

**CONTE**  
*COM A*  
**GENTE**

***FIESC***

***A FORÇA DA INDÚSTRIA CATARINENSE***

Segurança da Informação

Σεβντανα ρα νυοιναζοο

# Agenda



Estrutura FIESC

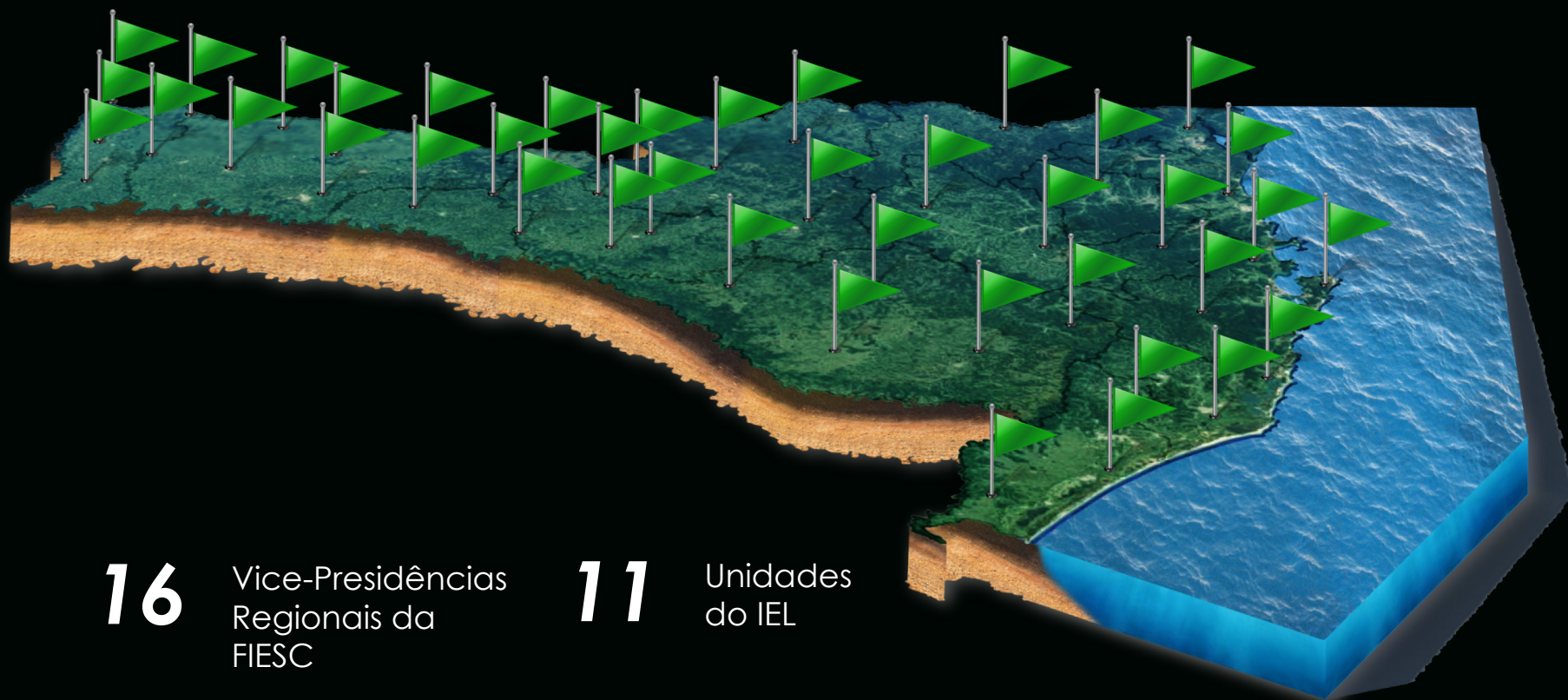
Segurança da Informação em 2004

Segurança da Informação em 2013

Programa de conscientização 2017

# ESTRUTURA FIESC

# FIESC



**16** Vice-Presidências Regionais da FIESC

**11** Unidades do IEL

**13** Núcleos Regionais

**268** Unidades do SESI

**62** Unidades do SENAI

# FIESC



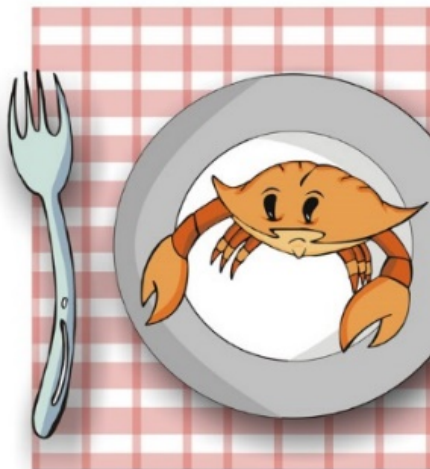
## **ESTRUTURA FIESC**

**FIESC**

- + 20.000** Dispositivos Corporativos
- + 9.000** Colaboradores
- + 6.500** Demandas de TI abertas por mês
- + 1.200** Servidores Físicos ou Virtualizados
- + 200** Aplicações suportadas
- + 120** Colaboradores de Tecnologia da Informação no Estado

# 2004

Não coloque o siri em perigo.



Organize seu ambiente de trabalho  
Evite deixar documentos largados  
Colabore com a campanha Boca do Siri



Unidade Regional  
de Florianópolis



Em breve, o Siri vai invadir  
sua praia.  
Aguarde.

Unidade Regional  
de Florianópolis

FIESC  
CIESC  
SESI  
SENAI  
SEL  
Serviço Nacional de Aprendizagem Industrial  
Centro de Tecnologia em Automação Industrial

## ***POLÍTICA DE SEGURANÇA SISTEMA FIESC***

**SENAI**<sup>sc</sup>  
Florianópolis **CTAI**

**CTAI**  
SECURITY

Este projeto foi desenvolvido pela equipe de especialistas de segurança do SENAI/CTAI.

**FIESC**

A top-down view of a whole cooked crab on a white plate. The crab is bright orange and is surrounded by several lemon wedges and fresh green cilantro leaves. The plate is set on a white tablecloth. To the left, a silver fork is partially visible. To the right, a glass of white wine and a teal napkin with silverware are also visible.

