**Atlântica - University Higher Institution,**

**Disciplina:** Security Incident Response

**Autor:** Jorge Almeida

**Rua**: Fábrica da Pólvora de Barcarena, Código Postal: 2730-036 Barcarena - PT

**Security Incident no Segmento Telecom**

**Dezembro**

**2019**

Dimensão & Estrutura New Connect Telecom

Iremos tratar neste trabalho os **Security Incident** da empresa New Connect Telecom, onde a mesma atua no mercado de telecomunicações no Brasil.

A mesma está situada no Distrito de Pernambuco a sua sede no conselho de Recife, Possuir mais de 10 anos no mercado de prestações de serviços no segmento de provedor de internet, com cerca de 10mil assinantes ativos, atendendo a todos os perfis necessários de clientes, sendo eles Físicos e Jurídicos, abrangendo as regiões norte e sul de Recife.

Com uma estrutura organizacional bem atípica a sua categoria. Uma pequena empresa, composta por 30 funcionários, dentre eles, alguns seguem nas atividades operacionais da empresa e outra parte no segmento administrativo.

A mesma possuir Técnicos habilitados para o exercício de instalações em seu contexto operacional.

Trazendo uma pouco sobre a estrutura da empresa, a mesma possuir cinco Sócios-Gerentes, ao qual cada sócio estão designados a tomarem conta, de determinadas áreas dentro da empresa.

A empresa é subdividida em duas etapas sendo elas: a parte Operacional e Administrativa; Na Parte Operacional está vinculado com o Sócio Saulo Rogério e Claudio Roberto, sendo que o Saulo Rogério toma conta dos técnicos de campo, aos quais estão designados a realizações de reparos e instalações, onde que abaixo de suas ordens está os supervisores que coordenam diretamente as equipas de campo.

Já o Claudio Roberto: está responsável pelo parque tecnológico da empresa, pelos reparos dos equipamentos, instalações de novos equipamentos e suporte administrativamente mediante as solicitações, neste caso está classificado como IT Manager da empresa.

