UNIVERSIDADE NOVE DE JULHO – UNINOVE
CURSO DE TECNOLOGIA EM REDES DE COMPUTADORES E SEGURANÇA DA INFORMAÇÃO

Breno Carvalho	**R.A.: 420104657**
Camila Hipólito de Siqueira	**R.A.: 420201587**
Guilherme Antonio Ortiz Trova de Lima	**R.A.: 318202477**
Kallahan Luan Makanaky Rosa	**R.A.:920126249**
Lindenberg Felix da Silva Junior	**R.A.:919124188**

PROJETO DE SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

SÃO PAULO
2020

Breno Carvalho **R.A.: 420104657**
Camila Hipólito de Siqueira **R.A.: 420201587**
Guilherme Antonio Ortiz Trova de Lima **R.A.: 318202477**
Kallahan Luan Makanaky Rosa **R.A.:920126249**
Lindenberg Felix da Silva Junior **R.A.:919124188**

PROJETO DE SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Trabalho apresentado ao curso de Redes de Computadores e Segurança da Informação da Universidade Nove de Julho – UNINOVE

Orientado pelo professor Edson Melo de Souza

SÃO PAULO
2020

RESUMO

O projeto demonstra a aplicação de dez processos essenciais para uma empresa de tecnologia que fornece serviços a outras empresas. Além dos dez processos essenciais, foi feito uma análise de risco e um plano de continuidade de negócio.

ABSTRACT

The project demonstrates the application of ten essential processes for a technology company that provides services to other companies. In addition to the ten essential processes, a risk analysis and a business continuity plan were carried out.

Sumário

1. Introdução

Este trabalho abordará dez processos de TI criados pela SysInfo Tecnologia, uma empresa que apresenta soluções tecnológicas para outras empresas, os presentes processos foram criados para uma empresa de grande porte, que possui informações confidenciais e diferentes setores, como por exemplo, empresas de segurança patrimonial, empresas criadoras de remédios, *startups* e no contexto atual, para empresas que estão produzindo vacinas para a doença que assola o mundo.

Além dos processos, foi feito uma análise de risco, pensando novamente em grandes empresas e, e pensando em eventuais problemas, para cada processo, foi elaborado um plano de continuidade de negócios.

1.1. Metodologia

A primeiro momento foi feito uma reunião para decidirmos como iria ser a nossa empresa e qual seria o ramo de atuação, então decidimos escolher uma empresa que tivesse alguma relação com a faculdade que estamos estudando.

Em uma reunião decidimos dividir o projeto em várias partes e cada pessoa iria fazer um pouco do projeto, fizemos essa divisão e decidimos ficar realizando reuniões e conversas via WhatsApp para manter a troca de experiencia entre o grupo, após isso conversamos para decidir quais softwares que iriam ser utilizados no trabalho.

Escolhemos o Word para escrever a documentação da empresa, para fazer a tabela dos orçamentos de hardware e software, escrever as definições dos sistemas operacionais, o organograma para hierarquias da empresa, topologias de redes, RAID, Estrutura Cliente/servidor e as informações de redes da empresa, ele também foi utilizado para desenvolver toda a parte de acessibilidade e inclusão. Utilizamos o Power point para fazer a montagem de uma imagem que representa a implantação dos sistemas do jeito que faríamos em uma empresa real.

O software utilizado para fazer a planta da nossa empresa foi o Floorplanner, além disso utilizamos o Google Chrome, Youtube e matéria do Ava como ferramenta de pesquisa do nosso projeto.

Foi utilizado o método de pesquisa explorativa com a finalidade de entender na prática como funciona uma empresa que presta serviços técnicos e qual a estrutura que achávamos necessária para essa empresa,

Fizemos uma reunião para decidir como iria ser o layout da sede da nossa empresa e como seria feito o planejamento de toda nossa estrutura de rede, nessa mesma reunião decidimos qual iria ser nosso sistema operacional e começamos a conversar sobre nosso orçamento de Hardware e Software. Após essas pesquisas e reuniões decidimos colocar nosso projeto em prática.

No nosso último encontro fizemos a revisão de todo projeto visando encontrar problemas ou erros que possam ter passado despercebidos ou até mesmo algo que acabamos esquecendo de realizar no projeto.

Juntamos todo o projeto para adequação das normas da ABNT e entregamos em formato PDF para o professor.

2. Empresa

2.1. Descrição

SysInfo Tecnologia é uma empresa que foi fundada em 2015, está empresa veio para suprir as pequenas empresas no suporte de TI. **SysInfo Tecnologia** teve um crescimento absurdo a partir do ano de 2018, onde assinou vários contratos com pequenas empresas, e ganhou espaço no mercado, fornecendo suporte para redes e software e implementação de serviços em nuvem, garantindo a produtividade dos negócios.

2.2. Área de atuação da empresa

Os principais focos de atuação da **SysInfo Tecnologia** são, suporte técnico para redes de computadores, desenvolvimento de software e suporte e serviços em nuvem.

2.3. Missão

Atuar de forma segura e responsável para o cliente, suprindo todas as necessidades do cliente, fornecendo o melhor suporte do Brasil para

software em desenvolvimento, redes de computadores e serviços em nuvem.