**E depois?**

**FIESC**

# 2013

**PROJETO**

**2. RESUMO DA CONSULTORIA**

Durante o processo de consultoria foram analisados os seguintes aspectos da segurança da informação: (1) Política de Segurança da Informação, (4) Segurança de Recursos Humanos, (5) Gerenciamento das Operações e Comunicações, (6) Gerenciamento de Incidentes, (7) Gerenciamento de Continuidade de Negócios, (8) Gerenciamento de Riscos, (9) Gestão de Incidentes de Segurança da Informação, (10) Gestão de Conformidade.

**2.1 Visão Geral dos Controles de Segurança da Informação**

Nesta sessão será apresentado o relatório gráfico contendo o percentual da situação de conformidade e andamento, especificamente, para cada capítulo de controles da segurança da informação.

SITUAÇÃO	Atende Total
Relevância	Critico

**3.5 SEGURANÇA FÍSICA E DO AMBIENTE**

**3.5.1 Áreas Seguras**

Observamos que a sede da FIESC atende de forma adequada este tópico, porém nas unidades o tratamento responsável pela segurança e também coordenador do expediente as restrições necessárias são nenhuma restrição de segurança física.

SITUAÇÃO	Atende Parcial
Controle 9.1.1: Perímetro de Segurança Física	

**2.2 Visão por Capítulos de Controles de Segurança da Informação**

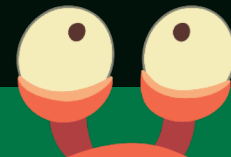
Nesta sessão será apresentado o relatório gráfico contendo o percentual da situação de conformidade e andamento, especificamente, para cada capítulo de controles da segurança da informação.