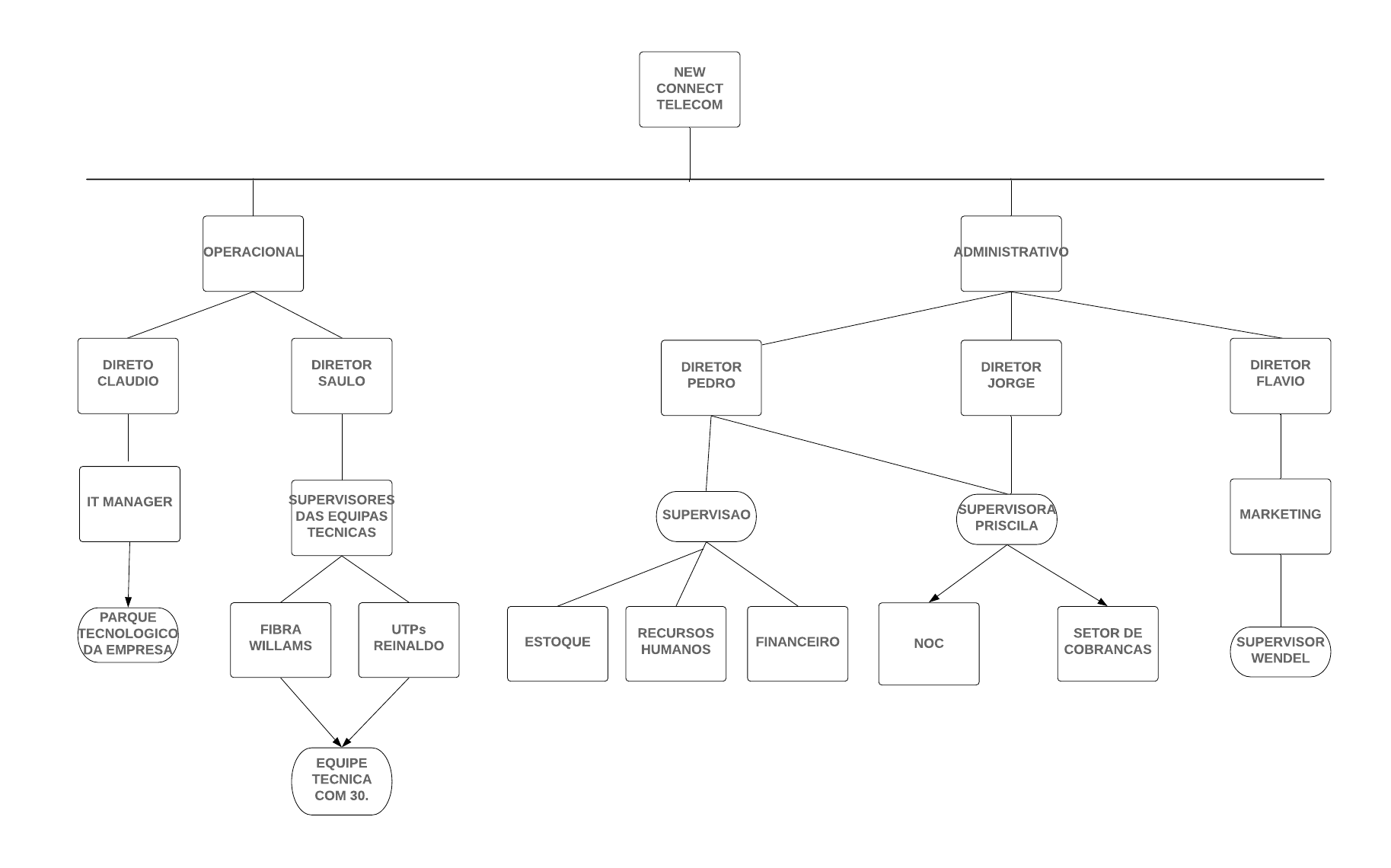
Na Parte Administrativa: Está responsáveis o Flavio pelo setor de Marketing onde preservar e divulgar a imagem da empresa, que abaixo de suas coordenadas está o supervisor e os funcionários do setor. Na Parte Financeira, RH e Estoque está uma supervisora sendo instruída e o sócio reportado é o Pedro Arruda, contudo Existe o Setor de Cobrança e o Núcleo de Atendimento que é o NOC, que está responsável é o Jorge Almeida, contudo existe uma supervisora que gerencia todos os requisitos dos setores (Noc e Cobrança). Sendo um dos carros chefes da empresa, principalmente o NOC, onde está voltado a relacionamento com o cliente, no quesito de atendimento e aberturas de ocorrências.

Neste setor há Telas de monitoramentos que avisam em tempo real, quedas de serviços requisitados por cliente residenciais ou empresariais. Ajudando na sintonia com o setor de operações para viabilizar os reparos em tempo hábil. Existe atendente que estão preparados e capacitados para gerenciar conflitos em momentos de instabilidades de alguma área afetada; A empresa é composta em seu parque tecnológica com mais de 10 servidores para atendimento de qualidade e escalabilidade de seus clientes, trabalhando com redundância em suas estações POP para não haver indisponibilidade.

Iremos agora abaixo descrever os ativos da empresa para manter os serviços aos clientes sempre disponíveis.

|  |  |  |
| --- | --- | --- |
| **RELAÇÃO DOS ATIVOS NEW CONENCT** | | |
| **ATIVOS** | **SETORES** | **QUANT** |
| NOTEBOOKS | NOC | 4 |
| TV DE MONITORAMENTO | NOC | 6 |
| TELEFONES VIA IP | NOC | 4 |
| NOTEBOOKS | RH | 2 |
| TELEFONES VIA IP | RH | 2 |
| NOTEBOOKS | ESTOQUE | 1 |
| TELEFONES VIA IP | ESTOQUE | 1 |
| TELEFONES VIA IP | COBRANCA | 1 |
| NOTEBOOKS | COBRANCA | 2 |
| NOTEBOOKS | MARKETING | 2 |
| TELEFONES VIA IP | MARKETING | 1 |
| SERVIDORES | CENTRAL | 3 |
| NOBREAK | CENTRAL | 3 |
| LINKS IPS | CENTRAL | 4 |
| CDN´S | CENTRAL | 4 |
| REDUDANCIA | CENTRAL | 2 |
| FIREWALL | CENTRAL | 1 |
| OLT FIBRAS | CENTRAL | 1 |
| SOFTWARE DE GERENCIAMENTO DE REDE ZABIX | CENTRAL | 1 |
| SOFTWARE DE GERENCIAMENTO EMPRESARIAL SGP | CENTRAL | 1 |