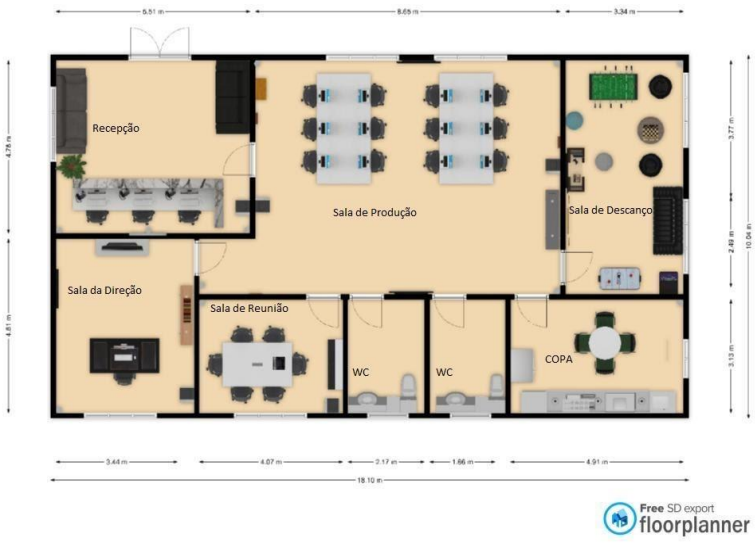
2.4. Visão

Seremos o melhor suporte do Brasil em tecnologia da informação até o próximo século.

2.5. VALORES

- Tratar os outros como queremos ser tratados;
- Integridade;
- Ser Direto;
- Gratidão e Valorização;
- Paixão; e
- Trabalhar para fazer a diferença no mundo.

2.6. Planta baixa da empresa



3. Processos de TI

3.1. Nome do Processo: Segurança em Firewall Externo

Escopo e limites: Este processo tem por finalidade garantir que toda a infraestrutura lógica da empresa tenha um grau a mais de segurança, visando manter os conceitos de confidencialidade, autenticidade e disponibilidade dos ativos da empresa. **Limite**: Este processo deve se manter em andamento em todo o funcionamento da

empresa, já que é necessário estar sempre de olho no que pode acontecer

Clientes: Usuários

Fornecedores: Suporte Técnico

Indicadores e Medidas: Como as técnicas de ataques são evoluídas e se adaptam de forma dinâmica, é necessário prover os meios para adaptar e atualizar o sistema em decorrência de tais eventos.

Requisitos de Entrada e Saída: **Entrada** - Em decorrência dos eventos de vazementos de roubos de dados e invasão de sistemas no cotidiano tecnologia, é necessário fazer relatórios e monitoramentos – **Saída**: Mecanismos de segurança para monitorarar e evitar acessos indevidos de pessoas mal intencionadas.

Documentação: Em todo final de expediente, é necessário criar um relátorio com todos os acessos dentro da rede da organização e identificar possíveis problemas.

Responsabilidades:

Processo: Segurançada de Firewall(Externa)

Dono do Processo: Gerente de TI

Papéis: Garantir o bom funcionamento e desenvolvimento do mesmo.

Responsabilidades: Fazer a distribuição e enviar os dados para análise.

3.2. Nome do Processo: Serviço de E-mail

Escopo e limites: Para o bom funcionamento e concordância com o ambiente de segurança da informação, foi criado um servidor de E-mail privado para a empresa, buscando trazer mais profissionalismo e privacidade para os funcionários da empresa., **Limite**: O processo é essêncial em todas as etapas da empresa e deve ser manter assim.

Clientes: Usuários

Fornecedores: Área de TI

Indicadores e Medidas: Como as técnicas de ataques são evoluídas e se adaptam de forma dinâmica, é necessário prover os meios para adaptar e atualizar o sistema em decorrência de tais eventos.

Requisitos de Entrada e Saída: **Entrada** - Para evitar o uso de e-mail pessoal no ambiente de trabalho, é fornecido um servidor próprio para cada funcionário, buscando novos meios para impedir tal vulnerabilidade. – **Saída**: Servidor de e-mail dentro da empresa para providenciar os meios necessários visando a disponibilidade e confidencialidade dos ativos.

Documentação: Em caso de eventuais problemas, é necessário criar um documento chamado de “Relatório de Riscos no Servidor” para listar e documentar qualquer impasse e para adicionar novos recursos.

Responsabilidades:

Processo: Servidor de E-mail

Dono do Processo: Gerente de TI

Papéis: Garantir o bom funcionamento e desenvolvimento do mesmo.

Responsabilidades: Fazer a distribuição e enviar os dados para análise.

3.3. Nome do Processo: Bloqueamento de ICMP

Escopo e limites: Para prevenir contra ataques de invasão, é necessário bloquear o protocolo de rede chamado de ICMP(PING) para impedir que possíveis ataques possam ser realizados. **Limite**: O processo é essêncial em todas as etapas da empresa e deve ser manter assim.

Clientes: Usuários

Fornecedores: Área de TI

Indicadores e Medidas: O protocolo de ICMP que possibilita o gerencimento de problemas de conexão entre diferentes hosts na rede da empresa sofre de um ataque chamando de ICMP tunneling, o qual permite a invasão por terceiros no sistema da empresa.

Requisitos de Entrada e Saída: **Entrada** - Visando problemas relacionados a Hackers na empresa, foi pensado no bloqueio da utilização de ping da empresa para qualquer host na rede.. – **Saída**: Mecanismo para bloquear a utilização do Ping nos processos da empresa.

Documentação: Para implementar tal processo, foi criado um documento para conscientizar todos os funcionários e explicar a situação e como evitar utilizar. Tal como as medidas adotadas para implementar o processo.

Responsabilidades:

Processo: ICMP Tunneling

Dono do Processo: Gerente da Área de Segurança da Informação

Papéis: Garantir o bom funcionamento e desenvolvimento do mesmo.

Responsabilidades: Conscientizar e implementar o processo.

