: Auditorias Técnicas, Auditorias de Risco, Business Impact Analysis, etc.
  - Seguimento dos Níveis de Risco
  - Avaliação de Segurança de "novos ambientes": Infraestruturas Cloud, Redes Sociais,…
- Cumprimento Normativo:
  - Avaliação, Auditoria e Implementação
  - ISO 27000, NIST, PCI DSS…
  - Proteção de Infraestruturas Criticas (NIS)
- Planeamento e Gestão de Segurança:
  - Planos de Segurança da Informação
  - Gabinetes de Segurança: Definição, Operação e Manutenção de Sistemas de Gestão (ISMS, BCMS, etc)
  - Planos de Continuidade de Negócio

COMPETÊNCIAS & EXPERIÊNCIA

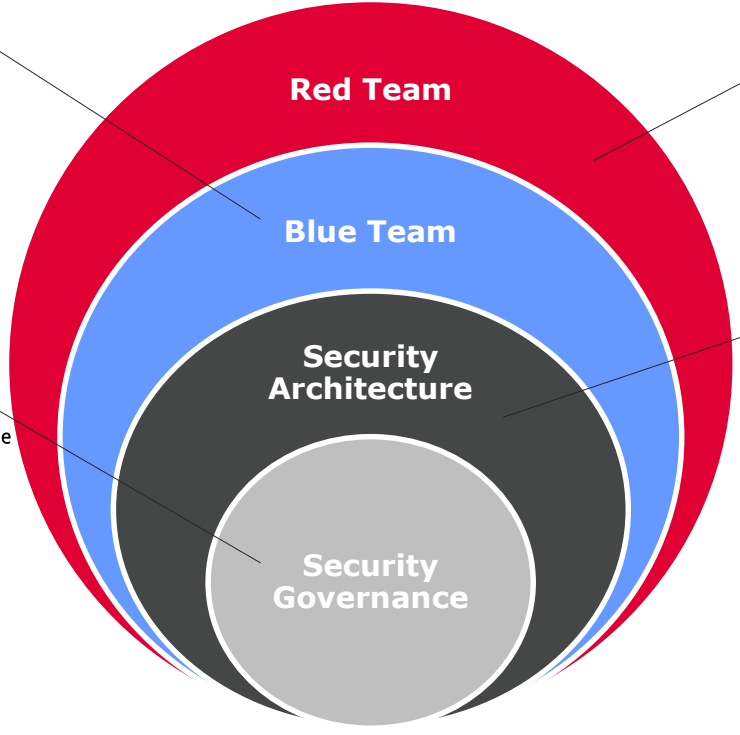
SERVIÇOS

- Assessoria na adoção e incorporação de novas tecnologias
- Implementação de soluções tecnológicas
- Segurança no Ciclo de Vida de Aplicações
- Security Operations Center (SOC)
- Vigilância Digital
- Ethical Hacking
- Análise Forense

COMPETÊNCIAS & EXPERIÊNCIA

TECNOLOGIA

A ABORDAGEM GMV



- Prevenção Fraude e Soluções Anti-Fraude
- Análise Forense
- Gestão de Vulnerabilidades
- OSINT (Open Source Intelligence)
- Security Operations Center (SOC) e Serviços de CERT
- Resposta a Incidentes
- Análise do Landscape de Ameaças

- Testes de intrusão (ou ethical hacking) em infraestruturas / a partir de endpoints
- Identificação e análise de vulnerabilidades
- Reconhecimento / Discovery de Sistemas Expostos à Internet e Vulnerabilidades
- Footprinting e análise de engenharia social
- Vigilância Digital

- Consultoria e Assessoria de Segurança
- Avaliação de Segurança da transição para a Cloud e novos paradigmas
- Auditorias (técnicas, de risco, análises de impacto, etc)
- Gestão e Análise de Risco
- Gap Analysis (ISO27001)
- CISO-as-a-Service
- Definição, Operação e Manutenção de Planos e Planos e Sistemas de Gestão (ISMS, BCMS, etc)