**Figura 1 - Situação geral de conformidade**

Controle	Situação	Relevância
Controle 9.1.3: Segurança em escritórios, salas e áreas comuns	Atende Parcial	Moderado
Controle 9.1.4: Proteção contra ameaças externas	Atende Informal	Moderado
Controle 9.1.5: Trabalhando em áreas seguras	Atende Parcial	Moderado
Controle 9.1.6: Acesso do público, áreas de estacionamento e áreas de acesso	Não Se Aplica	

Documento Confidencial

## Consultoria e GAP Analysis



**GETIC**

## Equipe de Segurança da Informação

2 responsáveis de Segurança da Informação  
Trabalham em SI

### Sustentação

Monitoramento

Incidentes

Solicitações de  
Serviço

### Inovação

Governança

Arquitetura

Segurança

Negócios

# Equipe de Segurança da Informação

2 responsáveis de Segurança da Informação  
Trabalhando exclusivamente em SI

**GETIC**

**TANGO**

Gabriel Conceição

Marcelo Gandra

Consultoria:



**Inovação**

Governança

Arquitetura

Segurança

Negócios



# Equipe de Segurança da Informação

2 responsáveis de Segurança da Informação  
Trabalhando exclusivamente em SI

**OKR**  
Objectives &  
Key Results





## Comitê Operacional de Segurança da Informação - COSIF

15 colaboradores de diversos setores com reuniões a cada 45 dias



## Grupo de resposta a incidentes de segurança - GRIS

Grupo formado por RH, Jurídico, Adm e TI  
Com acionamento sob demanda



# Grupo técnico de resposta a incidente de Segurança - GTRIS

Cinco analistas de TI

Reuniões quinzenais e acionamento sob demanda





**GTRIS**

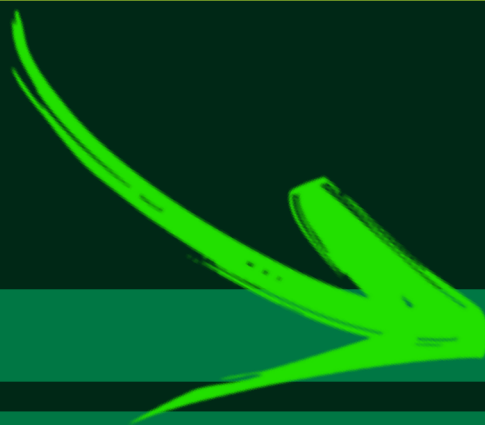
**GRIS**

**COSIF**

**Equipe de Segurança da Informação**

**FIESC**

Correção de vulnerabilidades.  
Atuação técnica



**GTRIS**

**GRIS**

**COSIF**

**Equipe de Segurança da Informação**

**FIESC**

# Medidas disciplinares



GRIS

GRIS

COSIF

Equipe de Segurança da Informação

**FIESC**

# Revisão da Política de Segurança

GTRIS

GRIS

COSIF

Equipe de Segurança da Informação

**FIESC**

# Responsáveis pela Gestão da Segurança da Informação



**GTRIS**

**GRIS**

**COSIF**

**Equipe de Segurança da Informação**

**FIESC**





Menu

Capacitação na Política de Se...

- Abertura
- Apresentação
- Conscientização 1
- Conscientização 2
- Segredos
- Pilares: confidencialidade
- Pilares: integridade
- Pilares: disponibilidade
- Histórico 1
- Histórico 2
- O que é
- Onde encontrar
- Importância
- Exemplos de aplicação
- Propriedade intelectual 1
- Propriedade intelectual 2
- Acesso à internet 1
- Acesso à internet 2
- Acesso à internet 3
- Dispositivos pessoais
- Dispositivos de armazenam...
- Telefonia
- Correio eletrônico
- Mensagens instantâneas
- Senhas 1
- Senhas 2
- Impressão
- Dispositivos corporativos

# Treinamento EAD

75% colaboradores atingidos  
Cerca de 7200 colaboradores

Olá, seja bem vindo à capacitação:  
Política de Segurança da  
Informação da FIESC



## Vídeo de integração

Material da integração de novos  
colaboradores.

possuam as principais atividades dos processos de continuidade, deve-se iniciar a execução dos processos ou atividades de negócio

3. IMPLEMENTAR

3.1. A Política de

O capítulo de introdução conter:

- Objetivos;
- Declaração da Adm;
- Documentos Relat;
- Definições;
- Autores;
- Divulgação e distri;
- Atualização e Revisão;
- Manutenção da S

O capítulo de introdução conter:

3.1.2 Segurança Lógica

O capítulo de Segurança deve conter:

- Acesso à Internet
- Acesso à Rede In
- Armazenamento e

seus objetivos para a

A classificação de impacto determinada atividade no

A descrição do impacto de consequências para a org

As definições de classificação observando os aspectos de imagem da organização per

A identificação de atividades realizadas através de entre que possuem. O objetivo atividades que requisitam GETIC e são o mapeament cada setor.