**Ativos New Conenct - Figura 1**

**Estrutura Organizacional**

Iremos Exemplicar em formar de Organograma a estrutura operacional e administrativa da empresa New Connect Telecom

**Estrutura Organizacional New Telecom - Figura 2**

**Desenho de um processo de gestão de incidentes de segurança**

Foram tabelados os principais incidentes, dentro da empresa New Connect Telecom. Entre eles aqueles que podem de forma brusca para a funcionalidade de todo o serviço da empresa, se não for reparado em tempo hábil.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gestão de Incidentes de Segurança | | | | |
|  |  |  |  |  |
| **Ativos** | **Ameaças** | **Vulnerabilidades** | **Riscos** | **Controles** |
| **SERVIDORES CDN´S** | INVAÇÃO;QUEDA DO CIRCUITO; | DDOS;MALWARE; | SERVIÇOS DE ACESSOS INDIPOSNIVEIS; | APLICAÇÃO DE ATUALIZAÇÕES DO SO´s |
| ROMPIMENTO DE FIBRA; FALTA DE ENREGIA | PHINSHING; UPDATES | CLIENTES NÃO AUTENTICAM NO SERVIDOR CLOUD; | IMPLEMENTAÇÃO FIREWALL COMPORTAMENTAIS COMO IDS E IPS |
|  |  | EMPRESA NÃO FUNCIONA. | INSTALAÇÃO DE DUPLA ABORDAGEM DE FIBRAS E GERADORES |
| **LINK´S DE DADOS** | ROMPIMENTOS DE FIBRA; SERVIÇOS EM POSTES | ATENUAÇÃO; | SERVIÇOS DE ACESSOS INDIPOSNIVEIS; | INSTALAÇÃO DE DUPLA ABORDAGEM DE FIBRAS |
| INDISPONIBILIDADE DO SERVIÇO POR PARTE DA | DDOS;ATAQUES ATRAVES DE | CLIENTES NÃO AUTENTICAM NO SERVIDOR CLOUD; | CONTRATAÇÃO DE SERVIÇOS DE REDUDANCIAS DE OUTRAS OPERADORAS |
| EMPRESA CONTRATADA; ATAQUES DE HACK´S | DNS | EMPRESA NÃO FUNCIONA. |  |
| **SOFTWARE DE GESTÃO DE REDES SGP** | SERVIDOR CLOUD FORA DO AR; SEM ACESSO A LINK | DDOS; HANSON; PHINSHING | CLIENTES NÃO AUTENTICAM NO SERVIDOR CLOUD; | APLICAÇÃO ACESSOS DE AUTENTICAÇÕES LOCAIS |
| DE DADOS; INDISPONIBILIDADE DA REDE LOCAL |  | EMPRESA NÃO ACESSAR DADOS DOS CLILENTES | ADCIONAR LINHA BACKUP DE OUTRA OPERADORA COM OUTRA ROTAR |
|  |  | SETORES ADM. NÃO FUNCIONA |  |
|  |  |  | TER REDUDANCIA DE SERVIDORES ESPELHAMENTOS |
| **TELEFONES IP´S** | PROBLEMA NA PRESTADORA DO SERVICO | ATAQUES DDOS | SETORES NÃO COMUNICA-SE | CONTROLES DE ACESSOS LOCAIS, PARA INIBIR VIRUS NA REDE |
| PROBLEMAS NA REDE LOCAL | ATIVOS DANIFICADOS | CLIENTES NÃO COMUNICAR-SE COM A EMPRESA | DUBLA ABORDAGEM DE LINKS |
| FALTA DE LINK OU VARIAÇÃO NA CONECÇÃO | VIRUS NA REDE LOCAL |  | TER TELEMOVEIS DISPONIVEIS PARA DETERMINADAS EVENTUALIDADES |