3.4. Nome do Processo: Autenticação Biométrica

Escopo e limites: Buscando a autenticidade no ambiente empresarial, foi implementado a fiscalização da entrada de funcionários por meio da biometria. Buscando trazer resoluções efetivas no que diz respeito a entrada e saída de funcionários. **Limite**: O processo é essêncial em todas as etapas da empresa e deve ser manter assim.

Clientes: Usuários

Fornecedores: Suporte Ténico

Indicadores e Medidas: É muito simples alguém entrar em uma empresa por meio de engenharia social se a mesma não tem qualquer mecanismo de proteção física para o mesmo. Desta forma é necessário se prevenir contra ataques de egenharia social e usar mecanismo de acesso físico para prevenir contra possíveis ameaças.

Requisitos de Entrada e Saída: **Entrada** - Buscando meios para impedir a entrada de pessoas não autorizadas, notou-se a necessidade de criar controles de acesso físico na empresa. – **Saída**: Máquinas e sistemas de biometria para controle de acesso.

Documentação: Documentos para ensinar como funciona o mecanismo e como passar pelo mesmo.

Responsabilidades:

Processo: Autenticação Biometria

Dono do Processo: Gerente da area de TI

Papéis: Garantir o bom funcionamento das máquinas.

Responsabilidades: Conscientiza, implementar e tratar dos recursos necessários e atualizações.

3.5. Nome do Processo: Utilização das Impressoras

Escopo e limites: Para organizar e implementar a utilização da impressão de documentos no ambiente empresarial, é foi criado um processo que delimita a utilização e de que cada funcionário avise com antecedência quanto a utilização das empresoras. **Limite**: O processo é essêncial em todas as etapas da empresa e deve ser manter assim.

Clientes: Usuários

Fornecedores: Suporte Ténico

Indicadores e Medidas: Para manter um ambiente mais limpo e organizado, foi implementado um processo que posiciona empresoras em toda a organização de forma eficiente para imprimir os documentos necessários.

Requisitos de Entrada e Saída: **Entrada** Para imprimir qualquer documento é necessário avisar com antecedência e mostrar o grau e a fila de espera do seu arquivo. Então, para imprimir qualquer documento deve-se antes ver como esta a fila de documentos e so então, colocar o seu para imprimir. – **Saída**: Impressoras e software para gerenciar a impressão de documentos

Documentação: Política para conscientizar e ensinar como usar as impressoras e indicar quais foram os arquivos e quem fez a solicitação do mesmo.

Responsabilidades:

Processo: **Utilização das Impressoras**

Dono do Processo: Gerente da area de TI

Papéis: Garantir o bom funcionamento das máquinas.

Responsabilidades: Implementar os softwares e manter as impressoras em bom funcionamento.

3.6. Nome do Processo: Cartões NFC

Escopo e limites: Buscando fazer a identificação dos funcionários da empresa, foram criados cartões com tecnologia NFC, a qual permite a função contactless, ou seja, sem precisar o contato, para identificar por meio de um código presente no cartão, a entrada e saída dos funcionários. **Limite**: O processo é essêncial em todas as etapas da empresa e deve ser manter assim.

Clientes: Usuários

Fornecedores: Suporte Ténico

Indicadores e Medidas: A implementação dos cartões NFC é feito a partir de uma tecnologia própria da empresa buscando trazer resoluções mais eficientes para a empresa.

Requisitos de Entrada e Saída: **Entrada**:O cartão NFC serve como um cracha de funcionário que pode ser levado em qualquer lugar, mas você precisa mante-lo presente no seu corpo, rente ao rosto na hora de passar nas entradas da empresa e informar ao segurança.– **Saída**: Tecnologia NFC para fins da empresa

Documentação: Foi documentado como funciona o sistema e os procedimentos para auxiliar o processo.

Responsabilidades:

Processo: : **Instalação de Cameras de Segurança**

Dono do Processo: Gerente da area de TI

Papéis: Por meio de reuniões e planejamento, implantar a tecnologia de autenticação NFC no meio da organização.

Responsabilidades: Criar, fazer manutenção e garantir o funcionamento da tecnologia.

3.7. Nome do Processo: Instalação de Câmeras de Segurança

Escopo e limites: Para auxiliar a monitoração dos ambientes de TI da empresa, foi implementado cameras em todo o ambiente da empresa para facilitar e ver se existe algum acesso indevido ao ambiente físico da empresa. **Limite**: O processo é essêncial em todas as etapas da empresa e deve ser manter assim.

Clientes: Usuários

Fornecedores: Suporte Ténico

Indicadores e Medidas: Para poder providenciar a confidencialidade da empresa, as cameras são uma importante ferramenta para fazer essa resolução de problemas.

Requisitos de Entrada e Saída: **Entrada**: As cameras fazem a identificação facial e por meio de um banco de dados indenticar os acesso indevidos.– **Saída**: Cameras para fazer o monitoramento.

Documentação: Documento para indicar os locais e quais lugares as cameras foram implantadas.

Responsabilidades:

Processo: : **Instalação de Cameras de Segurança**

Dono do Processo: Gerente da area de TI

Papéis: Garantir o bom funcionamento das máquinas.

Responsabilidades: Instalar, configurar e fazer a manutenção das máquinas.