3.1.2 Identificação de Recursos

A partir das atividades identificadas na análise de impacto de negócio, deve ser realizado levantamento dos recursos envolvidos com tais atividades. Os recursos podem estar divididos em recursos primários e recursos secundários. Recursos primários são aqueles diretamente ligados aos processos de negócio identificados na BIA (Business Impact Analysis). Recursos secundários são recursos não ligados diretamente aos processos de negócio identificados na BIA, mas sim ligados aos recursos primários ou mesmo a outros recursos secundários, ou seja, os recursos secundários são aqueles aos quais os processos de negócio dependem indiretamente.

Os recursos identificados no plano de continuidade de negócio de tecnologia da informação do Sistema FIESC podem ser classificados ou agrupados conforme a tabela representada na figura 10 abaixo.

TIPO DE RECURSO	
1	Ambientes Físicos
2	Utilidades
3	Infraestrutura de Rede
4	Servidor Físico (hardware)
5	Servidor Virtual (hardware)
6	Outros Hardwares
7	Software
8	Informação digital
9	Informação física

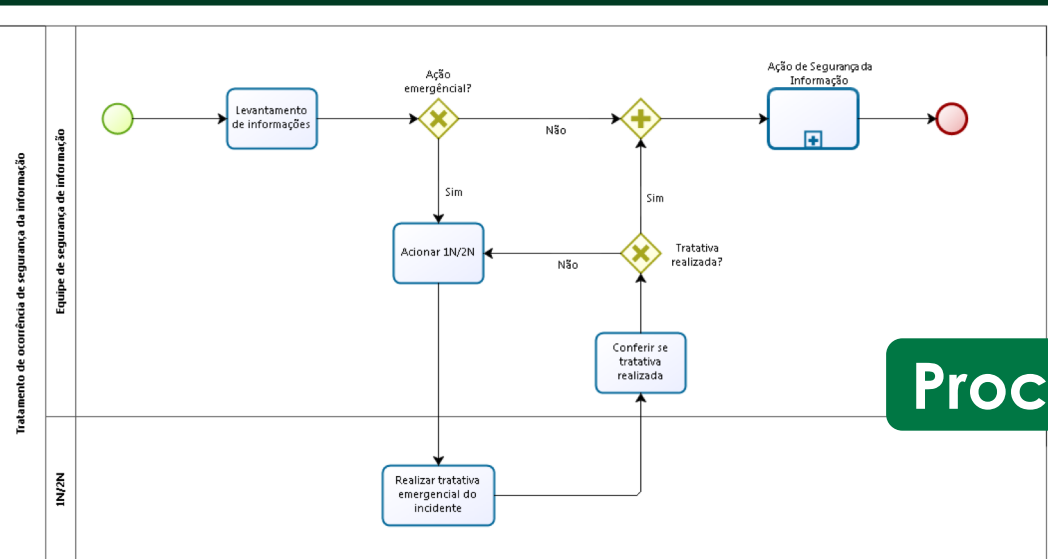
Figura 10 - Listagem de recursos para o PCNF.

Recursos do tipo informação digital e informação física consistem na própria informação para, por exemplo arquivos digitais de documentos em texto ou planilhas (informação digital), ou documentos em papel, por exemplo contratos (informação física).

Os sistemas de informação são recursos importantes para a continuidade de negócio e devem ser classificados na categoria de recursos de Software. Da mesma forma ocorre com Servidores Físicos (hardware) e servidores virtuais, os quais devem ser classificados em suas respectivas categorias. A categoria Outros Hardwares deve conter equipamentos que não se classificam como servidores físicos e nem como infraestrutura de rede.