**Gestão de Incidentes de Segurança- Tabela1**

**Procedimento de Classificação e Atribuição de Prioridades**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **CLASSIFICAÇÃO DE EVENTOS** | | | | **TIPO DO EVENTO** | **DESCRIÇÃO** | | | **LINK DE DADOS** | **DETECTADO A INDISPONIBILIDADE** | | | **DOS SERVICOS DE DADOS** | | | **MANUTENÇÃO DOS POSTES** | **NÃO TOMARAM OS DEVIDOS** | | | **CUIDADOS FIBRA ATENUOU** | | |  |  |  | | **CLASSECIFICAÇÃO DE INCIDENTES** | | | | **CLASSE DO INCIDENTE** | **TIPO DO INCIDENTE** | **DESCRIÇÃO** | | **LINK DE DADOS** | **INDISPONIBILIDADE** | **FIBRA DO LINK PRINCIPAL** | | **SOFREU ATENUACAO** | | **COM SERVIÇOS DE** | | **TERCEIROS EM POSTES** | |  | |  | | **DISPONIBILIDADE** | **INREGULARIDADES NOS TRABALHOS** | **MANUTENÇÃO EM POSTE** | |  |  | **POR OUTRAS EMPRESAS** | |  |  |  | | **RELAÇÃO ENTRE EVENTOS E INCIDENTES** | | | | **TIPO DE EVENTO** | **TIPO DO INCIDENTE** | **CLASSE DE INCIDENTE** | | **INFRA-ESTRURA DA** | **INDISPONIBILIDADE DOS** | **ROMPIMENTO DA** | | **BORDA PRINCIPAL** | **SERVIÇOS NA EMPRESA** | **FIBRA** | | **COM ROMPIMENTOS** |  |  | |  |  |  | | **ATRIBUIÇÃO DE PRIORIDADES** | | | | **NIVEL DE IMPACTO** | **DESCRIÇÃO** |  | | ORGANIZAÇÃO | ORGANIZAÇÃO FICOU S/ SERVIÇOS DE DADOS PARA OS CLIENTES | | | DEPARTAMENTOS | ORGANIZAÇÃO FICOU S/ SERVIÇOS DE DADOS PARA OS COLAB. | | | MULTIPLOS UTILIZADORES | ORGANIZACAO NÃO CONSEGUE FORNECER SERVIÇOS ALGUM | | | UTILIZADOR | ORGANIZACAO NÃO CONSEGUE FORNECER SERVIÇOS | | |  |  |  | | **NIVEIS DE PRIORIDADES** | | | | **NIVEL DE URGENCIA** | **DESCRIÇÃO** | | | **CRITICA** | O ROMPIMENTO AFETAR TODA A FUNCIONALIDADE DA EMPRESA ATÉ | | | SUBIR OUTRA ROTAR DE REDUNDANCIA. | | |  |  |  | | **NIVEIS DE SERVIÇOS** | | | | **PRIORIDADE** | **TEMPO MAXIMO DE REPOSTA** | **TEMPO MAXIMO DE RESOLUÇÃO** | | **1 CRITICA** | **5 MINUTOS** | **30 MINUTOS** | |  |  |