- Segurança no Ciclo de Vida de Aplicações (SAST, IAST, DAST, RASP, pentesting)
- Capacitação em Desenvolvimento de Código Seguro
- Levantamento, Recomendação e Definição de Controlos de Segurança
- Assessoria em scouting, adoção e incorporação de novas tecnologias
- Implementação e Serviços de Soluções de Segurança (SIEM, PAM, IAM, NGFW, EDR, mitigação DDoS, etc)
- Formação e Awareness para a Cibersegurança
- Prevenção Hacking ("hacktivism prevention")
- Preparação de resposta a incidentes

Data Privacy

- DPO-as-a-Service e DPA-as-a-Service
- Cumprimento GDPR
- Identificação de Dados Sensíveis a questões de Privacidade e Legislação Aplicável
- Levantamento e Definição de Controlos para Privacidade de Dados

Capacidades

SOC / CERT

INNOVATING SOLUTIONS

Serviços GMV-CERT

- Operação
- Prevenção
- Detecção
- Resposta
- Intelligence

- **Certificações:**
  - ISO 9001: Quality
  - ISO 20000: Service management
  - ISO 22301: Business continuity
  - ISO 27001: Information security
  - Continuous improvement
  - Proactivity

CYBERSECURITY

Serviços GMV-CERT

Operação

- Correção de anomalias para todos os elementos de segurança sob contrato, p.e., Firewall, WAF, SIEM, etc.

Prevenção

- Alertas / Avisos
- Gestão de Vulnerabilidades
- Auditorias de Segurança

Detecção

- Avaliar se as aplicações e sua infraestrutura de suporte funcionam no modo nominal
- Detecção de eventos de segurança que podem os ativos do cliente
- Centralização e correlação de logs

Resposta

- Determinar a origem de um incidente de segurança
- Conter e erradicar o incidente
- Corrigir deficiências de segurança
- Analisar, documentar e salvaguardar de evidências
- Estabelecer lições aprendidas
- Análise Forense

Intelligence

- Pesquisar informações associadas à organização ou a funcionários mais importantes em diferentes redes sociais (vulnerabilidades, ameaças, venda de informações, etc.)