3.8. Nome do Processo: HONEYPOT

Escopo e limites: Para providenciar meios para proteger e adquirir dados de ataques na empresa, foi criado um honeypot que serve como uma simulação do nosso sistema, mas que é acesso pelos atacantes, ou seja, quando eles tentarem entrar no nosso servidor

principal, vão cair nessa armadilha e fazer os ataques nela. A partir disso, conseguimos adquirir os dados necessários dos ataques mais recorrentes direcionados em nossa empresa. **Limite**: Para manter o bom funcionamento dos ativos da empresa, esse processo deve se manter em funcionamento em todo o ciclo de vida empresa.

Clientes: Usuários

Fornecedores: Suporte Ténico

Indicadores e Medidas: Implantação de Honeypot para adquirir informações e para se proteger de atacantes.

Requisitos de Entrada e Saída: **Entrada**: Como os ataques cibernéticos tem se tornado uma novidade no ambiente tecnólogico, foi criado uma armadilha com a finalidade de adquirir dados e se proteger de possíveis atacantes.– **Saída**: Honeypot colocado para acesso no lugar do servidor principal

Documentação: Documentos para ensinar como usar, manter e atualizar os honeypots, assim como os relatórios conseguidos a partir disso.

Responsabilidades:

Processo: : **HONEYPOT**

Dono do Processo: Gerente da area de TI

Papéis: Trabalhar com a área de TI para criar e desenvolver o honeypot

Responsabilidades: Criar os relatórios, providenciar os métodos necessários para fazer a avaliação das ameaças mais encontradas nesse tempo de recolhimento de informações.

3.9. Nome do Processo: Acesso ao DATACENTER

Escopo e limites: Visando a segurança dos ativos da empresa, foi criado um processo que tem a finalidade de restringir o acesso a pessoas não autorizadas no ambiente do DATACENTER. Assim como, foram criados meios de acesso para gerenciar e informar os acessos ao DATACENTER **Limite**: Este processo é muito importante e deve se manter em todo o ciclo de vida da empresa.

Clientes: Usuários

Fornecedores: Suporte Ténico

Indicadores e Medidas: Implantação de sistema para impedir acessos não permitidos ao datacenter

Requisitos de Entrada e Saída: **Entrada**: Mecanismos de controle de acesso físico foram implantados na entrada do datacenter para providenciar os meios necessários para. Por meio de biometria e seguranças, foi feito essa fiscalização dos acessos.– **Saída**: Maquinas de biometria e seguranças para garantir a segurança dos ativos.

Documentação: Documentos os quais listam as presenças e acessos ao datacenter no cotidiano da empresa.

Responsabilidades:

Processo: : **Acesso ao DATACENTER**

Dono do Processo: Gerente da area de TI

Papéis: Implantar e fazer o gerenciamento dos acessos ao DATACENTER

Responsabilidades: Auxiliar na criação dos relatórios de acesso ao DATACENTER, gerir e manter o bom funcionamento dos sistemas.

3.10. Nome do Processo: Backup dos dados

Escopo e limites: Visando a segurança e disponibilidade das informações da empresa, foi implementado um processo que inclui medidas como: tempo de backup, horarios e manutenção dos backups no ambiente da empresa. Assim, todos os dados presentes na empresa devem sofrer um backup todos os dias no final do expediente e então manter os mesmos em um lugar seguro e longe de ameças. **Limite**: Este processo é muito importante e deve se manter em todo o ciclo de vida da empresa.

Clientes: Usuários

Fornecedores: Área de TI

Indicadores e Medidas: Implantação de Políticas de Backup para garantir a disponibilidade dos dados assim que necessário.

Requisitos de Entrada e Saída: **Entrada**: Utilização de softwares específicos que fazem o backup dos dados da empresa todo dia e então são enviados para um armazenamento externo da empresa para manter a segurança em caso de riscos.– **Saída**: Software de backup e empresa para fazer a movimentação dos HDs com backup.

Documentação: É documentado o horário, data dos backups e tal como sua localização atual.

Responsabilidades:

Processo: **Backup dos dados**

Dono do Processo: Gerente da área de TI

Papéis: Criar e monitorar os backups da empresa

Responsabilidades: Auxiliar no transporte, manutenção e segurança dos backups.

4. Análise de risco e continuidade de negócio

4.1. Plano de continuidade de negócios

O PCN é um documento que auxilia a organização no tratamento de desastres, tentando diminuir perdas, oferecendo mais disponibilidade, segurança, confiabilidade na TI para que suporte com valor e qualidade o negócio da organização e garantir a recuperação de um ambiente de produção, independentemente de ocorrências que suspendam suas operações e dos danos nos componentes (softwares, hardware, infraestrutura, etc.) por ele utilizados.

4.2. Qual o objetivo do Plano de Continuidade de Negócio?

Plano de Continuidade de Negócios (PCN) que tem como objetivo, garantir a continuidade das operações da empresa numa eventual indisponibilidade dos recursos que dão suporte à realização de suas operações (equipamentos, sistemas de informação, instalações, pessoal e informações).

- O Plano de Continuidade de Negócios é pensado caso haja um problema, o que fazer enquanto o problema está ativo; e após uma crise acontecer, com um plano de continuidade de negócio bem estruturado, ele será capaz de recuperar o que foi perdido por conta da crise.
- Empresas que possuem sistemas informatizados, que na atualidade, todas as empresas precisam da informática para otimizar seus serviços. Qualquer sistema é suscetível a erros e falhas. Por conta das falhas possíveis surgiu o plano de continuidade de negócios.

4.3. Justificando um plano de continuidade de negócio

Mesmo sem ter planos formais de continuidade, através dos questionamentos abaixo a alta gerência poderá saber se a sua organização está preparada para uma fatalidade operacional:

• Quais são os principais negócios da minha organização?

• Quais são os fatores de risco operacionais que podem afetar seriamente os negócios da organização?

