Santos&Gozetto

RELATÓRIO AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Diagnóstico da atividade de T.I

Resumo

Relatório e Plano de ação prognóstico para adequação das atividades de T.I e aderência como a ISO 27001 e ISO 27701

Nome da empresa:
Responsável pelo preenchimento:
Cargo:
Data de preenchimento:

Santos&Gozetto
Consultoria em Gestão e Treinamento
AGREGANDO VALOR AOS SEUS VALORES

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

1- Auditoria de sistema e legalidade de software	
Plano de Auditoria	É realizada uma auditoria para verificação de sistemas e aplicativos instalados?
	Os clientes podem acessar os resultados dessa auditora de verificação?
	São feitos testes de invasão em sua rede (local, nuvem etc.)? Se sim, com qual frequência?
	Qual o prazo de resposta para resultados dos de testes de invasão de rede? NA.
Contatos de Emergência	A empresa mantém uma lista com nomes e números de autoridades para contato em caso de emergência? Sim.
Mapeamento de Regulamentos de sistemas de Informação	A empresa pode produzir relatórios com a devida segmentação de dados, evitando que dados não pertinentes sejam inadvertidamente importados? - OK
	Qual o intervalo de tempo máximo para a empresa recuperar arquivos em caso de eventos de falha ou perda de dados? -
Propriedade Intelectual	A empresa possui políticas e procedimentos aplicados para proteger a propriedade intelectual? Em outras palavras existe software não licenciado em uso? –

Item	**Descrições das ações a serem implementadas**	**Responsável**	**Prazo**	**Status das ações**

2- Governança de Dados e equipamentos utilizados	
Administração	A empresa tem seguido algum padrão de governança e proteção de dados pessoais?
	A empresa trabalha com máquinas virtuais? Se sim, como é feito o controle de identificação?
	Para máquinas físicas, inclusive impressoras, como é feito o controle de identificação?
	A empresa utiliza mecanismos de geolocalização? Se sim, com qual finalidade?

Santos&Gozetto
Consultoria em Gestão e Treinamento
AGREGANDO VALOR AOS SEUS VALORES

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

Políticas de Retenção	A empresa possui controles técnicos de retenção de dados? Se sim, qual?
Eliminação Segura	A empresa possui processo de eliminação segura de dados? Se sim, qual? Autoparque
Vazamento de Informações	A empresa possui controles para prevenir vazamento ou comprometimento intencional/acidental de informações? Se sim, qual ou quais?
Avaliação de risco	A empresa monitora de forma contínua a segurança de sua infraestrutura? Se sim, favor descrever.

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

3- Instalações e Contas de Usuários.	
Acesso Físico	Quais os controles utilizados pela empresa para controlar o acesso físico aos equipamentos de infraestrutura de rede e telecomunicações, inclusive, caso existam, de monitoramento por câmeras?
Impressoras	As impressoras são segregadas por departamento?
	Quais departamentos possuem impressoras?
	Existem impressoras instaladas para uso comum ou de grupos de usuários?
	É feito algum tipo de controle na impressão de documentos confidenciais ou sensíveis?
Trânsito de dados	A empresa permite que os colaboradores usem pen drives, equipamentos próprios ou outros meios para gravar e transferir dados? Se sim, existem controles aplicados?
Biometria	É feita coleta de digitais? Qual a finalidade?
Câmeras	A empresa utiliza câmeras para monitoramento de áreas internas e externas?
	Onde são armazenadas das câmeras e por quanto tempo?
Controle de Usuários	
Usuário Interno	Quem autoriza a criação de uma conta (login) para um novo colaborador?

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

	Como é documentada a solicitação para a criação de uma conta (login) para um novo colaborador? É utilizado um formulário? Se sim, anexar cópia.
	Uma conta de e-mail do novo colaborador é criada em conjunto com o login de usuário? –
	Quais os dados cadastrais que o Administrador utiliza para criação de um nova conta colaborador? –
	O novo usuário assina um termo de conduta para a utilização dos sistemas da empresa? Se sim, anexar cópia-
	Na criação de uma conta para um novo colaborador o login é criado classificando o tipo de usuário com nome completo, departamento, cargo e perfil de acesso?
	Em caso do desligamento do colaborador qual o procedimento administrativo adotado em relação à conta (login) e à caixa de e-mails? –.
Controle de Perfis	
Controle de Perfis	A política da empresa é revisada para que o Administrador possa compor novos perfis e alterar os perfis existentes, incluindo e excluindo permissões de acesso e funcionalidades?
	Os perfis possuem tipo de permissão (Leitura, modificação e exclusão)?

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

4- Segurança da Informação 1	
Políticas	A empresa estabeleceu uma política de segurança da informação?
	A empresa possui termos que garantem que seus fornecedores e/ou parceiros estão aderentes à LGPD? –
Requisitos de Baseline	A empresa possui documentação sobre segurança básica para cada um dos componentes de sua infraestrutura de rede? Se sim, com qual frequência é atualizado?
Revisão de Políticas	A empresa notifica seus colaboradores todas as vezes que faz alterações relevantes em suas políticas de segurança da informação e/ou privacidade? Se sim, como fica documentado?

