POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

A Política de Segurança da Informação é uma declaração formal do PREVINI acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários.

2. ABRANGÊNCIA

Todos os funcionários, diretores, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos do PREVINI.

3. MISSÃO

Garantir a integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios do PREVINI.

4. DOCUMENTOS DE REFERÊNCIA

- NBR ISO/IEC 17799:2005
- ABNT 21:204.01-010
- Lei 9.609/98 – Lei do Software
- Política de Segurança da Informação - Raízen

5. TERMOS E DEFINIÇÕES

- *TI*: Tecnologia da Informação
- *Software:* É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.
- *Backup:* É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
- *Mídias Removíveis:* Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.
- *USB:* É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.
- *VPN (Virtual Private Network):* Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.
- *Softwares de Mensageria:* São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes

programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

- *Firewall:* É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
- *Wi-Fi:* Rede sem fio se refere a uma rede de computadores sem a necessidade do uso de cabos, sejam eles telefônicos, coaxiais ou ópticos. Utiliza-se a radio frequência ou comunicação via infravermelho, como em dispositivos compatíveis com IrDA (Infrared Data Association).
- *MAC:* O Endereço MAC (Media Access Control) é um endereço físico associado à interface de comunicação, que conecta um dispositivo à rede. O MAC é um endereço "único", não havendo duas portas com a mesma numeração, é usado para controle de acesso em redes de computadores.
- *Clusters*: São aglomerados de dispositivos ou computadores conectados. Eles podem ser entendidos como um sistema único, por meio de diversos aspectos, uma vez que desempenham as mesmas tarefas de forma sequencial ou paralela.
- *Storage*: Uma expressão em inglês que remete a soluções de armazenamento, gerenciamento e proteção aos dados. O armazenamento de dados é uma responsabilidade de departamentos de TI, sendo um dos principais componentes de datacenters.
- *Raid*: Um conjunto redundante de discos independentes que visa obter vantagens na utilização de subsistemas de dois ou mais discos, entre elas podemos citar aumento de desempenho, segurança, alta disponibilidade e tolerância a falhas.

6. DIRETRIZES

6.1. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Conforme definição da norma NBR ISO/IEC 17799: 2005, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é aqui caracterizada pela preservação da:

a) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;
b) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
c) Disponibilidade, a Política de Segurança da Informação deve ser divulgada a todos os funcionários e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes pró-ativas e engajadas no que diz respeito à proteção das informações.

Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle destas diretrizes.

A Política de Segurança da Informação do PREVINI é aprovada e revisada pela Diretoria Executiva.

6.2. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

6.2.1. Definição

Cabe a todos os funcionários (funcionários, estagiários e prestadores de serviços) cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo PREVINI; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente ao Instituto quando do descumprimento ou violação desta política.

6.2.2. Diretorias, Gerências e Coordenações

Cabe às Diretorias, Gerências e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação.

6.2.3. Área de Gerência da Divisão de Informática e Diretoria Executiva

Cabem as duas áreas propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Gestores.

6.3. PROPRIEDADE INTELECTUAL

6.3.1. É de propriedade do PREVINI, todos os "designs", criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com o PREVINI.

6.4. ENGENHARIA SOCIAL

6.4.1. Engenharia social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas.

6.4.2. A Engenharia Social manifesta-se de diversas formas, e podemos dividi-los em dois grupos. No entanto, o grande ponto onde engenheiros sociais se baseiam é na falta de conscientização do usuário com relação à Segurança da Informação e na exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes, e como uma simples informação poderia trazer prejuízos ao Instituto:

6.4.2.1. Diretos: São aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido.

6.4.2.2. Indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir, como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países e etc. O melhor a fazer é ignorar a oferta tentadora e apagar o e-mail imediatamente.

6.5. CLASSIFICAÇÃO DA INFORMAÇÃO

6.5.1. É de responsabilidade do Gerente/Chefia imediata de cada setor estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

6.5.1.1. Pública: É uma informação do PREVINI ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional.

É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

6.5.1.2. Interna: É uma informação do PREVINI que não tem interesse em divulgar, onde o acesso por parte de indivíduos externos ao Instituto deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem do Órgão, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os funcionários e prestadores de serviços do PREVINI.

6.5.1.3. Confidencial: É uma informação crítica para os negócios do PREVINI ou de seus Patrocinadores/Segurados.

A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais ao PREVINI ou aos

seus Patrocinadores/Segurados. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por Funcionários, Segurados e/ou Fornecedores.

6.5.1.4. Restrita: É toda informação que pode ser acessada somente por usuários do PREVINI explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da Instituição.

6.6. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

6.6.1. As máquinas (servidores) que armazenam sistemas do PREVINI estão em área protegida – Data Center localizado na sede do Instituto em Nova Iguaçu / RJ.

6.6.2. As entradas ao Data Center têm acesso devidamente controlado.

6.6.3. A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

6.6.4. O acesso às dependências do Instituto com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização do setor de Patrimônio e mediante supervisão. Exceto para eventos e treinamentos organizados pelo próprio Instituto.

6.6.5. Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

6.7. BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL DENTRO E FORA DA EMPRESA

6.7.1. Cuidado ao tratar de assuntos do Instituto dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

6.7.2. Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora do Instituto ou próximos a pessoas desconhecidas.