• Qual seria o impacto nas receitas geradas pelos negócios da empresa se um ou mais fatores de risco acontecesse? • Como a empresa está preparada para lidar com o inevitável ou uma ameaça?

4.4. Relação dos planos de um PCN

Planos distintos são desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencentes ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência. Estes planos são:

• Plano de Gerenciamento de Crises PGC – Este documento tem o propósito de definir as responsabilidades de cada membro das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade. O comportamento da empresa na comunicação do fato à imprensa é um exemplo típico de tratamento dado pelo plano.

• Plano de Continuidade Operacional PCO – Tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, conseqüentemente, os impactos potenciais ao negócio. Orientar as ações diante da queda de uma conexão à Internet, exemplificam os desafios organizados pelo plano.

• Plano de Recuperação de Desastres PRD – Tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação, no menor tempo possível.

Para executar o plano com sucesso, é necessário estabelecer corretamente o mecanismo de gatilho para cada plano contínuo. Esses gatilhos são parâmetros de tolerância usados para sinalizar o início de operações de emergência para evitar ativação prematura ou atrasada.

Após o retorno à normalidade, relatórios deverão ser entregue pelas equipes que colocaram o plano em prática, ao Gestor do plano, com informações sobre o evento, apontando, por exemplo, características do objeto da contingência e etc..

4.5. Plano de continuidade de negócio para os processos

Segurança em Firewall Externo

<table>
<tr><td colspan="2">Escopo e objetivos</td></tr>
<tr><td>Garante-se que toda infraestrutura lógica tenha um grau a mais de segurança.

Visando manter os conceitos de confidencialidade, autenticidades e disponibilidade dos ativos.</td><td>- Para garantir que os firewalls sejam eficientes é necessário avaliar o que a empresa precisa (firewall de proxy, com inspeção de estado, UTM, NGFW e NGFW focado em ameaças).
- Interrupção de energia causaria grandes problemas, caso o firewall seja um software em cada computador.
- Problemas com acessibilidade, calor excessivo no ambiente, goteiras e quedas de energias, caso o firewall seja um hardware.
- - Ofertas de serviços impactadas: Todo rede computacional da empresa.</td></tr>
<tr><td colspan="2">Operações em Plano de Risco e Recuperação</td></tr>
<tr><td colspan="2">Caso de falha no software ou hardware do firewall, afetará toda empresa</td></tr>
<tr><td colspan="2">Operação 1.: Caso falte energia, é necessário ter um gerador para toda a rede</td></tr>
<tr><td>Área Operacional</td><td>Suporte</td></tr>
<tr><td>Descrição da operação</td><td>A equipe de suporte da empresa, ficará responsável por cuidar dos No Breaks, conferir se eles estão carregados e se estão conectados na rede principal.

Ficam responsáveis também por garantir que em caso de falha de energia o No Break funcionará imediatamente, sem interrupção.</td></tr>
</table>

Impacto da taxa na continuidade dos negócios	Crítico
Descrição do impacto	Todo o sistema cairá e ficará sem defesas, uma vez que algumas informações da empresa ficarão disponíveis em uma rede mundial de informações, as informações disponíveis ficará sem proteção
Estratégia de recuperação	Caso ocorra a interrupção por completo da energia, logo quando o sistema voltar a funcionar, será necessário fazer uma análise que mostrará se algum IP diferente do habitual, teve acesso às informações da empresa
Operação 2.: Recuperação de um Firewall	
Área Operacional	Equipe de TI
Descrição da operação	Se tratando de um plano de recuperação. Caso o sistema de firewall caia é necessário que ele volte a funcionar o mais rápido possível.
Impacto da taxa na continuidade dos negócios	Alta
Descrição do impacto	Sem um firewall ativo, todos os setores da empresa correm risco de invasão.
Estratégia de recuperação	Assim que o sistema voltar a funcionar é necessário restabelecer as configurações do firewall e fazer teste pra saber se ele está realmente funcionando
Funções e responsabilidades	
Setor de TI	

Gerente de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail
Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - - Também deve fazer a distribuição e enviar os dados para análise
Nome completo e Assinatura	Data

Serviço de E-mail

Escopo e objetivos

Pensando na segurança da empresa, foi criado um servidor de e-mail privado para a empresa.	Pensando na segurança da empresa, foi criado um servidor de e-mail privado para a empresa.
Operações em Plano de Risco e Recuperação	
Informações em risco	
Operação 1.: Plano de prevenção de vazamentos	
Área Operacional	Toda empresa
Descrição da operação	Para que não haja vazamentos de informação entre e-mails que saem de dentro da empresa para e-mails pessoais. Endereços de e-mails comerciais só podem trocar mensagens com e-mails confidenciais. Esses e-mail's só poderão ser acessados de máquinas com IP's registrados no sistema.
Impacto da taxa na continuidade dos negócios	Crítico
Descrição do impacto	Vazar informações confidenciais podem comprometer pesquisas, relatórios e dados pessoais dos clientes.
Estratégia de recuperação	Caso haja algum problema é necessário o funcionário elaborar um documento que chamado de "Relatório de Riscos no Servidor" para dizer e listar impasses e imprevistos que por ventura aconteceu
Funções e responsabilidades	

Setor de TI	
Gerente de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail
Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - - Também deve fazer a distribuição e enviar os dados para análise
Nome completo e Assinatura	Data