# Sistema de Gestão de Segurança da Informação

Auditoria de Segurança  
Plano de Continuidade  
Revisão da Política  
Análise de risco



## Processos

- Incidente de Segurança
- Inspeção de vulnerabilidades
- Participação em novos projetos



# Programa de Gestão de Segurança

- Projetos de análise de risco
- Projetos de PCN
- Projetos de auditoria



## Rotinas de inspeções técnicas

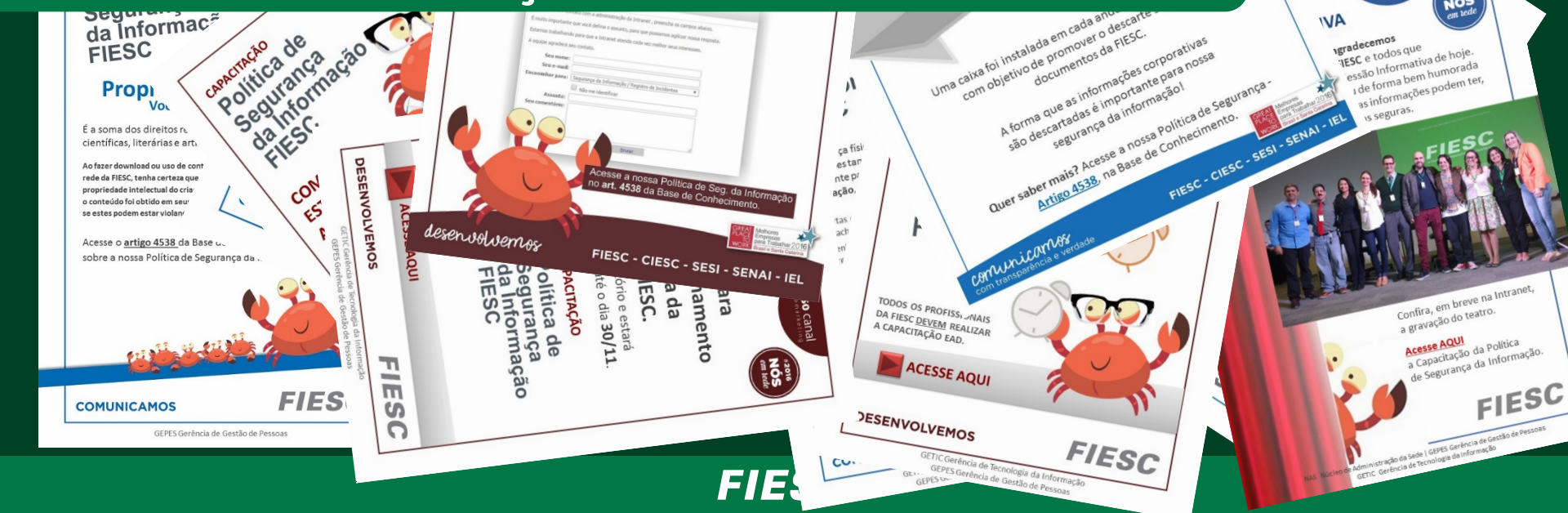
Acompanhamento de incidentes  
Avaliação de administradores  
Avaliação de VPNs  
...

18 Rotinas – 122 demandas/ano





**36 comunicados diferentes.  
Reforço de envio a cada 15 dias.**



# Programa de Conscientização



Competição  
entre regionais

- 13 núcleos regionais;
- 6 meses de duração;
- Atividades pré-agendadas;
- Ranking mensal;
- Incentivo aos vencedores.

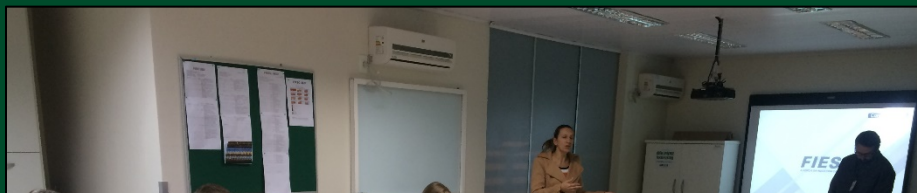


COLABORADORES



# Resultados do Programa

28 reuniões com Diretores e Gerentes



**FIESC SENAI**  
A FORÇA DA INDÚSTRIA CATORINENSE

**FIESC**

Local de realização: SESI SERRA CATORINENSE  
Data: 08/06/2017  
Nome dos Facilitadores:

