***SEGURANÇA E AUDITORIA DE SISTEMAS***

EMPRESA: {{NOME DA EMPRESA}}

O que precisamos fazer?

1-Precisamos de entender como a empresa funciona;

2- Como é a estrutura dela de segurança (caso houver);

3- Como podemos melhorar elas/ implementar dentro da empresa;

4- Se a solução que nós implementamos compensa para eles.

Para isso é necessário serem propostas/estudadas algumas possibilidades, no qual podem ser levadas em consideração.

### 1. Análise de Riscos

* Realizar uma avaliação completa dos riscos de segurança que a empresa enfrenta.
* Identificar ativos críticos e possíveis vulnerabilidades nos sistemas.

**2. Políticas de Segurança**

* Desenvolver e implementar políticas de segurança da informação, como controle de acesso, política de senhas, e uso adequado de dispositivos.

**3. Auditoria de Sistemas**

* Realizar auditorias periódicas nos sistemas e processos.
* Implementar ferramentas de monitoramento para detectar atividades suspeitas.

**4. Segurança de Infraestrutura**

* Avaliar e reforçar a segurança de redes, servidores e dispositivos.
* Implementar firewalls, VPNs e sistemas de prevenção/detecção de intrusões (IDS/IPS).

**5. Segurança de Aplicações**

* Analisar e corrigir vulnerabilidades em softwares e aplicações utilizadas pela empresa.
* Utilizar práticas de desenvolvimento seguro, como testes de penetração e revisão de código.

**6. Treinamento e Conscientização**

* Promover treinamentos regulares para os funcionários sobre boas práticas de segurança.
* Realizar simulações de phishing e outras ameaças para educar os usuários.

**7. Backup e Recuperação de Desastres**

* Estabelecer rotinas de backup frequentes e testar a recuperação dos dados.
* Criar um plano de continuidade de negócios e recuperação de desastres.

**8. Automação e Monitoramento**

* Implementar sistemas de SIEM (Security Information and Event Management) para monitoramento e resposta a incidentes em tempo real.

**9. Análise de Custo-Benefício**

* Avaliar se os investimentos em segurança trazem retorno adequado para a empresa.
* Medir o impacto das melhorias implementadas na redução de riscos.

***RESPOSTAS DOS FORMS {login = conta unis}:***

**-FORMS 1 :** [**https://docs.google.com/spreadsheets/d/1u03LafiFrastJjfIU88gNBoZpb3p5P5mKl214vZHFDQ/edit?usp=sharing**](https://docs.google.com/spreadsheets/d/1u03LafiFrastJjfIU88gNBoZpb3p5P5mKl214vZHFDQ/edit?usp=sharing)

**-FORMS 2:**

[**https://docs.google.com/spreadsheets/d/1-LTHYtmvVf0RkwSSO0z4p8GxVtBazjFxFRtkB2XLecc/edit?usp=sharing**](https://docs.google.com/spreadsheets/d/1-LTHYtmvVf0RkwSSO0z4p8GxVtBazjFxFRtkB2XLecc/edit?usp=sharing)

**Com base nessas respostas temos que realizar o diagnóstico sobre as vulnerabilidades.**

**O que é preciso ter em um diagnóstico sobre as vulnerabilidades?**

1. **Um resumo do que foi feito, o que foi achado e as soluções.**
2. **Crie uma planilha descrevendo em detalhes os potenciais riscos de segurança da informação que estão evidentes no texto. Ao elencar o risco comente também sobre os possíveis impactos.**

**Ex-1**: **Mapeamento de riscos em uma organização**

Há falta de conscientização dos usuários dos sistemas de informação no que se refere a controle e guarda de senhas. Usuários possuem permissão individual para acesso ao sistema, no entanto, há compartilhamento de senhas entre os usuários. Houve relatos de supervisores e gerentes que fornecem suas senhas para novos funcionários trabalharem até que a TI crie acesso aos sistemas. No caso de setores que trabalham com atendimento, alguns funcionários confirmaram que deixam os computadores do balcão de atendimento logados no sistema com um único usuário, que é utilizado durante todo o dia.

