GLOBAL
PERSONNEL CERTIFICATION SCHEME

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

HOTEL FAZENDA E SPA GLOBAL

Revisão 00

CONTEÚDO

1. INTRODUÇÃO 02

2. CONTEXTO DO SGSI 03

2.1 Partes interessadas 03
2.2 Questões internas 04
2.3 Questões externas 05

3. IDENTIFICAÇÃO, ANÁLISE E AVALIAÇÃO DO RISCO 06

3.1 Identificação do risco 07
3.1.1 Valor do ativo 07
3.1.2 Consequência das vulnerabilidades 09
3.1.3 Natureza das ameaças 10
3.2 Análise e avaliação do risco 14

4. Classificação e tratamento do risco 15

5. Declaração de aplicabilidade 19

1. Introdução

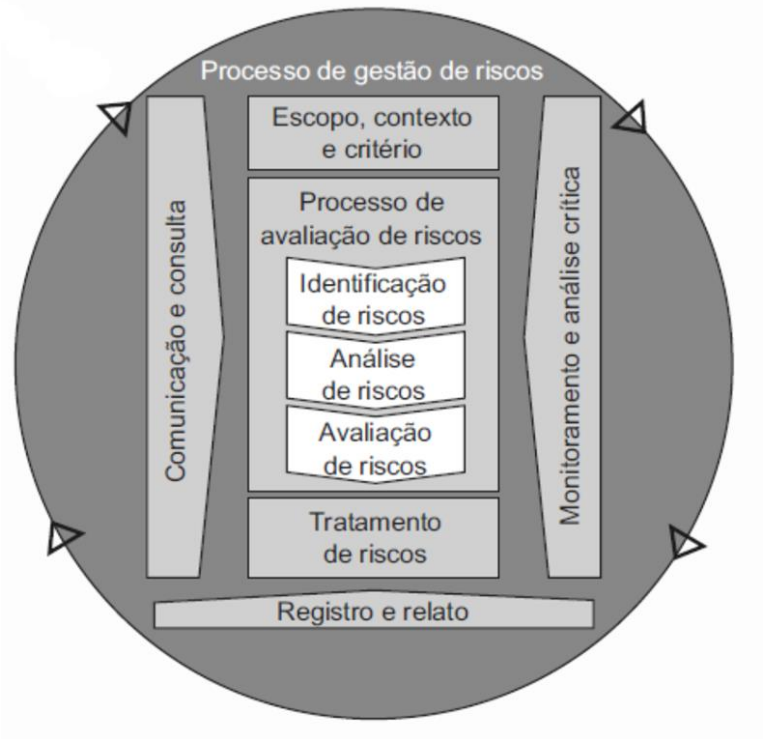
O Hotel Fazenda e Spa GLOBAL atua na prestação de serviços com alta qualidade, minimizando o impacto ambiental de suas atividades, garantindo aos clientes e funcionários espaços e locais de trabalho confortáveis e seguros, promovendo ações para garantir a Saúde e Segurança Ocupacional e a Segurança Alimentar.

Uma dimensão importante da qualidade do serviço prestado é proteger os dados pessoais das partes interessadas e proteger as informações utilizadas em todas as atividades.

Para fornecer controle e proteção eficazes das informações, o Hotel Fazenda e Spa GLOBAL implementou um Sistema de Gerenciamento de Segurança da Informação - SGSI baseado na ISO 27001 e está certificando esse sistema.

Este documento descreve o SGSI incluindo a metodologia de avaliação de segurança, as atividades e os conceitos para apoiar o SGSI, que envolvem a identificação, análise e avaliação de riscos, em conformidade com os requisitos da ISO 27001: 2013. Os objetivos de segurança e os requisitos técnicos associados propõem e implementam medidas adequadas para proteger as informações.

O desenvolvimento do SGSI é baseado no processo de avaliação de risco descrito na ISO 31000. Não é um procedimento isolado, mas depende do contexto do processo de gerenciamento de riscos, algo que requer pré-análise, pós-contramedidas e coordenação, monitoramento e feedback contínuos. A figura mostra a estrutura de avaliação de risco da ISO 31000.



A análise de risco do SGSI requer o conhecimento do contexto da organização. O contexto geral do Hotel Fazenda e Spa GLOBAL é identificado no Planejamento Estratégico e no documento de Avaliação de Riscos Corporativos. Para o SGSI, há considerações específicas relacionadas às partes interessadas, condições internas e externas que podem afetar a capacidade do sistema de alcançar os resultados esperados. Essas condições são apresentadas abaixo como o Contexto do SGSI.

2. Contexto do SGSI

As partes interessadas e as questões internas e externas relevantes para o planejamento do SGSI são indicadas a seguir.

2.1 Partes interessadas

- Clientes: Um incidente de segurança pode levar a perda ou mesmo a processo por parte de algum cliente prejudicado. Contratos devem abordar explicitamente as condições de segurança da informação requeridas pelo cliente.
- Funcionários e seus dependentes: A satisfação dos funcionários é importante para obter sua lealdade e bom desempenho quanto a segurança da informação.
- Parceiros do negócio: Podem ser agentes ou parceiros de sistemas, empresas de recrutamento ou outros. Suas reputações podem ser prejudicadas se tivermos um incidente, e podemos ser prejudicados se eles tiverem uma violação. Os contratos com alguns parceiros-chave devem ter cláusulas de SI.
- Fornecedores: Um fornecedor pode ser afetado por um incidente, podendo resultar em publicidade negativa fazendo com que eles interrompam o fornecimento. Fornecedores de dados podem deixar de confiar em nós, prejudicando a continuidade dos contratos.
- Seguradoras: Um incidente pode causar multas ou prejuízos fazendo com que tenhamos de acionar o seguro, implicando em aumento do prêmio na renovação do seguro.
- Agências governamentais: Notícias de violações podem motivar inspeções do governo ou aumento de fiscalização. Podem também implicar em multas e processos contra a empresa.
- Acionistas: Violações podem afetar o preço de nossas ações ou podem promover o descrédito nos mercados, fazendo com que a empresa perca valor.
- Direção / Gestores: A reputação profissional da empresa e da sua gestão pode ser questionada se ocorrer uma violação.
- Mídia: O interesse em Segurança da Informação está crescendo. Um incidente que for relatado sofrera publicidade negativa, resultando em perda de valor e, talvez, na perda de clientes.
- Associações de classe: Nossa participação nas Associações é importante devido ao posicionamento de liderança no mercado. Essa participação e liderança podem ser questionadas no caso de um incidente.

- Sindicatos: Podem ocorrer atritos com sindicatos durante a negociação do contrato coletivo de trabalho, podendo implicar em perda do controle de informação devido a situações de conflito com os trabalhadores ou dificuldade de acesso as instalações.

2.2 Questões internas:

Para as questões internas são a seguir abordados os itens seguintes:

- Sistemas de informação
- Cultura organizacional
- Segurança dos Recursos Humanos e Capacidades (conhecimento)
- Governança, organização, papéis e responsabilidades
- Procedimentos
- Relações contratuais com fornecedores

Sistemas de informação:
- Alguns dos nossos sistemas são antigos e devem ser substituídos. Novos sistemas serão mais complexos e, possivelmente, mais difíceis de manter. Podem ocorrer problemas de "integridade".

Cultura organizacional:
- Historicamente nossa empresa tem sido impulsionada pelas vendas. A necessidade de trazer trabalho tem superado as outras considerações, tais como confidencialidade e controle de acesso. Isso resultou em um desalinhamento entre o direcionamento estratégico e a política de SI. A integração dos controles de SI nos processos de vendas pode não ser implementada rigorosamente, especialmente nos casos de grandes encomendas.
- Relacionamentos, percepções e valores das partes interessadas internas não são conhecidos;
- Historicamente tivemos alta rotatividade de pessoal, o que significa que o pessoal poderia ter levado informação com eles.
- O pessoal tem dificuldade para entender a natureza das políticas de SI, sua importância e o papel que exercem na implantação e manutenção dessas políticas.

Segurança dos Recursos Humanos e Capacidades (conhecimento):
- Alta rotatividade de pessoal tem causado dificuldades com relação a retenção do conhecimento como, por exemplo, o suporte ao sistema de informação e relações com os clientes.
- Os funcionários são recrutados localmente e, por causa da baixa remuneração e pouca qualificação eles não tem boa situação financeira e não são bem educados. Essa situação pode deixá-los mais vulneráveis a suborno e corrupção.

Governança, organização, papéis e responsabilidades:
- Como uma empresa pequena, as responsabilidades são acumuladas por uma pequena equipe de gestão. A mesma pessoa desempenha diversos papéis na estrutura organizacional, o que não é o ideal mas é necessário.

Procedimentos:
- Alguns processos não foram documentados por causa da resistência de profissionais sêniores, que consideram a documentação como uma atividade burocrática. Esta falta de documentação pode causar problemas na continuidade das atividades.

Relações contratuais com fornecedores:
- Como um negócio de pequeno porte e novo, nosso poder de compra e de influenciar o mercado são restritos, o que nos impedirá de incluir requisitos de SI em contratos.
- Alguns fornecedores não têm contratos formais devido ao longo período no qual operam com a empresa.