**Lista de Presença**  
Segurança da Informação

Nº	Nome do participante	Unidade	Assinatura
1	Lucas		
2	Oliver		
3	mp		
4	ma	EM 200	
5	Ag		
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			



# Resultados do Programa

Grupo-Vulnerabilidade	Categoria-Vulnerabilidade	Item-Vulnerabilidade	Conformidade
1-Organização da Segurança Informaçãc 1A - Política de Segurança da Informação		Controle de propriedade intelectual é adequado	2-Parcial Superior
1-Organização da Segurança Informaçãc 1A - Política de Segurança da Informação		É realizada Avaliação de risco periódica	4-Não Atende
1-Organização da Segurança Informaçãc 1A - Política de Segurança da Informação		Existem Políticas de Uso adequado e sua correta implantação	3-Parcial Inferior
1-Organização da Segurança Informaçãc 1A - Política de Segurança da Informação		Procedimentos de Demissão, Admissão e Transferência é adequado	4-Não Atende
1-Organização da Segurança Informaçãc 1A - Política de Segurança da Informação		Processo de Treinamento e Conscientização de Colaboradores é adequado	4-Não Atende
1-Organização da Segurança Informaçãc 1C - Gestão de Partes Externas		A segurança de contratos com fornecedores e parceiros é adequada	2-Parcial Superior
1-Organização da Segurança Informaçãc 1C - Gestão de Partes Externas		Os riscos na relação com os clientes são gerenciados	2-Parcial Superior
1-Organização da Segurança Informaçãc 1C - Gestão de Partes Externas		Os riscos na relação com os terceiros e parceiros são gerenciados	2-Parcial Superior
1-Organização da Segurança Informaçãc 1C - Gestão de Partes Externas		Controle da Entrega de Serviços dos Terceiros	2-Parcial Superior
1-Organização da Segurança Informaçãc 1C - Gestão de Partes Externas		Gerenciamento de Mudanças para Serviços Terceirizados	3-Parcial Inferior
1-Organização da Segurança Informaçãc 1C - Gestão de Partes Externas		Monitoramento e Análise Crítica de Serviços Terceirizados	2-Parcial Superior
1-Organização da Segurança Informaçãc 1E - Gestão da Conformidade		A segurança de contratos com clientes é adequada	2-Parcial Superior
1-Organização da Segurança Informaçãc 1E - Gestão da Conformidade		São realizadas auditorias periódicas de segurança	3-Parcial Inferior

24 Coletas de dados para Análise de Riscos.

2-Processos de TIC	2A - Procedimentos e Responsabilidades Operacionais	Existe separação dos recursos de desenvolvimento, teste e produção	5-Não se Aplica
2-Processos de TIC	2B - Planejamento e Aceitação dos Sistemas	São levantados requisitos de segurança na aquisição de sistemas	2-Parcial Superior
2-Processos de TIC	2B - Planejamento e Aceitação dos Sistemas	Sistemas sempre são atualizados quando encontradas falhas de segurança	1-Atende Totalmente
2-Processos de TIC	2B - Planejamento e Aceitação dos Sistemas	Todos os sistemas são suportados atualmente por seus fornecedores	2-Parcial Superior
2-Processos de TIC	2B - Planejamento e Aceitação dos Sistemas	Existe uma gestão de capacidades para os sistemas atuais e futuros	3-Parcial Inferior
2-Processos de TIC	2C - Cópias de Segurança	Existe procedimento adequado e formal de backup	2-Parcial Superior
2-Processos de TIC	2C - Cópias de Segurança	O backup é transportado de modo seguro	2-Parcial Superior
2-Processos de TIC	2C - Cópias de Segurança	O backup é armazenado de modo seguro	1-Atende Totalmente
2-Processos de TIC	2C - Cópias de Segurança	Existe segregação de funções no processo de backup	2-Parcial Superior
2-Processos de TIC	2D - Gerenciamento da Segurança em Redes	Existem definições de funções quanto ao gerenciamento da segurança da rede	3-Parcial Inferior
2-Processos de TIC	2D - Gerenciamento da Segurança em Redes	Existem controles para garantir a confidencialidade das informações em rede	2-Parcial Superior
2-Processos de TIC	2D - Gerenciamento da Segurança em Redes	Existem controles para garantir a integridade das informações em rede	2-Parcial Superior
2-Processos de TIC	2D - Gerenciamento da Segurança em Redes	Existe segregação de redes com diferentes objetivos	2-Parcial Superior
2-Processos de TIC	2D - Gerenciamento da Segurança em Redes	Os componentes de rede são redundantes em nível adequado	3-Parcial Inferior