|  |  |  |
| --- | --- | --- |
| **CLASSIFICAÇÃO DE EVENTOS** | | |
| **TIPO DO EVENTO** | **DESCRIÇÃO** | |
| **SERVIDORES CDN´S** | **DETECTADO A INDISPONIBILIDADE** | |
| **DOS SERVICOS DE INTERNET DE DETERMINADOS SITES( NETFLIX E FACEBOOK)** | |
| **ATAQUES DE HACKER´S** | **DDOS** | |
| **IDS E IPS MAL CONFIGURADOS; NÃO REPOSTAS EM TEMPO HABIL** | |
|  |  |  |
| **CLASSECIFICAÇÃO DE INCIDENTES** | | |
| **CLASSE DO INCIDENTE** | **TIPO DO INCIDENTE** | **DESCRIÇÃO** |
| **SERVIDORES CDN´S** | **INDISPONIBILIDADE** | **SERVIDOR FORA** |
| **NÃO ABRE PAGINAS** |
| **NÃO ABRE STRIMING** |
| **FALTA DE ANALISE DOS LOGS** |
| **ATAQUES DE HACKERS** |
| **ATIVAR LINK´S IPS** |
| **DISPONIBILIDADE** | **INREGULARIDADES NOS SERVIÇOS** | **ATAQUES DE HACKERS** |
|  | **DE REQUISIÇÕES AOS SERVIDORES** | **AUMENTAR O FLUXO DE PACOTES** |
|  |  |  |
| **RELAÇÃO ENTRE EVENTOS E INCIDENTES** | | |
| **TIPO DE EVENTO** | **TIPO DO INCIDENTE** | **CLASSE DE INCIDENTE** |
| **INFRA-ESTRURA DA** | **INDISPONIBILIDADE DOS** | **SERVIDORES FORA DO AR** |
| **BORDA PRINCIPAL** | **SERVIÇOS PARA OS CLIENTES (NETFLIX E** | **ATAQUES DDOS** |
| **SEM SERVIÇOS DE STREAMING** | **FACEBOOK)** |  |
|  |  |  |
| **ATRIBUIÇÃO DE PRIORIDADES** | | |
| **NIVEL DE IMPACTO** | **DESCRIÇÃO** |  |
| ORGANIZAÇÃO | ORGANIZAÇÃO FICOU S/ SERVIÇOS DE STREAMING PARA OS CLIENTES (FACEBOOK E NETFLIX | |
| DEPARTAMENTOS | ORGANIZAÇÃO NÃO FOI AFETADA POIS NÃO FAZ PARTE DO CONTIDIANO | |
| MULTIPLOS UTILIZADORES | ORGANIZAÇÃO NÃO FOI AFETADA POIS NÃO FAZ PARTE DO CONTIDIANO | |
| UTILIZADOR | ORGANIZAÇÃO FICOU S/ SERVIÇOS DE STREAMING PARA OS CLIENTES (FACEBOOK E NETFLIX | |
|  |  |  |
| **NIVEIS DE PRIORIDADES** | | |
| **NIVEL DE URGENCIA** | **DESCRIÇÃO** | |
| **ALTA** | INDISPONIBILIDADES DOS SERVIÇOS DE STREAMING | |
| ATIVAÇÃO DE LINK IP´S |  |
|  |  |  |
| **NIVEIS DE SERVIÇOS** | | |
| **PRIORIDADE** | **TEMPO MAXIMO DE REPOSTA** | **TEMPO MAXIMO DE RESOLUÇÃO** |
| **2 ALTA** | **30 MINUTOS** | **1 HORA** |