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

	A empresa tem controles que garantem a remoção de contas de usuários que não são mais colaboradores da mesma? Se sim, como é documentado?
	Qual o critério utilizado para dar ao colaborador a concessão de nível de acesso

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

5- Segurança de Recursos Humanos	
Treinamento e Responsabilidade	A empresa treina seus colaboradores (independentemente de suas funções) sobre a responsabilidade individual nos controles de segurança da informação?
	Os administradores de sistemas e colaboradores são educados sobre suas responsabilidades legais relacionadas à segurança e integridade dos dados dos clientes (interno ou externo)?
	A empresa documenta o conhecimento e concordância de seus colaboradores em treinamentos realizados? Se sim, favor fornecer modelo(s).
Relatórios de Acessos	
Tipo	Relatório de trilha de auditoria, com filtro de login, data e IP etc.
	Relatório de Usuários e Perfis, com filtro de login, perfil, departamento, telas e data

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

6- Gestão de Senhas	
Autenticação	Os sistemas da empresa registram a data e hora do último acesso do usuário e tarefas efetuadas?
	Qual o tempo de validade das senhas de usuário?
	Os sistemas da empresa oferecem possibilidade de troca de senha pelo usuário através da digitação da senha atual e a nova senha, a qualquer momento?

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

	Os sistemas da empresa mostram ao usuário, durante a troca de senha, alguma indicação se a senha é fraca, média ou forte, de acordo com regras previamente definidas?
	Os sistemas da empresa registram todos os acessos sem sucesso do usuário contendo nome, data e hora, IP de origem?
	Em caso de acesso remoto, os usuários digitam suas senhas em ambiente seguro (SSL/HTTPS, VPN, etc.)?
Armazenamento das Senhas	Os sistemas da empresa armazenam a senha de todos os usuários de forma criptografada?
Recuperação automática de senha	Os sistemas da empresa possibilitam a recuperação automática de senhas (esqueci minha senha)? Se sim, quais são os controles nesta operação?
	Os usuários recebem um e-mail para onde será enviado uma senha expirada que o usuário deverá modificar ao acessar o sistema?
	Os sistemas da empresa registram todas as utilizações do "esqueci minha senha"?

Registros de Auditoria	
São auditados?	Logins efetuados com e sem sucesso
	Número de tentativas de acessos com e sem sucesso
	Bloqueio de usuários por tentativas de acesso sem sucesso
	Quantidade de troca de senhas por usuário
	Quantidade de senhas expiradas e troca de senha
	Usuários que utilizaram a opção "esqueci minha senha"
	Usuários que utilizaram a opção "troca de senha"
	Pedidos/requisições aprovados pelo fornecedor/cliente/parceiro
	Usuários e perfis cadastrados e modificados pelos usuários internos e fornecedor/cliente/parceiro
	Dados cadastrados e modificados na implantação de fornecedor/cliente/parceiro
	Dados cadastrais alterados pelo próprio fornecedor/cliente/parceiro

Item	**Descrições das ações a serem implementadas**	**Responsável**	**Prazo**	**Status das ações**

7- Gerenciamento de Configuração	
Atualização de software e hardware	Toda a estrutura física e de aplicativos, servidores de aplicação, banco de dados e servidores web e outros, recebem as atualizações mais recentes assim que disponíveis?

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

Segurança	O acesso a arquivos de backup e a outros arquivos não públicos, estão restritos aos administradores e/ou auditores? Se não, a quem é facultado o acesso?
	Aplicativos como sites de servidores padrão da web, e de testes foram removidos?
	Senhas padrão foram trocadas?
	Contas padrão foram desabilitadas?
	Os recursos de segurança de estruturas de aplicativo (por exemplo, ASP, .NET, PHP etc.) estão ativados?
	Atributos como autocomplete, cache-control e outros estão configurados adequadamente para evitar o armazenamento de informações sensíveis, como senhas dentro de caches?

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

8-Segurança de Código Fonte Web

Validação de Dados	Todas as entradas de usuário são validadas no lado servidor antes de ser usadas como parte de um comando de execução?
	Entradas de usuário relacionadas a operação de acesso a arquivos são normalizadas e validadas?
	Operações de envio de arquivos, tipo e conteúdo do arquivo são verificados?
	Entradas de usuário para redirecionamento são validadas para prevenir phishing?
	Existem soluções contra-ataques nos códigos das páginas do site implementadas, bem como para as aplicações nas aplicações web?
	É feito algum teste de penetração de uma aplicação web antes de colocá-la online (ativa)?

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

9-Termos de Uso, Privacidade e Segurança

Avisos Legais	A empresa dispõe no site os termos de uso e política de privacidade? Se sim, Favor fornecer cópia.
	Os termos de uso e política de privacidade estão disponíveis para o cliente consultar e/ou baixar? É fácil identificar isto no site?