Bloqueamento de ICMP

Escopo e objetivos

Para prevenir a empresa de invasões cibernéticas, é necessário bloquear um protocolo de rede. Essencial em todas as etapas.	- Para prevenir invasões, bloqueie o protocolo de rede ICMP. - O maior risco é o funcionário não receber o treinamento adequado para saber o momento certo de bloquear e se realmente há a necessidade do bloqueio. - Ofertas de serviços impactadas: Diferentes hosts dentro da empresa.
Operações em Plano de Risco e Recuperação	
Todos os hosts da rede	
Operação 1.: Plano de Continuidade - Bloquear a rede	
Área Operacional	Todas as áreas da empresa
Descrição da operação	A equipe precisa estar bem treinada para saber quando será necessário o bloqueio.A equipe precisa saber prevenir ataques e se mesmo assim acontecer uma invasão, será necessário o bloqueio. O profissional responsável pelo bloqueio deverá trabalhar durante todo o expediente da empresa e monitorar periodicamente o sistema.
Impacto da taxa na continuidade dos negócios	Crítico
Descrição do impacto	Quando os computadores estão ligados em uma única rede e um único computador é invadido, o hacker terá acesso a toda rede, por conta de um único computador invadido.

Estratégia de recuperação	É necessário ter um backup de todos os dados da rede em outro local, fora dessa rede única usada por todos, pois caso haja a necessidade de bloquear a rede geral, a rede ficará indisponível por um tempo. Logo após a ameaça ser neutralizada a rede poderá ser desbloqueada.
Funções e responsabilidades	
Setor de TI	
Gerente da Área de Segurança da Informação	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail
Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - - Também deve fazer a distribuição e enviar os dados para análise

Nome completo e Assinatura	Data

Autenticação biométrica

Escopo e objetivos	
Para levar uma autenticidade no ambiente empresarial. Soluções efetivas para a entrada e saída de funcionários	- - Para garantir a continuidade desse processo, sempre é necessário a empresa ter energia elétrica para que os controles de acesso sempre permanecem online. - O sistema responsável pela autenticação, sempre deve estar atualizado e nunca pode ficar fora do ar. O equipamento para fazer o reconhecimento deve ser um dos melhores do mercado, para pegar todas as características de cada um. - Ofertas de serviços impactadas: Todos os usuários

Operações em Plano de Risco e Recuperação	
Autenticidade	
Operação 1.: Para garantir a continuidade do negócio - Gerador	
Área Operacional	Suporte técnico
Descrição da operação	O suporte da empresa deve ficar atento primeiramente na parte da aquisição de No Breaks. Após a aquisição mantê-los sempre com a carga máxima. Deve-se garantir que os No Breaks estejam conectados em todas as partes envolvidas com informática da empresa. O responsável pelo suporte deve garantir que mesmo em falta de energia, esse processo não pode sair fora do ar.
Impacto da taxa na continuidade dos negócios	Crítico
Descrição do impacto	Se as limitações de acesso ficarem offline por conta da falta de energia (a falta de energia também acarretará na falha das câmeras de segurança, portanto a única limitação de acesso serão os que possuem autenticação por biometria), qualquer pessoa poderá acessar qualquer área da empresa sem se identificar.
Estratégia de recuperação	Caso haja uma falha geral no sistema. É necessário que ele volte a ficar online o mais rápido possível. Em caso de falha total, o encarregado de cada setor deverá manter seus subordinados sob sua supervisão até tudo ser normalizado.

	É necessário a empresa ter total controle de seus documentos, pois após uma falha completa será necessário rever todas as informações físicas, para saber se nada está faltando.
Funções e responsabilidades	
Setor de TI	
Gerente da Área de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail
Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - Também deve fazer a distribuição e enviar os dados para análise

Nome completo e Assinatura	Data

Utilização das impressoras

Escopo e objetivos	
Organização e implementação de impressoras. Aviso com antecedência do que deve ser enviado	- Para que não haja gastos a mais com a utilização de impressoras, haverá um controle - Falta de papel ou tinta pode afetar partes importantes e documentos que realmente precisam de impressão e documentos que fossem relevantes para a empresa deixarão de ser impressos. - - Ofertas de serviços impactadas: Todos os usuários
Operações em Plano de Risco e Recuperação	
Esgotamento de recursos	
Operação 1.: Continuidade das impressões - Controle do que será impresso	

Área Operacional	Todos os setores
Descrição da operação	Os chefes de cada setor deverá saber o que será impresso, portanto apenas um computador será conectado à impressora, o computador do chefe do setor. Caso seja necessário a impressão de qualquer documento por parte de qualquer funcionário, ele deverá mostrar ao chefe.
Impacto da taxa na continuidade dos negócios	Baixo
Descrição do impacto	Imprimir documentos não pertinentes ao serviço, acarretará em uma falta de recursos.
Estratégia de recuperação	Todos da empresa deverão estar cientes da norma da empresa e em casos mais graves e que comprovem que um único funcionário usou de maneira inadequada, ele deverá ser responsabilizado pelos possíveis problemas ocasionados
Operação 2.: Continuidade do negócio - Monitoramento do recursos	
Área Operacional	Suporte técnico e líderes dos setores
Descrição da operação	Os líderes dos setores estar cientes da quantidade de recursos que ainda possuem (folha de papel, tinta, funcionalidade da impressora). Quando notar que está acabando tais recursos ou tais recursos não estão atendendo mais suas necessidades, deverão fazer um documento para o suporte técnico,

	avisando do que precisa.
Impacto da taxa na continuidade dos negócios	Baixa
Descrição do impacto	Caso haja a falta de recursos, documentos que são extremamente necessários deixarão de ser impressos. Documentos para reuniões, contratos, marketing interno voltado para divulgações de tomadas de decisões internas, por exemplo, não poderão ser impressos.
Estratégia de recuperação	Em caso de falha de comunicação e consequemente em algum setor o recursos esgote, para não acarretar em um problema maior que seria a falta de continuidade no negócio; a empresa deverá ter disponível estoque de folhas e tintas. Em caso de comunicado de última hora, o setor não parará completamente, pois a empresa já terá disponível recursos para a troca ou reposição.
Funções e responsabilidades	
Setor de TI	
Gerente de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail

Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - - Também deve fazer a distribuição e enviar os dados para análise
Nome completo e Assinatura	Data

Cartões NFC

Escopo e objetivos	
Para a identificação dos funcionários, foram criados cartões com tecnologia NFC.	- Para garantir a continuidade do serviço de NFC não pode haver falta de energia. - Deverá haver cuidado com os códigos gerados e manter o sistema sempre atualizado Ofertas de serviços impactadas: Todos os usuários
Operações em Plano de Risco e Recuperação	
Acessibilidade	

Operação 1.: Continuidade do negócio - Sistema online	
Área Operacional	Suporte Técnico
Descrição da operação	O suporte técnico deverá garantir que o sistema não saia do ar. Tanto garantido a funcionalidade na questão da energia para alimentar o sistema. O suporte técnico deverá garantir que tenha No Breaks suficientes para alimentar o sistema, também deverá garantir que tais No Breaks estejam carregados para alimentar o sistema, caso haja uma falha
Impacto da taxa na continuidade dos negócios	Crítico
Descrição do impacto	Alguns funcionários poderão não ter acesso há algumas áreas da empresa; áreas que eles precisavam ter acesso para continuar com os seus trabalhos.
Estratégia de recuperação	A energia precisa ser restabelecida. Assim que ela voltar, todo sistema NFC voltará a funcionar.
Operação 2.: Evitar problemas de acessibilidade - Manter o sistema atualizado	
Área Operacional	Equipe de TI
Descrição da operação	Para evitar problemas com informações desatualizadas, problemas com choque de informações, é necessário manter o sistema sempre atualizado. Manter o próprio sistema atualizado e manter as informações também.

Impacto da taxa na continuidade dos negócios	Média
Descrição do impacto	Caso o sistema esteja desatualizado e haja choque de informações. O TI será contatado e resolverá tais problemas
Estratégia de recuperação	Problemas causados pelo sistema desatualizado e pelo choque de informação, será solucionado quando houver a atualização e sem perdas graves para a empresa.
Funções e responsabilidades	
Setor de TI	
Gerente de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail
Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - Também deve fazer a distribuição e enviar os dados para análise

Nome completo e Assinatura	Data

Instalação de câmeras de segurança

Escopo e objetivos	
Para auxiliar a monitoração dos ambientes, foi implantando câmeras em todos os ambientes.	- Para garantir o funcionamento das câmeras é sempre necessário ter energia nas dependências do prédio. - A empresa deve ter as imagens salvas e backup de tais imagens caso seja necessário fazer a utilização das imagens. - - Ofertas de serviços impactadas: Todos os usuários
Operações em Plano de Risco e Recuperação	
Segurança	
Operação 1.: Recuperação - Imagens salvas	
Área Operacional	TI da empresa

Descrição da operação	É necessário que algum segurança da empresa, monitore as imagens em tempo real, durante todo dia. Caso note algo que não está dentro dos conformes, avisar a polícia se necessário ou informar os próprios líderes da empresa. As imagens devem ser guardadas para futuras inspeções. A imagem original deve ser guardada e também deverá ter um backup de segurança em outro lugar.
Impacto da taxa na continuidade dos negócios	Média
Descrição do impacto	Se for bem monitorado, evitará futuros problemas com roubos de informação ou com acessos a áreas restritas por funcionários que não deveriam acessá-las.
Estratégia de recuperação	Caso haja roubo de informações, as imagens estarão disponíveis para verificação. Caso perca a original, o backup estará disponível para consulta.
Funções e responsabilidades	
Setor de TI	
Gerente de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail

Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - - Também deve fazer a distribuição e enviar os dados para análise
Nome completo e Assinatura	Data

HONEYPOT

Escopo e objetivos	
Criado para proteger a empresa de ataques, o honeypot serve como um simulador do sistema, mas que é acessado pelos atacantes	- Para garantir a continuidade dos serviços esse processo tem que se manter ativo durante todo o ciclo de vida da empresa - - Ofertas de serviços impactadas: Todos os usuários
Operações em Plano de Risco e Recuperação	
Toda empresa	
Operação 1.: Continuidade do negócio - Não pode haver falhas no	

HONEYPOT	
Área Operacional	TI
Descrição da operação	Equipe de TI fará um HONEYPOT que seja funcional e atenda as necessidades da empresa. A equipe deverá ficar atenta quanto às possíveis invasões no próprio HONEYPOT. O TI também deve garantir o seu funcionamento em todos os momentos, sem falhas ou interrupções.
Impacto da taxa na continuidade dos negócios	Crítico
Descrição do impacto	Uma vez que o HONEYPOT for acessado/derrubado, o invasor entrará direto no sistema da empresa, sendo assim, terá que invadir novamente um único sistema, uma vez que a proteção foi derrubada.
Estratégia de recuperação	Caso o HONEYPOT for invadido, o melhor a fazer é retirar o sistema funcional do ar por um tempo, até um novo HONEYPOT ser feito e enquanto o servidor principal estiver inativo, a empresa fará o uso dos backups que fez ao longo dos anos.
Funções e responsabilidades	
Setor de TI	
Gerente de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser

	responsável
Detalhes de contato	*Telefone e e-mail
Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - - Também deve fazer a distribuição e enviar os dados para análise
Nome completo e Assinatura	Data

Acesso ao Data Center

Escopo e objetivos	
Com o intuito de proteger e restringir o acesso de pessoas não autorizadas	- Para garantir que não haja roubo de informações, somente pessoas autorizadas podem acessar ao DATACENTER, pessoas com identificação e em um ambiente fiscalizado por câmeras, acesso com biometria e com a tecnologia NFC.