GMV

EXEMPLOS DO QUE FAZEMOS

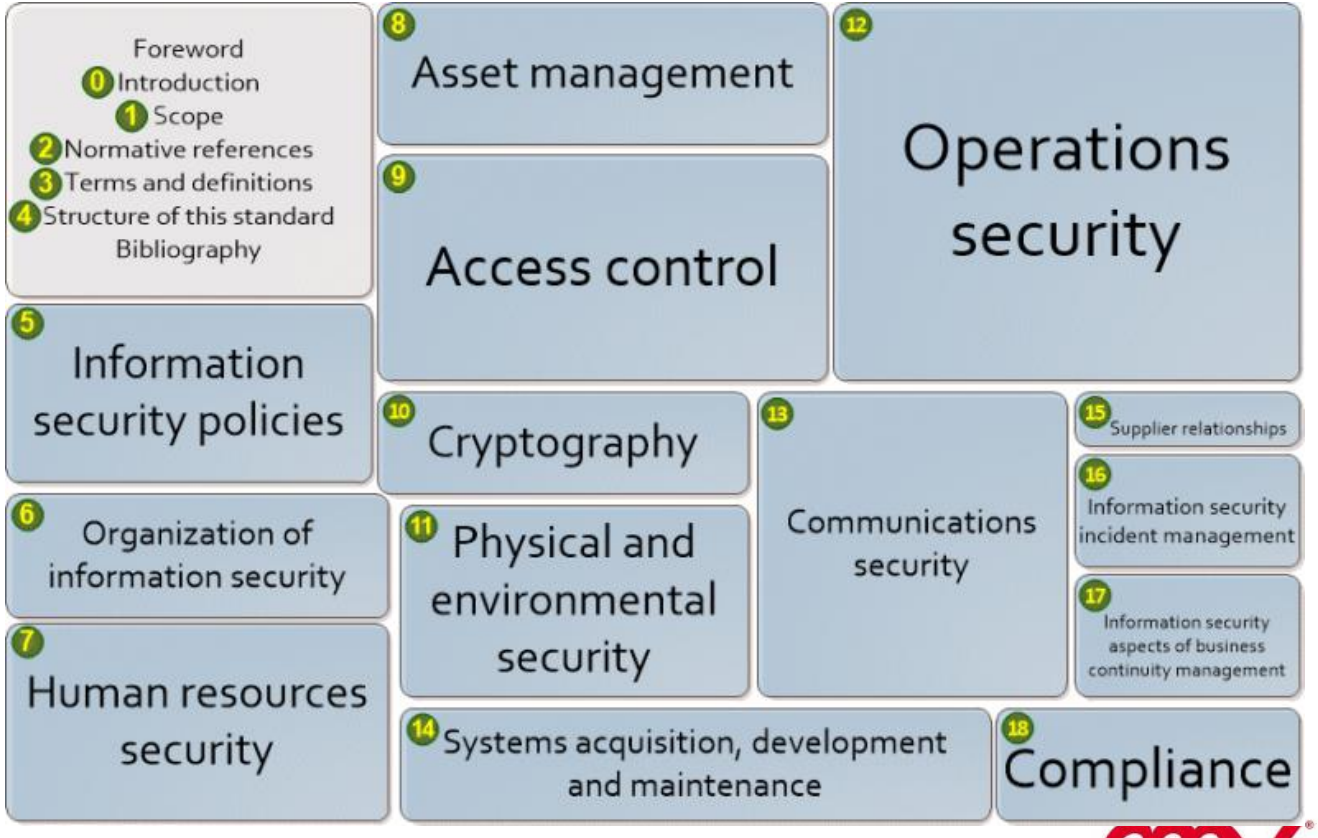
ANÁLISE DA SITUAÇÃO

SEGURANÇA DA INFORMAÇÃO vs. ISO27000

INNOVATING SOLUTIONS

FRAMEWORK DE REFERÊNCIA: ISO 27001/2

A GMV propõe realizar a análise da situação usando a framework ISO 27001-27002. Outros padrões, como NIST Cybersecurity Framework, podem ser utilizados.



FASES PROPOSTAS

01	AQUISIÇÃO DE INFORMAÇÃO	Entrevistas, revisão de políticas e procedimentos existentes
02	ANÁLISE DE LACUNAS	Análise da cobertura dos domínios de gestão das normas ISO 27001 e ISO 27002
03	PREPARAÇÃO DA DOCUMENTAÇÃO	Criação da documentação da análise e da apresentação aos sponsors do projeto, e revisão com a equipa do Cliente
04	APRESENTAÇÃO AOS SPONSORS DO PROJECTO	Apresentação dos resultados e principais conclusões do projeto aos sponsors do projeto, no Cliente
05	PLANO DIRETOR DE SEGURANÇA	Proposta de um Plano Diretor de Sistemas e Segurança baseado numa análise de risco, que incluirá as ações a serem tomadas para cobrir os controles necessários de acordo com ISO 27002 e as recomendações de gestão de TI de acordo com as boas práticas do ITIL-ISO2000
06	SERVIÇO "CISO AS A SERVICE"	Gestão do Segurança da Informação em modelo "CISO as a Service"

COMPETÊNCIAS & EXPERIÊNCIA

"CISO as a Service"

- Auditorias de Engenharia Social
- Formação e *Awareness* para a cibersegurança
- Assessoria na adoção e incorporação de novas tecnologias
- Segurança no Ciclo de Vida de Aplicações
- Avaliação do Nível de Segurança de organizações, processos e sistemas
- Auditorias de Risco
- Business Impact Analysis
- Cumprimento Normativo:
  - Avaliação, Auditoria e Implementação
  - ISO 27000, NIST, PCI DSS…
- Planeamento e Gestão de Segurança:
  - Planos de Segurança da Informação
  - Gabinetes de Segurança: Definição, Operação e Manutenção de Sistemas de Gestão (ISMS, BCMS, etc)
  - Planos de Continuidade de Negócio

ASSET AND ANOMALY DETECTION (AAD)

Detecção de Ativos e Anomalias (*Asset and Anomaly Detection* - AAD) é um produto para a gestão de ativos e detecção de anomalias para redes ICS (*Industrial Control Systems)* / SCADA que fornece reconhecimento situacional rápido e concreto por meio de alertas em tempo real. As soluções AAD monitoram constantemente o tráfego de rede do sistema de controle industrial e gera alertas para o comportamento anómalo da rede que indica uma presença maliciosa que tem o potencial de interromper processos industriais.