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

	Os termos de uso e política de privacidade do site da empresa estão atualizados?
	Qual a última data de atualização?
	Alterações nos termos de uso e política de privacidade são amplamente destacados no site da empresa?
	Os canais de atendimento ao cliente estão explícitos no site da empresa?
	Caso o cliente não concorde com os termos de uso e política de privacidade é oferecida alternativa para contato ou para acesso simplificado?
	É possível ao cliente solicitar o não compartilhamento de seus dados? Se sim, há prejuízo de acesso ao site como um todo?
	É possível ao cliente facilmente solicitar a remoção de seus dados? Qual o prazo para atender caso exista esta demanda? Como esta ação é documentada?

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

10-Trabalho Remoto	
	A empresa autorizou trabalho remoto?
	Foi fornecido (emprestado) equipamento aos colaboradores para o trabalho remoto?
	Algum equipamento emprestado retornou à empresa?
	Equipamento emprestado foi reconectado à rede?
	Equipamento emprestado foi reformatado antes de ser reconectado à rede?
	Foi feito um termo ou contrato para os colaboradores em trabalho remoto?
	Os colaboradores em trabalho remoto receberam algum tipo de orientação/treinamento de segurança da informação antes de se conectarem remotamente à rede corporativa?
	Foi estabelecido algum protocolo de comunicação com os colaboradores em trabalho remoto?
	Conexões remotas foram feitas com uso de VPN?

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

	Conexões remotas são monitoradas para desconexão em caso de inatividade? Se sim, após quanto tempo?
	Caso o colaborador em trabalho remoto tenha utilizado equipamento próprio (pessoal), o equipamento foi auditado antes do acesso à rede corporativa?
	Caso o colaborador em trabalho remoto tenha utilizado equipamento próprio (pessoal), o equipamento é auditado de alguma maneira?
	Caso o colaborador em trabalho remoto tenha utilizado equipamento próprio (pessoal), a empresa forneceu algum software?
	No caso do colaborador utilizando equipamento próprio, foi fornecido e exigido a instalação de um antivírus padronizado?
	Quais ferramentas eram/são utilizadas para reuniões virtuais?

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

12-Comunicação	
Interna	A empresa adota o sistema de e-mail como ferramenta de comunicação interna?
	São usados grupos de e-mail para as comunicações internas?
	Quantos são os grupos de e-mail? (Favor fornecer uma lista)
	Quem é responsável pela criação dos grupos?
	Quem é responsável pela manutenção dos grupos?
	É feita revisão periódica dos grupos?
	É feita revisão periódica da composição dos membros dos grupos?
	A empresa adota outros meios de comunicação interna, mensagens instantâneas, WhatsApp etc.? Se sim, qual ou quais.
	A empresa adota um sistema de mensagens para comunicação interna? Se sim, qual ou quais.
	No caso do uso de ferramentas de mensagens instantâneas, existe uma política de uso em vigor? Se sim, favor anexar cópia.
	Já houve algum caso de mensagem instantânea enviada a um colaborador ou grupo interno por engano? Se sim, que tipo de mensagem foi enviada e qual ação de controle de dano tomada?
	Quem tem acesso aos e-mails enviados/recebidos pelo RH?
	Circulam informações sobre colaboradores através de e-mail ou mensagens instantâneas?
	Já houve algum caso de mensagem por e-mail enviada a um colaborador ou grupo interno por engano? Se sim, que tipo de mensagem foi enviada e qual ação de controle de dano tomada?
	É utilizado malote interno para correspondência?
	Que tipos de documentos circulam no malote interno?
	Como é feito o controle de acesso ao malote interno?
	Já houve algum caso de desvio de correspondência? Se sim, que tipo de documento foi desviado e qual ação de controle de dano tomada?

Santos&Gozetto
Consultoria em Gestão e Treinamento
AGREGANDO VALOR AOS SEUS VALORES

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações

.13- Sistema Invadido	
(Crime de invasão de dispositivo de informática - Art. 154-A do Código Penal)	Quando foi a invasão? (data e horário)
	Favor fazer uma breve descrição dos eventos, num documento em separado, incluindo as seguintes informações: Tipo de invasão sofrida; Número de servidores afetados; Número de clientes (workstations) afetados;
	Os backups foram afetados?
	Foi detectado o IP de origem da invasão?
	Internamente - Foi detectada a origem ou causa da invasão?
	Houve vazamento de dados?
	Foi feita a preservação de evidências?
	As autoridades competentes foram acionadas, foi feito boletim de ocorrência?
	Em caso de ransomware ou cryptojacking, foi pago resgate?
	A empresa possui seguro para indenização de titulares de dados em caso de vazamento ou comprometimento de informações?
	A empresa possui seguro específico em caso de invasão de seus sistemas?
Ações pós invasão	Favor fazer uma breve descrição, num documento em separado, dos eventos imediatos após detectada a invasão.
	Quanto tempo demorou a recuperação dos sistemas?
	Houve perda de dados?
	Foram implementadas soluções para aumentar a segurança? Se sim, quais?
	Foi feito teste de penetração?

Santos&Gozetto
Consultoria em Gestão e Treinamento
AGREGANDO VALOR AOS SEUS VALORES

QUESTIONÁRIO DE VERIFICAÇÃO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO
QUESTIONÁRIO

Item	Descrições das ações a serem implementadas	Responsável	Prazo	Status das ações