|  |  |  |
| --- | --- | --- |
| **CLASSIFICAÇÃO DE EVENTOS** | | |
| **TIPO DO EVENTO** | **DESCRIÇÃO** | |
| **SOFTWARE DE GESTÃO DE REDES SGP** | **DETECTADO A INDISPONIBILIDADE** | |
| **SERVIÇOS CLOUD COM INDISPONIBILIDADE / ATIVAR SERVIDOR BACKUP** | |
| **ATAQUES DE HACKER´S** | **RANSON NO SERVIDOR DNS DA EMPRESA** | |
| **NÃO ANALISE DOS LOGS DE TENTATIVAS DE ACESSOS; IDS E IPS MAL CONFIGURADOS** | |
|  |  |  |
| **CLASSECIFICAÇÃO DE INCIDENTES** | | |
| **CLASSE DO INCIDENTE** | **TIPO DO INCIDENTE** | **DESCRIÇÃO** |
| **SOFTWARE GESTAO DE REDES SGP** | **INDISPONIBILIDADE** | **SERVIDOR DNS FORA** |
| **SEM ACESSOS AO SO SGP** |
| **CLIENTES NÃO AUTENTICAR NO SRV** |
| **FALTA DE ANALISE DOS LOGS** |
| **ATAQUES DE HACKERS** |
|  |
| **DISPONIBILIDADE** | **INREGULARIDADES NOS SERVIÇOS** | **ATAQUES DE HACKERS** |
|  | **DE REQUISIÇÕES AO SERVIDOR DNS FORA** | **CRIPTOGRAFIA DOS DISCO RIGIDO** |
|  |  |  |
| **RELAÇÃO ENTRE EVENTOS E INCIDENTES** | | |
| **TIPO DE EVENTO** | **TIPO DO INCIDENTE** | **CLASSE DE INCIDENTE** |
| **INFRA-ESTRURA DA** | **INDISPONIBILIDADE DE ACESSO A CLOUD** | **SERVIDORES FORA DO AR SGP** |
| **CLOUD** | **SERVIÇOS FORA DEVIDO ATAQUE DNS** | **DEVIDO A ATAQUES RANSON** |
| **AUTENTICAÇÕES E ACESSO AO** |  | **SERVIÇOS INDISPONIVEIS AOS** |
| **SISTEMA FORA** |  | **CLIENTES** |
| **ATRIBUIÇÃO DE PRIORIDADES** | | |
| **NIVEL DE IMPACTO** | **DESCRIÇÃO** |  |
| ORGANIZAÇÃO | ORGANIZAÇÃO FICOU S/ SERVIÇOS DISPONIVEIS AO SISTEMA | |
| DEPARTAMENTOS | ORGANIZAÇÃO FICOU SEM SERVIÇOS EM SUA TOTALIDADE | |
| MULTIPLOS UTILIZADORES | ORGANIZAÇÃO FICOU SEM SERVIÇOS EM SUA TOTALIDADE | |
| UTILIZADOR | ORGANIZAÇÃO FICOU S/ SERVIÇOS DE ACESSO A INTERNET DEVIDO AS AUTENTICAÇÕES | |
|  |  |  |
| **NIVEIS DE PRIORIDADES** | | |
| **NIVEL DE URGENCIA** | **DESCRIÇÃO** | |
| **CRITICA** | INDISPONIBILIDADES DOS SERVIÇOS DE DNS E AUTENTICAÇÃO DA REDE | |
| RECUPERCAÇÃO ATRAVES DE BACKUPS REALIZADOS DIAS ANTERIORES | |
|  |  |  |
| **NIVEIS DE SERVIÇOS** | | |
| **PRIORIDADE** | **TEMPO MAXIMO DE REPOSTA** | **TEMPO MAXIMO DE RESOLUÇÃO** |
| **1CRITICA** | **5 MINUTOS** | **30 MINUTOS** |