DESAFIOS DE CLOUD

Principais **inibidores** da migração para *Cloud*:

- Privacidade
- Integridade e localização dos dados
- *Compliance*
- *Skills*
- *Snooping* por parte de Governos e Autoridades

Fonte: Gartner

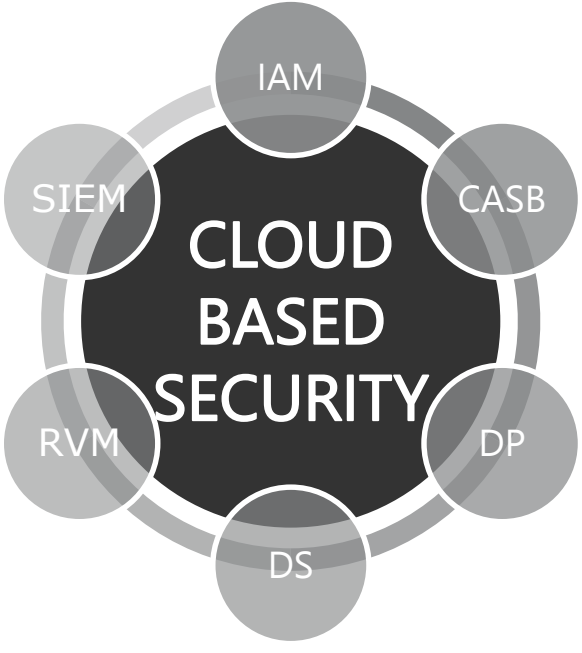
DESAFIOS DE SEGURANÇA

Principais desafios de segurança, em Cloud:

- Violações de dados
- Sequestro de contas
- Ameaças internas
- Injeção de Malware
- Abuso de serviços
- APIs inseguras
- Falta de visibilidade
- *Shadow IT*
- *Dark Data*
- Vulnerabilidades partilhadas

FRAMEWORK DE SEGURANÇA CLOUD GMV

Objetivo → Reduzir o próprio risco na adoção de *Cloud*



Identity Access Management (IAM)

Cloud Access Security Broker (CASB)

Proteção de Dados (DP)

Segurança de Dados (DS)

Gestão de Vulnerabilidades remota (RVM)

Gestão de Eventos e Incidentes de Segurança (SIEM)

"Secure, Vigiland and Resilient"

Be Secure

- Adote uma abordagem mensurada e baseada no risco para o que está protegido e como protegê-lo. A sua propriedade intelectual está segura? A sua cadeia de fornecimento ou ambiente de ICS é vulnerável?

Be Vigilant

- Monitore continuamente os sistemas, redes, dispositivos, pessoal e ambiente em busca de possíveis ameaças. A inteligência de ameaças em tempo real e a IA geralmente são necessárias para entender ações prejudiciais e identificar rapidamente ameaças na grande variedade de novos dispositivos conectados que estão sendo introduzidos.

Be Resilient

- Um incidente pode acontecer. Como a sua organização responderia? Quanto tempo levaria para recuperar? Com que rapidez poderia remediar os efeitos de um incidente?

www.gmv.com

OBRIGADO

João Sequeira
Director SES Portugal
joao.sequeira@gmv.com

GMVIS Skysoft S.A. (GMV)
Av. D. João II, Nº 43,
Torre Fernão de Magalhães, 7º,
1998-025 Lisboa, Portugal
Tel: +351 213829366, Fax: +351 213866493

gmv BLOG