Para acesso a rede, a senha de acesso é padronizada para os usuários. Segundo relato, a senha é a mesma utilizada no nome do usuário, por exemplo, usuário **joao** e senha **joao**.

Alguns usuários deixam senhas de acesso aos sistemas anotadas nos computadores. Também foi identificado, por relato de funcionários, que alguns usuários utilizam senhas de funcionários que não trabalham mais naquele setor, ou que trocam de setor sem que haja a troca da senha. Também neste ponto, não há alinhamento entre o RH e a TI, pois funcionários que trocam de setor ou se desligam da empresa não são comunicados a TI, tampouco o setor possui em seus sistemas mecanismos de consulta do status dos funcionários que utilizam o sistema.

Usuários também relataram que nunca trocaram a senha após esta ser criada pela TI. Alguns poucos usuários mais conscientes afirmaram que já efetuaram a troca da senha por medida de segurança e não compartilham sua senha com outras pessoas.

Em conversa com o gerente de TI, este relatou ter consciência que os usuários compartilham senhas entre si, no entanto, afirmou não ter controle sobre isso. As senhas são criadas pela TI, criptografadas e salvas no banco de dados e informadas aos usuários, ou é solicitado que o usuário cadastre a senha na presença de algum analista da TI. O sistema permite que o usuário altere a senha a qualquer momento e também possui uma rotina para expirar a senha do usuário após determinado período, no entanto, este recurso não é utilizado.

A Infraestrutura de equipamentos e rede elétrica é muitas vezes inadequada: *hubs* e cabeamento de rede expostos, ligações elétricas em cascata utilizando estabilizadores, adaptadores e filtros de linha, emaranhado de fios, cabeamento de rede exposto, e em uma das filiais, até baterias de carro colocadas junto a computadores. Também foram observados documentos dos setores expostos sobre mesas, balcões e caixas de papelão. Também foi verificado, num primeiro momento, que um *rack* com equipamentos de rede estava exposto e com porta aberta, permitindo acesso de qualquer pessoa.

Nota-se que há procedimentos de funcionários que também podem comprometer a segurança, como informações estratégicas e confidenciais que são passadas por comunicadores instantâneos. Foi constatado durante os trabalhos que alguns usuários deixam computadores ligados e sem qualquer bloqueio de uso, inclusive com tela do sistema aberto, seja durante intervalos de almoço ou café ou mesmo para saídas rápidas.

Nos sistemas do Departamento Pessoal, as permissões são gerenciadas por grupo de pessoas. Dentro de cada grupo, os usuários possuem acesso a todas as opções do grupo, inclusive para alterar permissões de usuários. Esta falha permite que qualquer usuário altere as permissões de acesso de outros usuários ou do próprio grupo.

Não há na empresa servidores de arquivos. Assim, o usuário é responsável pela guarda de seus arquivos nos computadores. A própria TI coloca a responsabilidade de backup de arquivos para o usuário, não oferecendo rotinas para guarda ou cópias de segurança. Alguns funcionários chegam a levar consigo notebooks contendo arquivos com informações particulares da empresa.

Os sistemas não possuem logs de acesso que permitem rastrear ações dos usuários. Há alguns relatórios gerais sobre opções acessadas por usuários e log de entrada e saída do usuário no sistema. Outro ponto é que a parceira de desenvolvimento da empresa possui acesso aos códigos-fontes e uma cópia da base de dados dos sistemas da empresa. Este é um ponto importante, pois a empresa de desenvolvimento possui acesso às informações privadas da empresa. Os sistemas de informação permitem ainda entradas erradas de dados, como datas, uso incorreto de valores de números, letras no lugar de números e valores duplicados.