2.3 Questões externas:

Para as questões externas foram considerados os itens seguintes:

- Legislação e contratos
- Cultura e pessoas
- Conectividade e tecnologia
- Localização e acesso
- Concorrência
- Condições econômicas

Legislação e contratos:
- Contrato: Os requisitos de SI estabelecidos nos contratos com os clientes e parceiros devem ser rigorosamente atendidos, o que implica numa análise prévia desses requisitos de forma a não prometer algo que não poderá ser atendido .podendo resultar em multas e perda do cliente ou do parceiro.
- Legislação de Saúde & Segurança: A legislação de saúde e segurança ocupacional deve ser rigorosamente atendida.
- Lei Geral de Proteção de Dados: A legislação de proteção de dados pessoais é mandatória e deve estar integralmente coberta pela SI e IT.
- Licenças operacionais: As licenças operacionais como, por exemplo, a Vistoria do Corpo de Bombeiros, a Autorização da Vigilância Sanitária e o Alvará de Funcionamento, devem ser integralmente atendidos e atualizados.

Cultura e pessoas
- Dados pessoais: Há uma demanda externa constante por ter acesso a dados pessoais, especialmente detalhes financeiro de cartão de crédito, endereço e data de nascimento. Incentivos significativos podem ser oferecidos aos funcionários para a coleta criminosa dessas informações, o que poderia afetar a confidencialidade.
- Atividades de hackers: Interceptação de comunicação ou acesso não autorizado são questões que sabemos importantes nos centros de serviços de TI, podendo afetar a confidencialidade e a integridade dos dados.
- Salários: Os salários em nossa indústria são baixos fazendo com o suborno possa ser uma ameaça sempre presente, pode afetar a confidencialidade e a integridade dos dados.

Conectividade e tecnologia
- Conectividade: A conectividade de TI foi interrompida algumas vezes devido a alta demanda, trazendo impacto sobre a integridade,
- Energia: Falhas nos serviços públicos são comuns. Tivemos cortes de energia devido ao aumento da demanda e infraestrutura antiga.
- Tecnologia: Os parceiros internacionais, especialmente os agentes de viagem, buscam uma operação no estado da arte, com velocidades de conexão elevadas, eficiente gerenciamento de chamados e relatórios imediatos, trazendo um forte impacto sobre compromissos contidos nas cláusulas de nível de serviço

Localização e acesso
- Localização: Nossa localização é remota, em área rural tranquila com baixa criminalidade.
- Acesso: O acesso ao local é controlado por uma portaria que verificada cada pessoa que entra nas instalações do Hotel Fazenda e Spa GLOBAL, embora o número de pessoas que circula pelas instalações é grande, podendo facilitar uma invasão intencional nas instalações do centro de serviço de TI.
- Dano ambiental: A região tem propensão a chuvas e ventos fortes mas as instalações do centro de serviço são localizadas em área bem protegida, não se antecipando problemas de inundação ou dano especifico devido a ventos e tempestade.

Concorrência
- Concorrentes: Não existem empresas próximas com as mesmas atividades.
- Pessoal: Não existe grande motivação para a retirada de funcionários visando fragilizar o trabalho no centro de TI e transferir informação dos clientes

Condições econômicas:
- Alguns dos nossos concorrentes estão sob pressão para obter novas receitas, o que os torna mais propensos a buscar uma concorrência desleal, podendo tentar acessar ilicitamente informações de nossos clientes e de nossos principais funcionários. A perda de um pessoa chave da equipe com os dados dos clientes que eles atendem pode ter grande impacto, afetando a confidencialidade e dificultando a viabilidade econômica.
- Em momentos de finanças apertadas os clientes buscam alternativas de redução de custos, o que tem resultado em grande aumento de solicitações comerciais de novos contatos. exercendo pressão sobre os recursos internos e sistemas de TI e SI.

3. Identificação, análise e avaliação do risco

A avaliação do risco, onde são identificadas as ameaças e oportunidades, é precedida das etapas de identificação do risco e de análise e classificação do risco, conforme descrito a seguir.

3.1 Identificação do risco

A identificação de riscos é o processo de encontrar, reconhecer e registrar riscos. O risco pode ser descrito como uma função de três variáveis:

- valor do ativo
- consequência das vulnerabilidades
- natureza das ameaças.

A influência externa é ameaça, e a influência interna é a vulnerabilidade. Eles atuam como entrada e fonte do incidente de segurança. O risco final também depende do valor do ativo e do ambiente.

As três variáveis serão usadas como entrada básica para uma função que avalia riscos e serão designadas como 'a' para o valor dos ativos, 't' para a probabilidade de ocorrência da ameaça e 'v' para as condições de vulnerabilidades que um sistema contém.

3.1.1 Valor do ativo

No Sistema de Gestão da Segurança da Informações do Hotel Fazenda e Spa GLOBAL, o valor dos ativos é o quanto representa o ativo que está em perigo para a organização, face aos compromissos financeiros, legais, estatutários, etc...

Os ativos podem existir em diferentes formas, tangíveis ou intangíveis, hardware ou software, serviço ou infraestrutura, etc. O SGSI considera três partes dos ativos de informações:

- a informação em si,
- as instalações que lidam com informações, e
- as pessoas que lidam com a informação.

As informações em si serão a parte principal a considerar na avaliação dos ativos dos sistemas de informação. A categorização dos ativos para realizar uma avaliação de risco mais eficiente também é importante. Os ativos podem ser categorizados com base no uso, por exemplo ativos de informação, ativos de software, ativos humanos, ativos intangíveis etc.

Na avaliação de riscos, a identificação dos ativos é uma etapa inicial, requerida para avaliar o valor do ativo e a consequência das vulnerabilidades. É necessário identificar todos os ativos e a correlação entre eles. A identificação foi conduzida da maneira abrangente.

A **Tabela 1** a seguir identifica os ativos do SGSI do Hotel Fazenda e Spa GLOBAL.

Codificação do Ativo	Identificação do Ativo	Abrangência e detalhes do Ativo	Dono do Ativo
A01-I	Informações fornecidas pelos clientes e terceiros	Vendas, atendimento, faturamento, itens comprados	Gerente Administrativo

A02-I	Informações contratuais	Contratos com clientes e fornecedores	Gerente Administrativo
A03-I	Informações financeiras e bancárias	Contas em banco, investimentos	Gerente Administrativo
A04-I	Informações de recursos humanos	Salários, contas bancárias, advertências, férias, licenças	Gerente Administrativo
A05-I	Informações de saúde e segurança	Exames admissionais, periódicos e demissionais. Exames médicos, Tratamentos clínicos e internações	Chefe do Serviço Médico
A06-I	Informações de Gestão	Planejamento estratégico, resultados financeiros	Gerente Administrativo
A07-I	Informações do hotel, da fazenda e do spa	Cardápios, estoque de produtos, rotinas de trabalho, etc...	Gerentes do Hotel, da Fazenda e do Spa
A08-I	Informações dos sistemas de gestão da qualidade, do meio ambiente, da saúde e segurança ocupacional e da SI	Auditorias, não conformidades, análise pela direção, melhorias, etc..	Gerente responsável (Qualidade, Meio Ambiente, etc..)
A09-I	Informação de TI	Controles de acessos, arquitetura do software e do hardware, comunicações	Chefe da TI
A10-P	Pessoal da administração	10 pessoas – Finanças e RH	Gerente Administrativo
A11-P	Pessoal da segurança	8 pessoas – Vigilância, rondas, acidentes, furtos, etc..	Chefe da Segurança
A12-P	Pessoal de TI	4 pessoas – Hardware e software	Chefe da TI
A13-P	Pessoal do atendimento telefônico e de internet e de vendas	4 pessoas – Vendas	Gerente Administrativo
A14-P	Pessoal da limpeza e higienização	20 pessoas - Empresa terceirizada – RH	Gerente Administrativo
A15-P	Pessoal do hotel, fazenda e spa	240 pessoas – Hotel, Fazenda e Spa	Gerentes do Hotel, da Fazenda e do Spa
A16-P	Pessoal de Gerência e Chefia	8 pessoas	Diretor
A18-E	Servidor principal	Sala da computação	Chefe da TI
A19-E	Sistema nobreak	Sala da computação	Chefe da TI
A20-S	Backup	Empresa terceirizada -	Chefe da TI
A21-E	Roteadores e cablagem	Diversos locais	Chefe da TI
A22-S	Servidor de internet e de email	Empresa terceirizada	Chefe da TI
A23-E	Terminais de acesso	Diversas salas	Gerente ou Chefe da área
A24-E	Computadores de mesa	Diversas salas	Gerente ou Chefe da área
A25-E	Laptops	Diversas salas e acesso remoto	Gerente ou Chefe da área
A26-E	Mídias móveis	Diversos salas	Chefe da TI
A27-E	Mesa telefônica	Sala da recepção do hotel	Gerente Administrativo
A28 -E	Telefones celulares	Diversas salas e acesso remoto	Gerente ou Chefe da área
A29-E	Arquivo de pastas suspensas - Financeiro	4 arquivos - Financeiro	Gerente Administrativo
A30-E	Arquivo de pastas suspensas - RH	2 arquivos - RH	Gerente Administrativo
A31-E	Arquivo de pastas suspensas – Geral	6 arquivos – Vendas, Compras, Fazenda, Hotel, Spa	Gerente Administrativo
A32-H	Clientes	Diversos, inclui agências de viagens	Gerente Administrativo
A33-H	Funcionários	Diversos, inclui familiares	Gerente Administrativo
A34-H	Fornecedores e parceiros	Diversos, inclui empresas de recrutamento	Gerente Administrativo
A35-H	Seguradoras	2 empresas - Administração	Gerente Administrativo
A36-H	Agências governamentais	Diversas - Administração	Gerente Administrativo