|  |  |  |
| --- | --- | --- |
| **CLASSIFICAÇÃO DE EVENTOS** | | |
| **TIPO DO EVENTO** | **DESCRIÇÃO** | |
| **TELEFONE IP´S** | **DETECTADO A INDISPONIBILIDADE DE SERVICOS NA REDE** | |
| **REDE LOCAL SEM TRAFEGO** | |
| **REDE LOCAL** | **RANSON NO SERVIDOR DNS DA EMPRESA** | |
| **MAL CONFIGURAÇÕES DAS ESTAÇÕES; VIRUS DENTRO DA REDE** | |
|  |  |  |
| **CLASSECIFICAÇÃO DE INCIDENTES** | | |
| **CLASSE DO INCIDENTE** | **TIPO DO INCIDENTE** | **DESCRIÇÃO** |
| **TELEFONE IP´S** | **INDISPONIBILIDADE** | **SEM ACESSO A REDE LOCAL** |
| **DHCP NÃO TRAFEGANDO NA REDE** |
| **VIRUS NA REDE** |
| **FALTA DE CONFIGURAÇÕES** |
| **CORRETAS NOS FIREWALL** |
|  |
| **DISPONIBILIDADE** | **INREGULARIDADES NOS SERVIÇOS** | **VIRUS NA REDE** |
|  | **DE REQUISIÇÕES AO SERVIDOR LOCAL** | **REDE NULA OU LIMITADA** |
|  |  |  |
| **RELAÇÃO ENTRE EVENTOS E INCIDENTES** | | |
| **TIPO DE EVENTO** | **TIPO DO INCIDENTE** | **CLASSE DE INCIDENTE** |
| **INFRA-ESTRURA DA** | **INDISPONIBILIDADE DE ACESSO AOS DHCP NO TELEFONES** | **DHCP NÃO TRAFEGA NA REDE** |
| **LOCAL DA REDE** | **SERVIÇOS FORA DEVIDO A VIRUS NA REDE LOCAL** | **VIRUS NA REDE** |
|  |  | **SERVIÇOS INDISPONIVEIS AOS** |
|  |  | **DEPARTAMENTOS** |
| **ATRIBUIÇÃO DE PRIORIDADES** | | |
| **NIVEL DE IMPACTO** | **DESCRIÇÃO** |  |
| ORGANIZAÇÃO | ORGANIZAÇÃO FICOU S/ SERVIÇOS DE COMUNICAÇÃO COM OS CLIENTES E SETORES | |
| DEPARTAMENTOS | ORGANIZAÇÃO FICOU SEM SERVIÇOS DE COMUNICAÇÃO ENTRE OS SETORES | |
| MULTIPLOS UTILIZADORES | ORGANIZAÇÃO FICOU SEM SERVIÇOS EM SUA TOTALIDADE | |
| UTILIZADOR | ORGANIZAÇÃO FICOU S/ SERVIÇOS DE COMUNICAÇÃO COM OS CLIENTES | |
|  |  |  |
| **NIVEIS DE PRIORIDADES** | | |
| **NIVEL DE URGENCIA** | **DESCRIÇÃO** | |
| **MEDIA** | REPARAÇÃO DAS ESTAÇÕES ZUMBIR NAS REDES |  |
| RECUFIGURAÇÃO DOS SERVIÇOS DHCPS |  |
|  |  |  |
| **NIVEIS DE SERVIÇOS** | | |
| **PRIORIDADE** | **TEMPO MAXIMO DE REPOSTA** | **TEMPO MAXIMO DE RESOLUÇÃO** |
| **3 MEDIA** | **15 MINUTOS** | **1 HORA** |

**Procedimento de Comunicação e escalada de Incidentes**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **ITEM** | **DESCRIÇÃO/OBJETIVO** | **RESP. PELA COMUNICAÇÃO** | **DESTINATARIO** | **CONTATO** | **PERIODOCIDADE** | **REGISTO/ARQUIVO** |
| 1 | **LINK´S DE DADOS** | DOCUMENTO COM INFORMAÇÃO | SUPORTE OPERACIONAL | EQUIPA OPERACAO |  | A CADA OCORRENCIA | REPOSITORIO CSIRT |
|  | RELATIVA AO INCIDENTE DO | 1 LINHA |  |  |  |  |
|  | ROMPIMENTO DA FIBRA NA BORDA |  |  |  |  |  |
|  | **SERVIDORES CDN´S** | DOCUMENTO COM INFORMAÇÃO |  |  |  |  |  |
| 1 | INVAÇÃO;QUEDA DO CIRCUITO; | COORDENADOR CSIRT | IT MANAGER |  | A CADA OCORRENCIA | REPOSITORIO CSIRT |
|  | ROMPIMENTO DE FIBRA; FALTA DE ENREGIA |  |  |  |  |  |
|  | **SOFTWARE DE GESTÃO DE REDES SGP** | DOCUMENTO COM INFORMAÇÃO |  |  |  |  |  |
| 2 | SERVIDOR CLOUD FORA DO AR; SEM ACESSO A LINK | 2 LINHA OPERACIONAL | IT MANAGER |  | A CADA OCORRENCIA | REPOSITORIO CSIRT |
|  | DE DADOS; INDISPONIBILIDADE DA REDE LOCAL |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **NIVEIS / ACOES** | **PRIORIDADE CRITICO** | | **PRI0RIDADE ALTO** | **PRIORIDADE MEDIO** | **PRIORIDADE BAIXO** | **>= 50%** | **>= 70%** | **>= 100%** |
|  |  | **INCIDENTE GRAVE** |
| 1 LINHA | TEMPO DE RESOLUÇÃO |  | 50 MINUTOS | 01:30:00 H | 2 H | 3 H |  | NOTIFICAÇÃO | NOTIFICAÇÃO |
|  | TEMPO DE RESPOSTA |  | 5 MINUTOS | 30 MINUTOS | 1 H | 2 H |  | COORDENADOR | COORDENADOR |
|  |  |  |  |  |  |  |  |  |  |
| 2 LINHA | TEMPO DE RESOLUÇÃO |  | 40 MINUTOS | 1 H | 3H | 6 H |  | NOTIFICAÇÃO | NOTIFICAÇÃO |
|  | TEMPO DE RESPOSTA |  | 10 MINUTOS | 30 MINUTOS | 1H | 3H |  | COORDENADOR | COORDENADOR |