# Resultados do Programa



21 Dias de Segurança da Informação.

# Resultados do Programa



30 Processos corrigidos.

**FIESC**



# Resultados do Programa



al	
9	41%
9	45%

11 Atividades livres.

# Resultados do Programa

2.034 – (22,4%) dos colaboradores capacitados.



135 Apresentações realizadas.



# Resultados do Programa



Visita dos líderes a Futurecom

**FIESC**



# Resultados do Programa



Visita das equipes a Florianópolis

**FIESC**



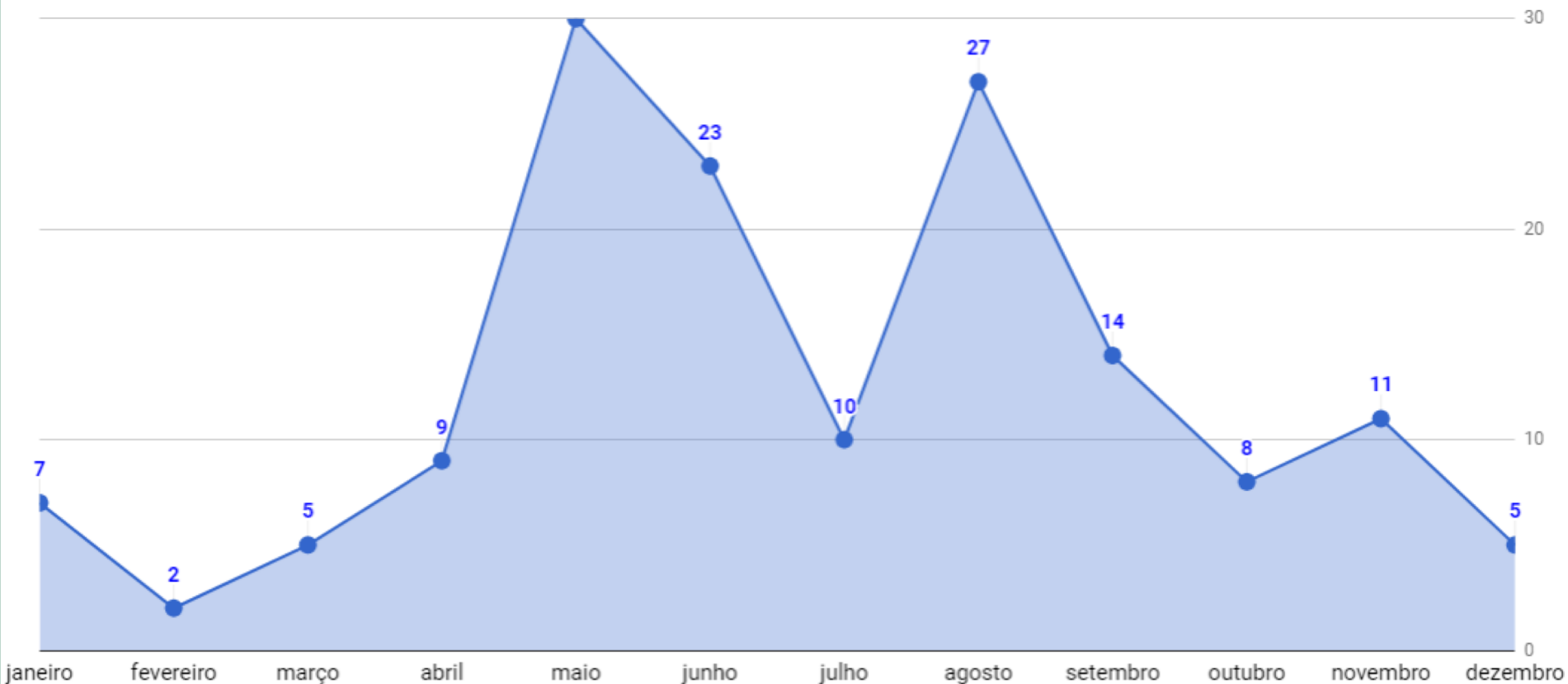
# Resultados do Programa



Premiação das equipes.