A37-H	Acionistas	6 pessoas	Diretor Presidente
A38-H	Direção e gestores	8 pessoas	Diretor Presidente
A39-H	Mídia	Diversas	Gerente Administração
A40-H	Associações de classe	3 associações	Diretor Presidente
A41-H	Sindicatos	1 sindicato	Gerente Administrativo
A42-I	Sistema de informação antigo	5 softwares	Chefe da TI
A43-I	Controle de vendas dos grandes clientes	50 clientes	Gerente Administrativo
A44-I	Pouco conhecimento das relações internas	Todos os funcionários	Gerente Administrativo
A45-I	Alta rotatividade do pessoal	Todos os funcionários	Gerente Administrativo
A46-I	Dificuldade para entender segurança da informação	Todos os funcionários	Chefe da TI
A47-I	Baixa remuneração pode motivar suborno	Todos os funcionários	Gerente Administrativo
A48-I	Responsabilidades exercidas por poucas pessoas	Gerentes	Diretor Presidente
A49-I	Falta de documentação de processos	Todos os processos de segurança da informação	Chefe da TI
A50-I	Fornecedores informais, sem contrato	4 fornecedores	Gerente Administrativo
A51-E	Garantir informações de atendimento da LGPD	Todos os clientes, fornecedores, etc..	Gerente Administrativo
A52-E	Controlar atividades de hackers	Acesso de todos os funcionários, clientes, fornecedores, etc...	Chefe TI
A53-E	Dificuldades de conectividade devido a sobrecarga da TI	Acesso de todos os funcionários, clientes, fornecedores, etc...	Chefe da TI
A54-E	Falhas de interrupção de energia	Equipamentos de nobreak e outros	Chefe da Manutenção
A55-E	Tecnologia desatualizada	Sistemas de TI	Chefe da TI
A56-E	Controle de acesso aos locais críticos	Todos	Chefe da Segurança
A57-E	Controle de acesso a concorrentes	Todos os concorrentes e clientes	Chefe da Segurança

3.1.2 Consequências das vulnerabilidades

Vulnerabilidade refere-se à abertura de um sistema de informações às ameaças. As vulnerabilidades do sistema geralmente são exploradas pelas ameaças potenciais identificadas.

Vulnerabilidade refere-se à fraqueza relacionada aos ativos da organização, que às vezes pode causar um incidente inesperado. Vulnerabilidade também significa falha ou fraqueza do fluxo, projeto e implementação de segurança dos sistemas que podem levar a violações ou violações da política de segurança.

As vulnerabilidades podem ser divididas em duas categorias.

- O primeiro tipo de vulnerabilidade afeta o próprio ativo, como problemas técnicos, violações do sistema etc.

- O segundo tipo é causado pelo gerenciamento insuficiente da organização em um nível superior.

Vulnerabilidades podem ser identificadas por meio de documentos, audições, entrevistas e questionários de pessoas, inspeção no local, verificador de vulnerabilidades, etc.

As vulnerabilidades de cada ativo são dependentes da natureza das ameaças existindo, enfim, uma interdependência, que tem de ser considerada ao fazer a identificação dos riscos.

3.1.3 Natureza das ameaças

As ameaças referem-se aos eventos que causam danos aos sistemas de informação em geral e serão classificados quanto a sua natureza. Uma ameaça é uma situação potencial, para uma fonte de ameaça específica, de que ela acesse, com êxito, uma vulnerabilidade específica.

Há três aspectos a serem considerados na probabilidade de ameaça:
- fonte da ameaça,
- vulnerabilidades em potencial
- controles existentes.

Para identificar fontes de ameaças, todas as ameaças em potencial para os ativos importantes devem ser reconhecidas. As fontes de ameaças podem ser categorizadas em fatores ambientais ou humanos.

Fatores ambientais como terremoto ou inundação não podem ser evitados. O usuário sempre deve considerar as ameaças ao ambiente de acordo com o ambiente de operação, mesmo que seja difícil considerá-las. Enquanto isso, os fatores humanos são mais preocupantes porque são vagantes em relação a pessoas e situações diferentes, e é mais difícil prever o comportamento humano do que desastres naturais comuns.

A forma existente de uma ameaça pode ser um ataque direto ou indireto aos sistemas, como modificação não autorizada, vazamento etc., que leva à violação da confidencialidade, integridade ou disponibilidade do sistema ou a um incidente não intencional.

Uma ameaça pode ser o resultado de um incidente externo e não controlável ou um ataque ao sistema. As ameaças são classificadas em 8 categorias principais:

- Dano físico
- Eventos naturais
- Perda de serviços essenciais
- Perturbação devido a radiação
- Compromisso de informação
- Falhas técnicas
- Ações não autorizadas

- Comprometimento de funções

Para obter um objetivo de segurança, é avaliado o impacto da ameaça em termos de Disponibilidade (A), Confidencialidade (C) e Integridade (I). A lista completa das ameaças consideradas no Sistema de Gestão da Segurança da Informação do Hotel Fazenda e Spa GLOBAL está disponível na Tabela 2.

TABELA 2 – LISTA DAS AMEAÇAS

TIPO	DETALHE	A	C	I	DESCRIÇÃO
Dano Físico	Fogo	X		X	Concentração de materiais inflamáveis ou explosivos em um ambiente confinado, pegando fogo por um evento externo ou acidente interno. Terroristas ou vândalos que obtêm acesso à propriedade para iluminar materiais inflamáveis ou explosivos direta ou indiretamente (bombas incendiárias, adulteração de dispositivos de ventilação etc.).
	Dano Causado pelo Água	X		X	Inundação devido a um vazamento ou ruptura do tubo. Terroristas ou vândalos que ganham acesso à propriedade para causar inundações nos cômodos.
	Poluição	X		X	Presença de poeira, vapores, gases corrosivos ou tóxicos no ar ambiente. Deliberar a poluição do ar ambiente, violando os dispositivos de ar condicionado ou colocando uma fonte de poluição nos cômodos.
	Acidente de Grande Porte	X		X	Evento externo ou dano ligado ao ambiente natural ou industrial próximo aos ativos e capaz de causar danos físicos muito graves. Evento externo ou dano ligado a um ato de vandalismo ou terrorismo próximo aos bens capazes de causar danos físicos muito graves.
	Destruição de Equipamento ou Mídia	X		X	Negligência ou evento acidental causando destruição de equipamento ou mídia. Pessoa que obtém acesso ao equipamento e está causando sua destruição.
Eventos Naturais	Fenômeno Climático	X		X	Condições climáticas específicas (nos limites de operação do equipamento).
	Fenômeno Sísmico	X		X	Tremor de terra ou terremoto causando vibração extrema ou provocando um desastre (maremoto).
	Fenômeno Vulcânico	X		X	Erupção vulcânica causando vibrações ou desencadeando outro desastre (maremoto).
	Fenômeno Meteorológico	X		X	Perturbação atmosférica isolada causando condições climáticas extremas. Um sabotador obtém acesso a dispositivos de proteção contra raios.
	Inundação	X		X	Rio, curso de água ou lençol freático subterrâneo, causando inundações periódicas ou excepcionais de terra por perto.
Perda de Serviço Essencial	Falha do Ar Condicionado	X			Falha, desligamento ou inadequação do serviço de ar condicionado pode fazer com que ativos que exijam refrigeração ou ventilação sejam desativados, funcionem mal ou falhem completamente. Uma pessoa pode sabotar o equipamento usado para operar o sistema de ar condicionado (cortar a água ou a fonte de alimentação, destruir o sistema).