	- - Ofertas de serviços impactadas:Todos os usuários
Operações em Plano de Risco e Recuperação	
Informações	
Operação 1.: Acesso restrito	
Área Operacional	TI e área da segurança da informação
Descrição da operação	Para acessar o DATA CENTER, primeiramente o funcionário deverá ter um motivo justificado por meio de documentos da alta diretoria. Para acessar o local o funcionário não poderá levar nada além do necessário, por tanto ela passará por uma revista antes de acessar a área. O ambiente é altamente seguro, portanto tem que haver compatibilidade com a biometria e seu cartão com tecnologia NFC. O ambiente externo é monitorado por câmeras.
Impacto da taxa na continuidade dos negócios	Crítico
Descrição do impacto	Se alguém não autorizado e mal intencionado, tiver contato com o DATA CENTER, haverá roubo de informações da empresa.

Estratégia de recuperação	É necessário a empresa ter um backup dos seus dados. Monitorar quaisquer sinais de dispositivos não reconhecidos pela área do TI, vindo daquele lugar.
Funções e responsabilidades	
Setor de TI	
Gerente de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail
Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - - Também deve fazer a distribuição e enviar os dados para análise

Nome completo e Assinatura	Data

Backup de dados

Escopo e objetivos	
Para ter uma garantia que os backups sejam feitos, serão estabelecidos padrões para eles serem realizados.	- Para garantir a continuidade dos serviços de TI o backup deve ser feito periodicamente. - Ofertas de serviços impactadas: Todos os usuários
Operações em Plano de Risco e Recuperação	
Backup	
Operação 1.: Continuidade dos negócios - Periodicidade dos backups	
Área Operacional	TI e área de segurança da informação
Descrição da operação	A equipe de TI e de segurança da informação, deverá se responsabilizar pela

	periodicidade dos backups. Também devem garantir que os backups fiquem em lugares seguros. Deverão ser responsáveis pelos softwares escolhidos. Deverão garantir que os backups funcionem quando necessário.
Impacto da taxa na continuidade dos negócios	Crítico
Descrição do impacto	Se um backup for feito e em caso de necessidade, ele não funcionar; a empresa perderá todas as suas informações.
Estratégia de recuperação	Para não acontecer da empresa perder todos os seus dados, é necessário que ao menos o penúltimo backup fique guardado. Tenha um software que possibilite isso.
Funções e responsabilidades	
Setor de TI	
Gerente de TI	
Representante	*nome do representante
Papel	*preferencialmente o líder deve ser responsável
Detalhes de contato	*Telefone e e-mail
Descrição das responsabilidades	- Deve garantir o bom funcionamento e desenvolvimento do sistema - - Também deve fazer a distribuição e enviar os dados para análise

Nome completo e Assinatura	Data

4.6. Análise de Risco

ITEM	SEVERIDADE	DESCRIÇÃO DOS RISCOS
1	24	FALTA DE ENERGIA
2	23	FALHA NO FIREWALL
3	14	INCÊNDIO
4	24	DESASTRES NATURAIS
5	13	QUEBRA DE CRIPTOGRAFIA DA REDE
6	20	SOFTWARE DESATUALIZADO
7	9	ERRO SMPT NOS SERVIDORES DE EMAIL
8	4	FALHA DE BIOMETRIA
9	14	FALHA NAS CAMÊRAS DE SEGURANÇA

10	**24**	ERRO NO SERVIDOR DE HONEYPOT
11	**22**	FALHA NO BACKUP DE DADOS
12	**4**	FALTA DE TREINAMENTO ADEQUADO

PROBABILIDADE	Matriz de Probabilidade x Impacto				
5	20	21	22	23	24
4	15	16	17	18	19
3	10	11	12	13	14
2	5	6	7	8	9
1	0	1	2	3	4
IMPACTO	1	2	3	4	5

5. Conclusão

Com esse projeto, é notório que uma empresa de grande porte, precisa ter processos bem estruturados, para garantir o bom funcionamento da empresa. E que tais processos precisam ser avaliados, para que haja continuidade dos negócios. Toda empresa também deve saber seus riscos, seus impactos e quais são as probabilidades dos acontecimentos.

6. Referências

Análise de Impacto de negócios (BIA)

https://gestaodeseguranca privada.com.br/analise-de-impacto-no-negocio-bia/

Acessado em: 12 de novembro de 2020 às 13h28.

Plano de continuidade de negócios – planejando

http://www.lyfreitas.com.br/ant/artigos_mba/artpcn.pdf

Acessado em: 12 de novembro de 2020 às 15h.

Diretrizes para a elaboração de um plano de continuidade de negócio

http://comum.rcaap.pt/bitstream/10400.26/17317/1/140313005_Tese_MSIO.pdf

Acessado em: 13 de novembro de 2020 às 16h38.

Guia de boas práticas para planos de continuidade de negócios

http://www.abrapp.org.br/GuiasManuais/guia_continuidade_negocios.pdf

Acessado em: 10 de novembro de 2020 às 14h00.