# Resultados do Programa

Número de Incidentes 2017



# Resultados do Programa

----- Forwarded message -----

From: **Ministério da Saúde** <[cadastrofpopular@saude.gov.br](mailto:cadastrofpopular@saude.gov.br)>

Date: 2017-04-05 8:00 GMT-03:00

Subject: Irregularidades / Programa Farmácia Popular - SERVIÇO SOCIAL DA INDÚSTRIA

To: SERVIÇO SOCIAL DA INDÚSTRIA <[fm505@sesifarmacias.com.br](mailto:fm505@sesifarmacias.com.br)>

A/C

O Ministério da Saúde informa que ao realizar uma **auditoria**, foram identificadas **irregularidades** recorrentes no cadastro abaixo:

**Razão Social:** SERVIÇO SOCIAL DA INDÚSTRIA

**Nome Fantasia:** SESI-DEPARTAMENTO REGIONAL DO ESTADO DE SANTA CATARINA

**Endereço:** RUA VISCONDI DE TAUNAY - , CENTRO - SAO BENTO DO SUL/SC

**Telefone:** (47) 3633-3515 /

## **Representante Legal**

Nome: FABRIZIO MACHADO PEREIRA

CPF:

## **Contato**

Nome:

CPF: 000.000.000-00

Telefone:

Email:

# Resultados do Programa

Em 9 de maio de 2017 11:11, <[Fernanda.Thomazi@bmw.com.br](mailto:Fernanda.Thomazi@bmw.com.br)> escreveu:

Olá Bianca,

Tudo bem?

Recentemente, a nossa ex-funcionária Denise Borges, entrou em contato com vocês para alguns questionamentos/documentos de data privacy, auditoria que sofreremos ainda este mês.

Acabei assumindo esse tópico no meio do caminho, portanto, não sei é com você. Se não for, peço a gentileza de me direcionar para o contato certo.

Durante alguns questionamentos de armazenamento de dados, o IEL mencionou que possui uma política a respeito. Gostaria de saber se vocês podem compartilhar essa política com a **BMW**.

Obrigada.

## **BMW Group**

Fernanda Thomazi  
Production Network 2 - Plant Brazil  
Human Resources, TV-446  
HR Analyst  
Rodovia BR-101, Km 67 - Corveta  
CEP 89245-000  
Araquari - SC - Brasil

Mobile: [+55-47-99194-3733](tel:+55-47-99194-3733)

Office: [+55-47-3016-1178](tel:+55-47-3016-1178)

Mail: [fernanda.thomazi@bmw.com.br](mailto:fernanda.thomazi@bmw.com.br)

Web: <http://www.bmw.com.br>

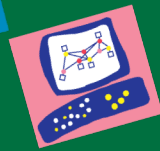
THE NEXT  
100 YEARS



**FIESC**

# Resultados do Programa

Aquisição de Next Generation Firewall



Check Point®  
SOFTWARE TECHNOLOGIES LTD.

FORTINET®

Aquisição de serviço Anti DDoS



**FIESC**

Disponibilidade  
Visibilidade  
Consciência  
Não-repúdio  
Autenticidade  
Confidencialidade  
Conformidade  
Cultura  
Conhecimento  
Integridade

# #FAÇOPARTE

Confiabilidade  
Consciência  
Autenticidade  
Disponibilidade  
Visibilidade  
Integridade  
Confidencialidade  
Conformidade  
Não-repúdio  
Cultura  
Segurança  
FIESC



FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SANTA CATARINA

# ***FIESC***

***A FORÇA DA INDÚSTRIA CATARINENSE***

**FIESC - CIESC - SESI - SENAI - IEL**

**Gabriel Ferreira Ramos da Conceição**  
**E-mail: [gabriel.conceicao@fiesc.com.br](mailto:gabriel.conceicao@fiesc.com.br)**

**fiesc.com.br | 0800 48 1212**  
**Rodovia Admar Gonzaga, 2765 Itacorubi 88034-001**  
**Florianópolis, SC**