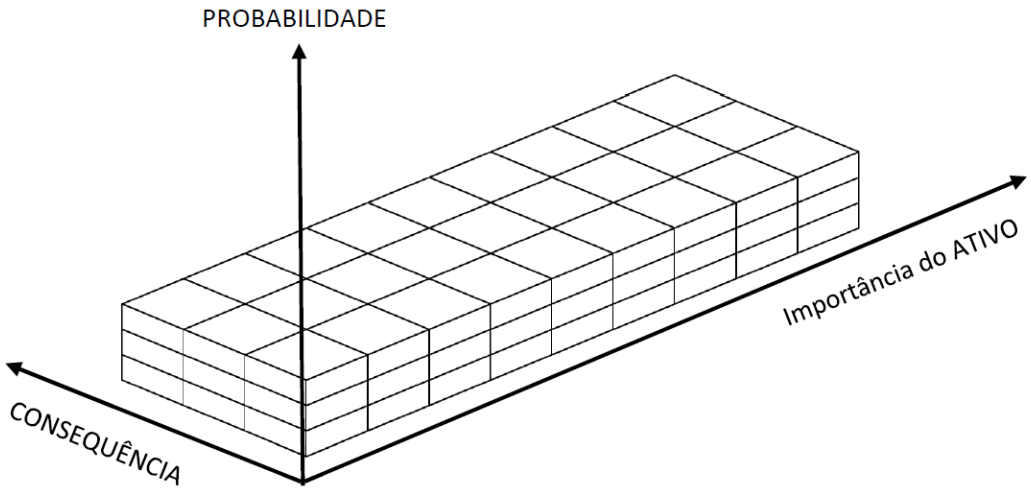
	Perda de Suprimento de Energia	X			Falha, paralisação ou dimensionamento incorreto da fonte de alimentação para os ativos decorrentes do serviço do fornecedor ou do sistema de distribuição interno. Sabotagem ou perturbação da instalação elétrica por alguém que tenha acesso ao equipamento (terminal, transformador de baixa tensão, inversor, etc.)
	Falha de Equipamento de Comunicação	X			Perturbação, desligamento ou dimensionamento incorreto dos serviços de telecomunicações (telefone, acesso à Internet, rede da Internet). Sabotagem ou perturbação da instalação de telecomunicações por alguém que tenha acesso ao equipamento de telecomunicações (terminal, PABX, quadro de distribuição, cabos externos, etc.)
Distúrbio Devido a Radiação	Radiação Eletromagnética	X		X	Interferência eletromagnética de um dispositivo interno ou externo. Pessoa que usa radiação dispersa para obstruir ou saturar as comunicações ou perturbar a operação de um aparelho.
	Radiação Térmica	X		X	Efeito térmico causado por danos ou condições climáticas excepcionais. Dispositivo que causa um efeito térmico, resultando em mau funcionamento ou destruição do equipamento.
	Pulso Eletromagnético	X		X	Danos causando um efeito eletromagnético excepcional. Pulsos eletromagnéticos de fontes nucleares.
Comprometimento da Informação	Intercepção de sinal de interferência comprometedor		X		Interferir sinais de uma fonte eletromagnética emitida pelo equipamento (por condução nos cabos de alimentação elétrica ou fios de terra ou por radiação no espaço livre). Captura desses sinais dependendo da distância do equipamento visado ou da possibilidade de conexão com cabos ou qualquer outro condutor que passe próximo ao equipamento (fenômeno de acoplamento).
	Espionagem remota	X	X	X	Ações de pessoal observáveis à distância.
	Bisbilhotar		X		Alguém conectado a um equipamento ou mídia de comunicação ou localizado dentro dos limites de cobertura de transmissão de uma comunicação pode usar equipamentos, que podem ser muito caros, para ouvir, salvar e analisar as informações transmitidas (voz ou dados).
	Roubo de mídia ou documento		X		Alguém dentro ou fora da organização acessando mídia digital ou documentos em papel com a intenção de roubar e usar as informações nelas.
	Roubo de equipamentos	X	X		Alguém dentro ou fora da organização acessando equipamentos localizados nas instalações ou transportados para fora, por ganância ou por razões estratégicas.
	Recuperação ou mídia reciclada ou descarregada		X		Recuperação de mídia eletrônica (discos rígidos, disquetes, cartuchos de backup, chaves USB, discos ZIP, discos rígidos removíveis etc.) ou cópias em papel (listas, impressões incompletas, mensagens etc.) destinadas à reciclagem e à contenção informações recuperáveis.
Comprometimento da Informação	Divulgação		X		Alguém dentro da organização que, por negligência, passa informações para outras pessoas na organização que não precisam saber ou para o exterior (o último caso geralmente tem maiores consequências).

					Alguém conscientemente passando informações dentro da organização para outras pessoas que não precisam saber ou para o exterior (o último caso geralmente tem maiores consequências).
	Dados de fontes não confiáveis	X		X	Receber dados falsos ou equipamento inadequado de fontes externas e usá-los na organização. Alguém transmitindo informações falsas para integração no sistema de informações com a intenção de desinformar o destinatário e atacar a confiabilidade do sistema ou a validade de suas informações.
	Adulteração de hardware		X		Alguém com acesso a um meio de comunicação ou equipamento instala um dispositivo de interceptação ou destruição nele.
	Adulteração de software	X	X	X	Ação não intencional envolvendo software realizado dentro ou fora da organização e resultando em corrupção ou destruição de programas ou dados, operação prejudicada do recurso ou mesmo execução de comandos no nome de um usuário sem seu conhecimento. Invasor introduz um programa ou comandos para modificar o comportamento de um programa ou adicionar um serviço não autorizado ao sistema operacional. Esse agente de ameaça pode atuar no sistema de informações durante a fase de design, pré-produção, produção, operação, transporte ou manutenção.
	Detecção de posição		X		Alguém com acesso ao equipamento usado para detectar a posição de um usuário do sistema de informação
Falhas Técnicas	Falha de equipamento	X			Evento causando falha do equipamento
	Mau funcionamento do equipamento	X			Um evento lógico ou físico que causa o mau funcionamento de um item de equipamento.
	Saturação do sistema de informação	X			Hardware, software ou recurso de rede inadequado para atender às necessidades dos usuários. Um invasor simula uma demanda intensa de recursos configurando bombardeios contínuos
	Mau funcionamento do software	X			Erro de projeto, erro de instalação ou erro operacional confirmado durante a modificação, causando execução incorreta.
	Violação da manutenção do sistema de informação	X			Falta de experiência no sistema, impossibilitando a adaptação e a atualização; por exemplo, incapacidade de corrigir um problema operacional ou responder a novas necessidades.
Ações não Autorizadas	Uso não autorizado de equipamentos	X	X	X	Uma pessoa dentro ou fora da organização acessa o sistema de informações e usa um de seus serviços para penetrá-lo, executar operações ou roubar informações.
	Cópia fraudulenta de software		X		Alguém dentro da organização faz cópias fraudulentas (também chamadas de cópias piratas) de software de pacote ou software interno.
	Uso de software falsificado ou copiado	X			Perda ou destruição de documentos comprovativos da compra de licenças ou negligência cometida pela instalação de software
	Corrupção de dados		X	X	Alguém obtém acesso ao equipamento de comunicação do sistema de informação e corrompe a transmissão de informações (interceptando, inserindo, destruindo etc.) ou tenta repetidamente acessar até obter êxito.

	Tratamento ilegal de dados		X		Uma pessoa realiza o processamento de informações que é proibido por lei ou regulamento.
Comprometi-mento de funções	Erro no uso	X	X	X	Uma pessoa comete um erro operacional, erro de entrada ou erro de utilização no hardware ou software. Alguém com direitos especiais (administração de rede, especialistas em informática, etc.) modifica as características operacionais dos recursos sem informar os usuários
	Abuso de direitos	X	X	X	Alguém acessa o sistema para modificar, excluir ou adicionar características operacionais ou realizar qualquer outra operação não autorizada possível aos titulares dessas informações.
	Falsificação de direitos	X	X	X	Uma pessoa assume a identidade de uma pessoa diferente para usar seus direitos de acesso ao sistema de informação, desinformar o destinatário, cometer uma fraude etc.
	Negação de ações			X	Uma pessoa ou entidade nega estar envolvida em uma troca com terceiros ou realizar uma operação.
	Violação de disponibilidade de pessoal	X			Ausência de pessoal qualificado ou autorizado por razões alheias ao seu controle. Ausência deliberada de pessoal qualificado ou autorizado.

3.2 Análise e avaliação do risco

Para a análise e avaliação do risco, o SGSI do Hotel fazenda e Spa GLOBAL considerou o valor do ativo, a consequência, baseada na vulnerabilidade e na natureza da ameaça e a probabilidade da ameaça ocorrer. Foi montada a Matriz de Significância apresentada a seguir.



Para obter o valor do ativo, após a identificação já processada, os ativos foram analisados e avaliados a fim de obter a categorização da sua

importância face a segurança da informação. A análise realizada de maneira qualitativa, por brainstorming, identifica a importância dos ativos, com base no nível de segurança determinado pelos três aspectos: **confidencialidade**, **integridade** e **disponibilidade**.

A classificação considera os níveis 1, 2 ou 3 para Disponibilidade (A), Confidencialidade (C) e Integridade (I), sendo o nível 3 sempre o mais crítico quanto a segurança da informação. Um ativo que deve estar disponível constantemente, tem nível de confidencialidade alto e integridade baixa será pontuado como 3, 3 e 3, sendo sua classificação final 9, soma das classificações individualizadas, constituindo-se em um ativo de grande relevância.

A análise e avaliação da consequência das vulnerabilidades é feita também por brainstorming, utilizando o melhor julgamento de uma equipe de especialistas. Dados históricos e o melhor conhecimento técnico-científico foram utilizados. A classificação

Para a análise e avaliação da natureza das ameaças foram considerados os aspectos a seguir, tomando por base a identificação das ameaças já identificada.

- Estatísticas de ameaças em relatórios de segurança anteriores.
- Coleta de dados em um ambiente prático, usando ferramentas de detecção de intrusão, verificando os arquivos de log ou outros métodos.
- Referência de fontes autorizadas que possuem bancos de dados com as ameaças mais populares.

A probabilidade de ocorrer uma ameaça foi classificada em três níveis, tomando como referência o tempo provável entre ocorrências:

- Baixa: probabilidade de ocorrer uma vez em 10 anos
- Média: probabilidade de ocorrer uma vez por ano
- Alta: probabilidade de ocorrer pelo menos uma vez por mês

A análise da probabilidade de ocorrer uma ameaça foi feita, também, por brainstorming, utilizando o melhor julgamento de uma equipe de especialistas. Dados históricos e o melhor conhecimento técnico-científico foram utilizados.

4. Classificação e Tratamento do risco

O SGSI do Hotel Fazenda e Spa GLOBAL tratou todos os riscos classificados como "significativos", levando em conta os pontos obtidos pela soma dos valores estabelecidos para o ativo, multiplicado pela probabilidade e pela consequência. A classificação assim obtida leva em conta as três dimensões que caracterizam o risco de um ativo. São considerados significativos todos

os riscos com valor superior a 20. a partir do valor do ativo, da consequência, baseada na vulnerabilidade e na natureza da ameaça e da probabilidade da ameaça ocorrer.