**Procedimento de análise forense e recolha de evidencias**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **AÇÕES** | **OBJETIVO** | **RESPONSAVEL** | **RECURSOS** | **DATA** | **DATA** | **CUSTO** | **EFICACIA** | **OBSERVAÇÕES** |
| **PLANEJADAS / EXECUTADAS** | **NECESSARIOS** | **INICIO** | **CONCLUSÃO** | **ESTIMADO EFETIVO** | **DAS ACOES** | **AVALIAR** |
| RECONFIGURAÇÕES E TESTE | MITIGAR | IT MANAGER | CONFIGURAÇÕES DE SERVIÇOS | 16/12/2019 | 20/12/2019 | 1 MIL EUROS | FECHAR E AVALIAR POR UM SRV LOCAL | CONTINUAMENTE |
| DOS FIREWALL E DNS´S | OS PROCESSOS |  |  |  |  |  | COM TESTE DE PENETRAÇÃO AS VUNERABILIDADES | OS LOGS |
|  | DE ATAQUES |  |  |  |  |  |  |  |
| APLICAÇÃO DA DUPLA | MITIGAR | EQUIPE | INSTALÇÃO DE FIBRA POR | 20/12/2019 | 25/12/2019 | 3 MIL EUROS | CRIAR UMA CONEXAO OSPF, COM OS SERVIDORES | TESTAR |
| BORADGEM PRA CONTIGENCIA | INDIPONIBILIDADE | OPERAÇÃO | OUTRA ROTA |  |  |  | FAZENDO UM ANEL NOS SEUS ENLACES | A FUNCIONALIDADE |
| DO LINK DADOS |  |  |  |  |  |  |  | DO OSPF |
|  |  |  |  |  |  |  |  |  |
| APLICAÇÃO DE ANTIVIRUS | MITIGAR | IT MANAGER | INSTALAÇÃO DE ANTIVIRUS | 26/12/2019 | 31/12/2019 | 2 MIL EUROS | CRIAR LOGS DE ACESSOS E RESTRIÇÕES EM LOGAR | MONITORAR OS |
| E RESTRIÇÕES DE ACESSOS | ENTRADAS |  | LDAP NAS ESTAÇÕES |  |  |  | NAS ESTAÇÕES DE TRABALHO COM CONTROLE | LOGS |
| A APLICAÇÕES NA WEB | DE VIRUS |  | PROXY NOS NAVEGADORES |  |  |  | DE PASTAS E COMPARTILHAMENTOS |  |

CONCLUSÃO

Percebemos a grande importância dos processos as aplicados em uma empresa que trabalhar no segmento de telecomunicações, onde o tempo e indisponibilidade dos serviços oferecidos não podem ultrapassar a faixa de 1 hora, sendo de suma importância medidas aplicadas para mitigar esses processos e sempre haver funcionalidades em seus serviços oferecidos.

Contudo é de grande relevância que percebemos as aplicações dos relatos dos incidentes em suas categorias de notificações, conseguimos enxergar cada fator importante.