Os valores considerados, a classificação obtida para cada ativo e a indicação geral das ações tomadas estão incluídas na Tabela 3, a seguir.

Tabela 3 – Classificação e Tratamento do Risco

Ativo	Identificação do Ativo	Confidencialidade	Integridade	Disponibilidade	Valor do Ativo	Probabilidade	Consequência	Classificação Risco	Risco Significativo ?	Tratamento dos Riscos Significativos
A01-I	Informações fornecidas pelos clientes e terceiros	2	3	2	7	3	2	42	sim	IT11 – Controle da Informação Recebida e Gerada internamente
A02-I	Informações contratuais	2	3	2	7	3	3	63	sim	IT11 – Controle da Informação Recebida e Gerada internamente
A03-I	Informações financeiras e bancárias	2	3	1	6	3	3	54	sim	IT11 – Controle da Informação Recebida e Gerada internamente
A04-I	Informações de recursos humanos	2	3	2	7	3	3	63	sim	IT11 – Controle da Informação Recebida e Gerada internamente
A05-I	Informações de saúde e segurança	2	3	2	7	3	3	63	sim	IT11 – Controle da Informação Recebida e Gerada internamente
A06-I	Informações de Gestão	1	2	3	6	3	1	18	não	Sem tratamento específico no SGSI
A07-I	Informações do hotel, da fazenda e do spa	1	2	2	5	2	2	20	não	Sem tratamento específico no SGSI
A08-I	Informações dos sistemas de gestão da qualidade, do meio ambiente, da SSO e da SI	1	2	2	5	2	2	20	não	Sem tratamento específico no SGSI
A09-I	Informação de TI	3	3	3	9	3	3	81	sim	IT11 – Controle da Informação Recebida e Gerada internamente
A10-P	Pessoal da administração	1	2	2	5	2	2	20	não	Sem tratamento específico no SGSI
A11-P	Pessoal da segurança	2	2	3	7	2	2	28	sim	IT12 – Segurança da Informação - Controle do Pessoal
A12-P	Pessoal de TI	3	3	3	9	2	3	54	sim	IT12 – Segurança da Informação - Controle do Pessoal
A13-P	Pessoal do atendimento telefônico e de internet e de vendas	1	2	2	5	2	2	20	não	Sem tratamento específico no SGSI

A14-P	Pessoal da limpeza e higienização	2	2	2	6	3	2	36	sim	IT12 – Segurança da Informação - Controle do Pessoal
A15-P	Pessoal do hotel, fazenda e spa	1	2	2	5	2	2	20	não	Sem tratamento específico no SGSI
A16-P	Pessoal de Gerência e Chefia	2	2	2	6	3	2	36	sim	IT12 – Segurança da Informação - Controle do Pessoal
A18-E	Servidor principal	1	2	3	6	3	2	36	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A19-E	Sistema nobreak	1	2	3	6	3	2	36	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A20-S	Backup	2	2	2	6	2	2	24	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A21-E	Roteadores e cablagem	2	2	3	7	2	2	28	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A22-S	Servidor de internet e de email	1	2	3	6	3	2	36	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A23-E	Terminais de acesso	2	2	2	6	2	2	24	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A24-E	Computadores de mesa	2	1	1	4	2	3	24	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A25-E	Laptops	2	2	2	6	2	2	24	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A26-E	Mídias móveis	2	2	2	6	2	2	24	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A27-E	Mesa telefônica	1	2	2	5	2	2	20	não	Sem tratamento específico no SGSI
A28-E	Telefones celulares	2	2	2	6	2	2	24	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A29-E	Arquivo de pastas suspensas - Financeiro	3	1	1	5	2	1	10	não	Sem tratamento específico no SGSI
A30-E	Arquivo de pastas suspensas – RH	3	1	1	5	2	2	20	não	Sem tratamento específico no SGSI
A31-E	Arquivo de pastas suspensas - Geral	3	1	1	5	1	1	5	não	Sem tratamento específico no SGSI
A32-H	Clientes	2	1	1	4	2	1	8	não	Sem tratamento específico no SGSI
A33-H	Funcionários	2	1	1	4	2	2	16	não	Sem tratamento específico no SGSI
A34-H	Fornecedores e parceiros	2	3	1	6	1	3	18	não	Sem tratamento específico no SGSI
A35-H	Seguradoras	3	1	1	5	2	2	20	não	Sem tratamento específico no SGSI
A36-H	Agências governamentais	3	1	1	5	2	2	20	não	Sem tratamento específico no SGSI
A37-H	Acionistas	3	1	1	5	2	3	30	sim	IT12 – Segurança da Informação - Controle do Pessoal

A38-H	Direção e gestores	3	2	1	6	2	3	36	sim	IT12 – Segurança da Informação - Controle do Pessoal
A39-H	Mídia	3	2	1	6	2	3	26	sim	IT11 – Segurança da Informação – Recebidas e Geradas Internamente
A40-H	Associações de classe	2	2	1	5	2	2	20	não	Sem tratamento específico no SGSI
A41-H	Sindicatos	3	2	1	6	2	2	24	sim	IT11 – Segurança da Informação – Recebidas e Geradas Internamente
A42-I	Sistema de informação antigo	1	2	3	6	3	2	36	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A43-I	Controle de vendas para os grandes clientes	2	3	1	6	2	2	24	sim	IT12 – Segurança da Informação - Controle do Pessoal
A44-I	Pouco conhecimento das relações internas	2	2	1	5	2	2	20	não	Sem tratamento específico no SGSI
A45-I	Alta rotatividade do pessoal	3	2	1	6	2	2	24	sim	IT12 – Segurança da Informação - Controle do Pessoal
A46-I	Dificuldade para entender segurança da informação	3	2	2	7	2	2	28	sim	IT12 – Segurança da Informação - Controle do Pessoal
A47-I	Baixa remuneração pode motivar suborno	2	2	1	5	2	2	20	não	Sem tratamento específico no SGSI
A48-I	Responsabilidades exercidas por poucas pessoas	2	2	1	5	2	2	20	não	Sem tratamento específico no SGSI
A49-I	Falta de documentação de processos	2	2	1	5	2	2	20	não	Sem tratamento específico no SGSI
A50-I	Fornecedores informais, sem contrato	3	2	1	6	2	2	24	sim	IT11 – Segurança da Informação – Recebidas e Geradas Internamente
A51-E	Garantir informações de atendimento da LGPD	3	2	2	7	2	2	28	sim	IT12 – Segurança da Informação - Controle do Pessoal
A52-E	Controlar atividades de hackers	3	3	2	8	3	2	48	sim	IT12 – Segurança da Informação - Controle do Pessoal
A53-E	Dificuldades de conectividade devido a sobrecarga da TI	2	2	2	6	2	2	24	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A54-E	Falhas de interrupção de energia	1	1	2	4	3	3	36	sim	IT13 – Segurança da Informações – Equipamentos e Infraestrutura
A55-E	Tecnologia desatualizada	2	1	1	4	2	2	16	não	Deve ser buscada a atualização tecnológica com intuito de melhoria da produtividade
A56-E	Controle de acesso aos locais críticos	3	2	3	8	3	2	48	sim	IT12 – Segurança da Informação - Controle do Pessoal
A57-E	Controle de acesso a concorrentes	3	1	1	4	2	2	16	não	Sem tratamento específico no SGSI

Como resultado da avaliação, foram estabelecidas as seguintes Instruções Técnicas para tratar os riscos classificados como “significativos”:

- IT11 – Segurança da Informação - Controle da Informação Recebida e da Gerada Internamente
- IT12 – Segurança da Informação - Controle do Pessoal
- IT13 – Segurança da Informação – Equipamentos e Infraestrutura

Durante o processo de análise, avaliação, classificação e tratamento dos riscos foram identificados:

- origem e os controles aplicados sobre os riscos significativos
- dono do risco.

5. Declaração de Aplicabilidade

Visando compilar todos os itens relevantes do Sistema de Gestão da Segurança da Informação, face aos riscos significativos e controles estabelecidos, a Tabela 4 mostra a Declaração de Aplicabilidade.

Na Declaração de Aplicabilidade são dadas informações especificas sobre como o SGSI abordou cada um dos critérios requeridos no Anexo A da norma ISO 27001, indicando também:

- justificativa para sua inclusão ou exclusão no SGSI
- planejamento e a situação efetiva de implantação
- forma do seguimento anual

A Declaração de Aplicabilidade para o SGSI do Hotel Fazenda e Spa GLOBAL está apresentada a seguir, na Tabela 4.

TABELA 4 - Declaração de Aplicabilidade

CRITÉRIO		CONTROLE REQUERIDO	APLICÁVEL?	IMPLEMENTADO?	COMENTÁRIO E / OU JUSTIFICATIVA
5 Políticas de segurança da informação					
5.1 Orientação da Direção para segurança da informação Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.					
5.1.1	Políticas para segurança da informação	Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela Direção, publicado e comunicado para os funcionários e partes externas relevantes.	Sim	Sim	Política de SI está aprovada, publicada e comunicada
5.1.2	Análise crítica das políticas para segurança da informação	As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.	Sim	Sim	Política de SI é analisada criticamente na Revisão Anual pela Direção
6 Organização da segurança da informação					

6.1 Organização interna Objetivo: Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.					
6.1.1	Responsabilidades e papéis da segurança da informação	Todas as responsabilidades pela segurança da informação devem ser definidas e atribuídas.	Sim	Sim	Organização e papéis na SI estão definidos.
6.1.2	Segregação de funções	Funções conflitantes e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.	Sim	Sim	Funções de SI são independentes de outros setores.
6.1.3	Contato com autoridades	Contatos apropriados com autoridades relevantes devem ser mantidos.	Sim	Sim	Diretor Administração é responsável por contatos externos
6.1.4	Contato com grupos especiais	Contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação devem ser mantidos.	Sim	Sim	Chefe da TI é responsável por contatos com grupos
6.1.5	Segurança da informação no gerenciamento de projetos	Segurança da informação deve ser considerada no gerenciamento de projetos, independentemente do tipo do projeto.	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza projetos
A.6.2 Dispositivos móveis e trabalho remoto. Objetivo: Garantir a segurança das informações no trabalho remoto e no uso de dispositivos Móveis					
6.2.1	Política para o uso de dispositivo móvel	Uma política e medidas que apoiam a segurança da informação devem ser adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.	Sim	Sim	A política para uso de dispositivo móvel está indicada na IT03
6.2.2	Trabalho remoto	Uma política e medidas que apoiam a segurança da informação devem ser implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.	Não	Não	O Hotel Fazenda e Spa GLOBAL não dá acesso remoto aos dados.
7 Segurança em recursos humanos					
7.1 Antes da contratação Objetivo: Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.					
7.1.1	Seleção	Verificações do histórico devem ser realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e deve ser proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.	Sim	Sim	RH processa seleção atendendo aos critérios
7.1.2	Termos e condições de contratação	As obrigações contratuais com funcionários e partes externas devem declarar a sua responsabilidade e a da organização para a segurança da informação	Sim	Sim	São assinados contrato e termos de confidencialidade e segurança da informação
7.2 Durante a contratação Objetivo: Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.					
7.2.1	Responsabilidades da Direção	A Direção deve requerer aos funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.	Sim	Sim	Responsabilidade está estabelecida.
7.2.2	Conscientização, educação e treinamento em segurança da informação	Todos os funcionários da organização e, onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e	Sim	Sim	Treinamento é dado pelo RH e pela TI na integração do novo colaborador. É feita atualização periódica.

		procedimentos organizacionais relevantes para as suas funções			
7.2.3	Processo disciplinar	Deve existir um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.	Sim	Sim	RH controla o processo disciplinar, conforme Política de Mal-Administração
7.3 Encerramento e mudança da contratação Objetivo: Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação					
7.3.1	Responsabilidades pelo encerramento ou mudança da contratação	As responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação devem ser definidas, comunicadas aos funcionários ou partes externas e cumpridas	Sim	Sim	RH controla processo verificando autorização de desligamento e liberação prévia pela TI
8 Gestão de ativos					
8.1. Responsabilidade pelos ativos Objetivo: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.					
8.1.1	Inventário dos ativos	Os ativos associados com informação e com os recursos e processamento da informação devem ser identificados, e um inventário destes ativos deve ser estruturado e mantido.	Sim	Sim	Inventário indicado na Tabela 1 acima
8.1.2	Proprietário dos ativos	Os ativos mantidos no inventário devem ter um proprietário.	Sim	Sim	Donos dos ativos indicados na Tabela 1 acima
8.1.3	Uso aceitável dos ativos	Regras para o uso aceitável das informações, dos ativos associados com informação e os recursos de processamento da informação devem ser identificados, documentados e implementados.	Sim	Sim	Chefe da TI informa e todos assinam termo de confidencialidade e de segurança da informação.
8.1.4	Devolução de ativos	Todos os funcionários e partes externas devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.	Sim	Sim	Controle dos ativos é feita pelo Chefe da TI. Devolução é controlada na autorização de desligamento
8.2 Classificação da informação Objetivo: Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.					
8.2.1	Classificação da informação	A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.	Sim	Sim	Tabela 3 acima indica a classificação de cada ativo
8.2.2	Rótulos e tratamento da informação	Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.	Sim	Sim	É seguida a indicação da significância indicada na Tabela 3.
8.2.3	Tratamento dos ativos	Procedimentos para o tratamento dos ativos devem ser desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização.	Sim	Sim	Instruções IT11, IT12 e IT13 são aplicáveis.
8.3 Tratamento de mídias Objetivo: Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.					
8.3.1	Gerenciamento de mídias removíveis	Procedimentos devem ser implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.	Não	Não	No SGSI do Hotel Fazenda e Spa GLOBAL não é permitido o uso de midia removível

8.3.2	Descarte de mídias	As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.	Não	Não	No SGSI do Hotel Fazenda e Spa GLOBAL não é permitido o uso de midia removível
8.3.3	Transferência física de mídias	Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.	Não	Não	No SGSI do Hotel Fazenda e Spa GLOBAL não é permitido o uso de midia removível
9 Controle de acesso					
9.1 Requisitos do negócio para controle de acesso Objetivo: Limitar o acesso à informação e aos recursos de processamento da informação.					
9.1.1	Política de controle de acesso	Uma política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios	Sim	Sim	Instrução IT12 – Controle do Pessoal e do Acesso trata o assunto
9.1.2	Acesso às redes e aos serviços de rede	Os usuários devem somente receber acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.	Sim	Sim	O controle de acesso é indicado pelo Chefe da TI, autorizado pelo dono do ativo e liberado pela Gerente Administrativa
9.2 Gerenciamento de acesso do usuário Objetivo: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.					
9.2.1	Registro e cancelamento de usuário	Um processo formal de registro e cancelamento de usuário deve ser implementado para permitir atribuição dos direitos de acesso.	Sim	Sim	O controle de acesso é indicado pelo Chefe da TI, autorizado pelo dono do ativo e liberado pela Gerente Administrativa
9.2.2	Provisionamento para acesso de usuário	Um processo formal de provisionamento de acesso do usuário deve ser implementado para conceder ou revogar os direitos de acesso para todos os tipos de usuários em todos os tipos de sistemas e serviços.	Sim	Sim	O controle de acesso é indicado pelo Chefe da TI, autorizado pelo dono do ativo e liberado pela Gerente Administrativa
9.2.3	Gerenciamento de direitos de acesso privilegiado	A concessão e uso de direitos de acesso privilegiado devem ser restritos e controlados.	Sim	Sim	O controle de acesso é indicado pelo Chefe da TI, autorizado pelo dono do ativo e liberado pela Gerente Administrativa
9.2.4	Gerenciamento da informação de autenticação secreta de usuários	A concessão de informação de autenticação secreta deve ser controlada por meio de um processo de gerenciamento formal.	Sim	Sim	O Chefe da TI controla a informação de autenticação
9.2.5	Análise crítica dos direitos de acesso do usuário	Os proprietários de ativos devem analisar criticamente os direitos de acesso dos usuários, a intervalos regulares.	Sim	Sim	O controle de acesso é indicado pelo Chefe da TI, autorizado pelo dono do ativo e liberado pela Gerente Administrativa
9.2.6	Retirada ou ajuste dos direitos de acesso	Os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.	Sim	Sim	Controle dos direitos de acesso é feito pelo Chefe da TI. Retirada de direito é autorizada pelo dono do ativo e liberada pela Gerente Administrativa
9.3 Responsabilidades dos usuários Objetivo: Tornar os usuários responsáveis pela proteção das suas informações de autenticação.					

9.3.1	Uso da informação de autenticação secreta	Os usuários devem ser orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.	Sim	Sim	Usuários são treinados e assinam termo de confidencialidade e segurança da informação
9.4 Controle de acesso ao sistema e à aplicação Objetivo: Prevenir o acesso não autorizado aos sistemas e aplicações.					
9.4.1	Restrição de acesso à informação	O acesso à informação e às funções dos sistemas de aplicações deve ser restrito de acordo com a política de controle de acesso.	Sim	Sim	Controle dos direitos de acesso é feito pelo Chefe da TI, com autorização pelo dono do ativo e liberação pela Gerente Administrativa
9.4.2	Procedimentos seguros de entrada no sistema (*log-on*)	Onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (*log-on*).	Sim	Sim	Controle dos direitos de acesso é feito pelo Chefe da TI, com autorização pelo dono do ativo e liberação pela Gerente Administrativa
9.4.3	Sistema de gerenciamento de senha	Sistemas para gerenciamento de senhas devem ser interativos e devem assegurar senhas de qualidade.	Sim	Sim	Controle dos direitos de acesso é feito pelo Chefe da TI, com autorização pelo dono do ativo e liberação pela Gerente Administrativa
9.4.4	Uso de programas utilitários privilegiados	O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.	Não	Sim	Não é autorizado o uso de programas que podem sobrepor ou bypassar os controles de acesso
9.4.5	Controle de acesso ao código-fonte de programas	O acesso ao código-fonte de programa deve ser restrito.	Sim	Sim	Somente o Chefe da TI e o Analista de TI têm acesso ao código-fonte
10 Criptografia					
10.1 Controles criptográficos Objetivo: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.					
10.1.1	Política para o uso de controles criptográficos	Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.	Sim	Sim	O uso de controles criptográficos estão incluídos nos softwares de proteção e são de acesso exclusivo do Chefe da TI
10.1.2	Gerenciamento de chaves	Uma política sobre o uso, proteção e tempo de vida das chaves criptográficas deve ser desenvolvida e implementada ao longo de todo o seu ciclo de vida.	Sim	Sim	A política de controle de chaves criptográficas é controlada pelo Chefe da TI.
11 Segurança física e do ambiente					
11.1 Áreas seguras Objetivo: Prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização.					
11.1.1	Perímetro de segurança física	Perímetros de segurança devem ser definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.	Sim	Sim	O controle dos ativos é de responsabilidade do Dono do Ativo, conforme indicado na Tabela 1. Áreas de exclusão e controles de acesso são

					implementados conforme requerido
11.1.2	Controles de entrada física	As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.	Sim	Sim	Câmeras de supervisão e autorizações de acesso são controladas pelo Chefe da Segurança
11.1.3	Segurança em escritórios, salas e instalações	Deve ser projetada e aplicada segurança física para escritórios, salas e instalações.	Sim	Sim	Câmeras de supervisão e autorizações de acesso são controladas pelo Chefe da Segurança
11.1.4	Proteção contra ameaças externas e do meio ambiente	Deve ser projetada e aplicada proteção física contra desastres naturais, ataques maliciosos ou acidentes.	Sim	Sim	Câmeras de supervisão e autorizações de acesso são controladas pelo Chefe da Segurança. O Plano de Emergência (P20) atua para mitigar riscos ambientais e de saúde e segurança.
11.1.5	Trabalhando em áreas seguras	Devem ser projetados e aplicados procedimentos para o trabalho em áreas seguras.	Sim	Sim	Conforme estabelecido no SGSSO
11.1.6	Áreas de entrega e de carregamento	Pontos de acesso, como áreas de entrega e de carregamento, e outros pontos em que pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.	Sim	Sim	Chefe da Segurança tem plano de controle de acesso e é responsável por controlar.
11.2 Equipamentos Objetivo: Impedir perdas, danos, roubo, ou comprometimento de ativos e interrupção das operações da organização.					
11.2.1	Localização e proteção do equipamento	Os equipamentos devem ser protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.	Sim	Sim	Os ativos e seus Donos estão indicados na Tabela 1. Os riscos ambientais e os perigos de segurança estão analisados nos SGA e SGSSO.
11.2.2	Utilidades	Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.	Sim	Sim	A Instrução IT13 indica os controles aplicados aos equipamentos, infraestrutura e software
11.2.3	Segurança do cabeamento	O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos.	Sim	Sim	A Instrução IT13 indica os controles aplicados aos equipamentos, infraestrutura e software
11.2.4	Manutenção dos equipamentos	Os equipamentos devem ter uma manutenção correta para assegurar a sua contínua integridade e disponibilidade.	Sim	Sim	O Chefe da TI é responsável por garantir que as manutenções feitas por pessoal interno ou por contratados seja

					processada de forma adequada.
11.2.5	Remoção de ativos	Equipamentos, informações ou *software* não devem ser retirados do local sem autorização prévia.	Sim	Sim	Compete ao Dono do ativo controlar seu uso adequado, manutenção e remoção, caso necessário.
11.2.6	Segurança de equipamentos e ativos fora das dependências da organização	Devem ser tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.	Não	Não	Não existem ativos fixos que operam fora do local onde os Dono do ativo controla ou mesmo fora da organização. Telefones celulares y laptops não acessam os dados da empresa e não arquivam registros do SGSI
11.2.7	Reutilização e ou descarte seguro de equipamentos	Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.	Sim	Sim	Dono do ativo é responsável por liberar equipamento para descarte ou reutilização
11.2.8	Equipamento de usuário sem monitoração	Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada.	Não	Não	Não existem ativos do SGSI não controlados
11.2.9	Política de mesa limpa e tela limpa	Devem ser adotadas uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.	Sim	Sim	Gerente da Administração garante que política de mesa limpa está implantada e é seguida. Pessoal da Limpeza
12 Segurança nas operações					
12.1 Responsabilidades e procedimentos operacionais Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.					
12.1.1	Documentação dos procedimentos de operação	Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que necessitam deles.	Sim	Sim	Procedimentos e instruções estão online com acesso permitido para as pessoas envolvidas
12.1.2	Gestão de mudanças	Mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação devem ser controladas.	Sim	Sim	Gerente da Qualidade controla as modificações, atualiza os documentos e treina os envolvidos
12.1.3	Gestão de capacidade	A utilização dos recursos deve ser monitorada e ajustada, e as projeções devem ser feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.	Sim	Sim	Análise Crítica pela Direção estabelece planejamento e disponibiliza recursos
12.1.4	Separação dos ambientes de desenvolvimento, teste e de produção	Ambientes de desenvolvimento, teste e produção devem ser separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.	Não	Não	Não são realizados desenvolvimentos e testes
12.2 Proteção contra malware Objetivo: Assegurar que as informações e os recursos de processamento da informação estão protegidos contra malware.					
12.2.1	Controles contra malware	Devem ser implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com	Sim	Sim	Chefe da TI é responsável por manter controles

		um adequado programa de conscientização do usuário.			contra malware e outras ameaças ao sistema processamento de dados
12.3 Cópias de segurança Objetivo: Proteger contra a perda de dados.					
12.3.1	Cópias de segurança das informações	Cópias de segurança das informações, *softwares* e das imagens do sistema devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.	Sim	Sim	Chefe da TI é responsável por manter cópias de segurança arquivadas no Dropbox
12.4 Registros e monitoramento Objetivo: Registrar eventos e gerar evidências.					
12.4.1	Registros de eventos	Registros de eventos (*log*) das atividades do usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente, a intervalos regulares	Sim	Sim	Chefe da TI é responsável por estabelecer e controlar log de eventos
12.4.2	Proteção das informações dos registros de eventos (*logs*)	As informações dos registros de eventos (*log*) e seus recursos devem ser protegidos contra acesso não autorizado e adulteração.	Sim	Sim	Controle de acesso é feito pelo Chefa da TI
12.4.3	Registros de eventos (*log*) de administrador e operador	As atividades dos administradores e operadores do sistema devem ser registradas e os registros (*logs*) devem ser protegidos e analisados criticamente, a intervalos regulares.	Sim	Sim	Chefe da TI é responsável por estabelecer e controlar log de eventos
12.4.4	Sincronização dos relógios	Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados com uma fonte de tempo precisa.	Sim	Sim	Chefe da TI é responsável por estabelecer e controlar sincronização com fonte de tempo precisa
12.5 Controle de software operacional Objetivo: Assegurar a integridade dos sistemas operacionais.					
12.5.1	Instalação de *software* nos sistemas operacionais	Procedimentos para controlar a instalação de *software* em sistemas operacionais devem ser implementados	Sim	Sim	Chefe da TI é responsável por estabelecer e controlar instalação de software
12.6 Gestão de vulnerabilidades técnicas Objetivo: Prevenir a exploração de vulnerabilidades técnicas.					
12.6.1	Gestão de vulnerabilidades técnicas	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas em tempo hábil; a exposição da organização a estas vulnerabilidades deve ser avaliada e devem ser tomadas as medidas apropriadas para lidar com os riscos associados.	Sim	Sim	Vulnerabilidades técnicas dos ativos foram analisadas e consideradas na análise de risco, conforme indicado na Tabela 1
12.6.2	Restrições quanto à instalação de *software*	Regras definindo critérios para a instalação de *software* pelos usuários devem ser estabelecidas e implementadas.	Não	Não	Instalação de softwares nos ativos do SGSI são efetuadas diretamente pelo Chefe da TI
12.7 Considerações quanto à auditoria de sistemas de informação Objetivo: Minimizar o impacto das atividades de auditoria nos sistemas operacionais.					
12.7.1	Controles de auditoria de sistemas de informação	As atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar interrupção nos processos do negócio.	Sim	Sim	Gerente da Qualidade programa e controla execução das auditorias do SGSI
13 Segurança nas comunicações					

13.1 Gerenciamento da segurança em redes Objetivo: Assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam.					
13.1.1	Controles de redes	As redes devem ser gerenciadas e controladas para proteger as informações nos sistemas e aplicações.	Sim	Sim	Chefe da TI é responsável por estabelecer e gerenciar as redes
13.1.2	Segurança dos serviços de rede	Mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos	Sim	Sim	Ativos envolvidos com redes foram identificados e os Donos dos ativos indicados na Tabela 1
13.1.3	Segregação de redes	Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.	Sim	Sim	Chefe da TI é responsável por estabelecer e gerenciar as redes
13.2 Transferência de informação Objetivo: Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.					
13.2.1	Políticas e procedimentos para transferência de informações	Políticas, procedimentos e controles de transferências formais devem ser estabelecidos para proteger a transferência de informações por meio do uso de todos os tipos de recursos de comunicação.	Sim	Sim	A transferência de dados ocorrerá dentro das necessidades operativas dos processos do Hotel Fazenda e Spa GLOBAL, sendo sempre protegida pelo acesso controlado dos dados que serão transferidos. Uso de dados em nuvem fazem parte da operação regular do SGSI
13.2.2	Acordos para transferência de informações	Devem ser estabelecidos acordos para transferência segura de informações do negócio entre a organização e partes externas.	Sim	Sim	A transferência de dados para além do autorizado pelas partes envolvidas no processo não é autorizada.
13.2.3	Mensagens eletrônicas	As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas.	Sim	Sim	Mensagens eletrônicas não devem contar dados sigilosos, protegidos por acordo entre as partes
13.2.4	Acordos de confidencialidade e não divulgação	Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados, analisados criticamente e documentados.	Sim	Sim	Sempre que necessário, somente são transferidos dados conforme estabelecido em acordos e contratos.
14 Aquisição, desenvolvimento e manutenção de sistemas					
14.1 Requisitos de segurança de sistemas de informação Objetivo: Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.					
14.1.1	Análise e especificação dos requisitos de segurança da informação	Os requisitos relacionados com segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.	Sim	Sim	Dono do ativo sendo afetado ou do novo ativo estabelecem os requisitos, que são incorporados no SGSI
14.1.2	Serviços de aplicação seguros em redes públicas	As informações envolvidas nos serviços de aplicação que transitam em redes públicas devem ser protegidas de atividades	Sim	Sim	Controle de acesso e da operação das redes da dados

		fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.			públicas são controlados por senhas.
14.1.3	Protegendo as transações nos aplicativos de serviços	Informações envolvidas em transações nos aplicativos de serviços devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.	Sim	Sim	Chefe da TI controla a qualidade das transmissões e verifica adequação da infraestrutura, promovendo melhoria, quando necessário.
14.2 Segurança em processos de desenvolvimento e de suporte Objetivo: Garantir que a segurança da informação está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.					
14.2.1	Política de desenvolvimento seguro	Regras para o desenvolvimento de sistemas e *software* devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza desenvolvimento ou integração ou modificação de software
14.2.2	Procedimentos para controle de mudanças de sistemas	Mudanças em sistemas dentro do ciclo de vida de desenvolvimento devem ser controladas utilizando procedimentos formais de controle de mudanças.	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza desenvolvimento ou integração ou modificação de software
14.2.3	Análise crítica técnica das aplicações após mudanças nas plataformas operacionais	Aplicações críticas de negócios devem ser analisadas criticamente e testadas quando plataformas operacionais são mudadas, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.	Sim	Sim	Chefe da TI é responsável pelo controle
14.2.4	Restrições sobre mudanças em pacotes de *software*	Modificações em pacotes de *software* devem ser desencorajadas e devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.	Sim	Sim	Chefe da TI é responsável pelo controle
14.2.5	Princípios para projetar sistemas seguros	Princípios para projetar sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza desenvolvimento ou integração ou modificação de software
14.2.6	Ambiente seguro para desenvolvimento	As organizações devem estabelecer e proteger adequadamente os ambientes seguros de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza desenvolvimento ou integração ou modificação de software
14.2.7	Desenvolvimento terceirizado	A organização deve supervisionar e monitorar as atividades de desenvolvimento de sistemas terceirizado	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza desenvolvimento ou integração ou modificação de software
14.2.8	Teste de segurança do sistema	Testes de funcionalidade de segurança devem ser realizados durante o desenvolvimento de sistemas.	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza desenvolvimento ou integração ou modificação de software
14.2.9	Teste de aceitação de sistemas	Programas de testes de aceitação e critérios relacionados devem ser estabelecidos para novos sistemas de informação, atualizações e novas versões.	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza desenvolvimento ou integração ou

					modificação de software
14.3 Dados para teste Objetivo: Assegurar a proteção dos dados usados para teste.					
14.3.1	Proteção dos dados para teste	Os dados de teste devem ser selecionados com cuidado, protegidos e controlados	Não	Não	Hotel Fazenda e Spa GLOBAL não realiza desenvolvimento ou integração ou modificação de software
15 Relacionamento na cadeia de suprimento					
15.1 Segurança da informação na cadeia de suprimento Objetivo: Garantir a proteção dos ativos da organização que são acessados pelos fornecedores.					
15.1.1	Política de segurança da informação no relacionamento com os fornecedores	Requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização devem ser acordados com o fornecedor e documentados.	Sim	Sim	Os ativos que se relacionam com fornecedores são controlados conforme indicado na IT11
15.1.2	Identificando segurança da informação nos acordos com fornecedores	Todos os requisitos de segurança da informação relevantes devem ser estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.	Sim	Sim	Os ativos que se relacionam com fornecedores são controlados conforme indicado na IT11
15.1.3	Cadeia de suprimento na tecnologia da informação e comunicação	Acordos com fornecedores devem incluir requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação.	Sim	Sim	Os ativos que se relacionam com fornecedores são controlados conforme indicado na IT11
15.2 Gerenciamento da entrega do serviço do fornecedor Objetivo: Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.					
15.2.1	Monitoramento e análise crítica de serviços com fornecedores	A organização deve monitorar, analisar criticamente e auditar, a intervalos regulares, a entrega dos serviços executados pelos fornecedores	Sim	Sim	Gerente da Administração e o setor de compras controlam o fornecimento
15.2.2	Gerenciamento de mudanças para serviços com fornecedores	Mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos e a reavaliação de riscos.	Sim	Sim	Dono do ativo gerencia suas interfaces e Chefe da TI integra e controla o SGSI.
16 Gestão de incidentes de segurança da informação					
16.1 Gestão de incidentes de segurança da informação e melhorias Objetivo: Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.					
16.1.1	Responsabilidades e procedimentos	Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.	Sim	Sim	Incidentes de segurança são documentados como Não Conformidades e tratados imediatamente, sendo promovidas ações corretivas, quando adequado.
16.1.2	Notificação de eventos de segurança da informação	Os eventos de segurança da informação devem ser relatados por meio dos canais de gestão, o mais rapidamente possível.	Sim	Sim	O tratamento dado é por registro de não conformidade e ação

					corretiva, com análise pela gerência.
16.1.3	Notificando fragilidades de segurança da informação	Os funcionários e partes externas que usam os sistemas de informação e serviços da organização devem ser instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.	Sim	Sim	O tratamento dado é por registro de não conformidade e ação corretiva, com análise pela gerência.
16.1.4	Avaliação e decisão dos eventos de segurança da informação	Os eventos de segurança da informação devem ser avaliados, e deve ser decidido se eles são classificados como incidentes de segurança da informação.	Sim	Sim	O tratamento dado é por registro de não conformidade e ação corretiva, com análise pela gerência.
16.1.5	Resposta aos incidentes de segurança da informação	Incidentes de segurança da informação devem ser reportados de acordo com procedimentos documentados.	Sim	Sim	O tratamento dado é por registro de não conformidade e ação corretiva, com análise pela gerência.
16.1.6	Aprendendo com os incidentes de segurança da informação	Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação devem ser usados para reduzir a probabilidade ou o impacto de incidentes futuros.	Sim	Sim	O tratamento dado é por registro de não conformidade e ação corretiva, com análise pela gerência.
16.1.7	Coleta de evidências	A organização deve definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.	Sim	Sim	O tratamento dado é por registro de não conformidade e ação corretiva, com análise pela gerência.
17 Aspectos da segurança da informação na gestão da continuidade do negócio					
17.1 Continuidade da segurança da informação Objetivo: A continuidade da segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização.					
17.1.1	Planejando a continuidade da segurança da informação	A organização deve determinar seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre	Sim	Sim	A continuidade é garantida pelo arquivamento dos dados em nuvem, no Google Drive. Backup no Dropbox é efetuado com periodicidade semanal.
17.1.2	Implementando a continuidade da segurança da informação	A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.	Sim	Sim	Os dados do SGSI estão arquivados no Google Drive e podem ser acessados de diferentes locais, mantendo-se os controles de acesso implementados.
17.1.3	Verificação, análise crítica e avaliação da continuidade da segurança da informação	A organização deve verificar os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.	Sim	Sim	A auditoria interna avalia a continuidade da segurança da informação e a Análise Crítica pela Direção faz a verificação
17.2 Redundâncias Objetivo: Assegurar a disponibilidade dos recursos de processamento da informação.					
17.2.1	Disponibilidade dos recursos de processamento da informação	Os recursos de processamento da informação devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade.	Sim	Sim	Responsabilidade da Gerente Administrativo garantir disponibilidade e adequação dos recursos.

18 Conformidade					
18.1 Conformidade com requisitos legais e contratuais Objetivo: Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.					
18.1.1	Identificação da legislação aplicável e de requisitos contratuais	Todos os requisitos legislativos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a esses requisitos, devem ser explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.	Sim	Sim	Requisitos legais são controlados pela Gerente Administrativa e pelo Chefe da TI, contando com apoio externo de escritório de advocacia
18.1.2	Direitos de propriedade intelectual	Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual e sobre o uso de produtos de softwares proprietários.	Sim	Sim	Direitos de propriedade são controlados pela Gerente Administrativo
18.1.3	Proteção de registros	Registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio	Sim	Sim	Controle de registros segue o indicado no F02.
18.1.4	Proteção e privacidade de informações de identificação de pessoal	A privacidade e proteção das informações de identificação pessoal devem ser asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.	Sim	Sim	Requisitos legais relativos a Segurança da Privacidade são controlados pela Gerente Administrativo
18.1.5	Regulamentação de controles de criptografia	Controles de criptografia devem ser usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.	Sim	Sim	O uso de controles criptográficos estão incluídos nos softwares de proteção e são de acesso exclusivo do Chefe da TI
18.2 Análise crítica da segurança da informação Objetivo: Assegurar que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização.					
18.2.1	Análise crítica independente da segurança da informação	O enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, controles, políticas, processos e procedimentos para a segurança da informação) deve ser analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.	Sim	Sim	Análise Crítica é feita no ciclo anual de Revisão pela Direção
18.2.2	Conformidade com as políticas e normas de segurança da informação	Os gestores devem analisar criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.	Sim	Sim	Verificação da conformidade é feita na auditoria interna anual e na Análise Crítica pela Direção.
18.2.3	Análise crítica da conformidade técnica	Os sistemas de informação devem ser analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.	Sim	Sim	Verificação da conformidade é feita na auditoria interna anual e na Análise Crítica pela Direção.