6.7.3. Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem do PREVINI.

6.8. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

6.8.1. Diretrizes Gerais

6.8.1.1. Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação

da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

6.8.2. Diretrizes Específicas

6.8.2.1. Sistemas

6.8.2.1.1. Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

6.8.2.1.2. Cópia de segurança (Backup) deve ser testada e mantida atualizada para fins de recuperação em caso de desastres. .

6.8.2.1.3. Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

6.8.2.1.4. Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

6.8.2.1.5. Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção.

No mínimo, o arquivo deve contar com a proteção de uma senha "robusta".

6.8.2.2. Máquinas – Estação de Trabalho

6.8.2.2.1. As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

6.8.2.2.2. As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

6.8.2.2.3. O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.

6.8.2.2.4. Quando se ausentar da mesa, deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os funcionários com estações de trabalho, incluindo equipamentos portáteis.

6.8.2.2.5. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades do PREVINI, só devem ser utilizadas em equipamentos com controles adequados.

6.8.2.2.6. Os usuários de TI devem utilizar apenas softwares licenciados pela Gerencia da Divisão de Informática/CPD, nos equipamentos do Instituto.

6.8.2.2.7. A Gerência da Divisão de Informática/CPD deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

6.8.2.3. Boas práticas de segurança para seu notebook

6.8.2.3.1. Quando em deslocamentos de carro, coloque o mesmo no porta-malas ou em local não visível.

6.8.2.3.2. Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para notebook e sim mochilas ou malas discretas.

6.8.2.3.3. Não coloque o notebook em carrinhos de aeroportos ou despache junto à bagagem.

6.8.2.3.4. Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento.

6.8.2.3.5. Evite utilizar o notebook em locais públicos.

6.8.2.3.6. Nos hotéis, preferencialmente, guarde o notebook no cofre do seu apartamento.

6.8.2.3.7. Avalie se em pequenas viagens é realmente necessário levar o notebook.

6.8.2.4. Utilização de equipamentos particulares / terceiros dentro da empresa

6.8.2.4.1. Notebooks particulares para serem usados dentro da rede do PREVINI, precisam ser avaliados pelo pessoal responsável de TI.

6.8.2.4.2. Equipamentos de terceiros devem ser levados ao suporte para serem verificadas atualização do antivírus e existência de vírus.

6.8.2.4.3. É responsabilidade da área contratante/Setor/Departamento encaminhar os terceiros sob sua responsabilidade para esta verificação.

6.8.2.5. Boas práticas de segurança para Impressões e Fax

6.8.2.5.1. Documento enviado para a impressão deverá ser retirado imediatamente.

6.8.2.5.2. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora para retirada, ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora do Instituto.

6.8.2.5.3. Cuidado com o uso do Fax Eletrônico, os arquivos ficam na rede por 24 horas, podendo ser acessado e copiado por outros funcionários e/ou terceiros. Após o recebimento e/ou cópia do arquivo de Fax, o mesmo deverá ser excluído da rede.

6.8.2.6. A Instalação de Softwares

6.8.2.6.1. Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado a área de Suporte Técnico – Infraestrutura TI, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente.

6.8.2.6.2. O PREVINI respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores do Instituto. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) no PREVINI.

6.8.2.6.3. A Gerência de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

6.8.2.7. Diretrizes quanto à utilização da Rede Corporativa

6.8.2.7.1. Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

6.8.2.7.2. Somente os funcionários que estão devidamente autorizados a falar em nome do PREVINI para os meios de comunicação podem escrever em nome do Instituto em sites de BatePapo(Chat Room), Redes Sociais (Facebook) ou Grupos de Discussão (fóruns, newsgroups). Em caso de dúvidas, procurar a Diretoria Executiva.

6.8.2.7.3. Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador(local) não possuem cópias de segurança (backup) e podem ser perdidos. O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante citar que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.

6.8.2.7.4. Arquivos que estão na rede com mais de 24 meses sem acesso serão copiados em fita via Backup específico e excluídos após. Para ter acesso a esses arquivos, é necessário solicitar a TI.

6.8.2.7.5. Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos drivers de rede, pois ocupam espaço comum limitado do departamento.

6.8.2.8. Diretrizes quanto ao uso de Mídias Removíveis e da porta USB

6.8.2.8.1. O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra.

6.8.2.8.2. A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, neste caso, os modens 3G e os pen

drives merecem a atenção. Tal vulnerabilidade não pode ser contida com firewalls ou com programas antivírus já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários do Instituto.

6.8.2.8.3. Para liberação das portas USB dos desktops e notebooks é necessário justificar o uso e a aprovação da chefia do departamento do solicitante.

6.8.2.8.4. Dentro da empresa dê preferência à utilização da rede evitando a utilizando de modem 3G conectado à porta USB do computador, pois é considerada uma forma de burlar a segurança de rede, protegida por Firewall e regras de segurança. Assim o funcionário abre a porta para acesso sem qualquer controle.

6.8.2.8.5. Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados.

6.8.2.8.6. É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

6.8.2.9. Diretrizes quanto ao uso da Internet

6.8.2.9.1. A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas ao Instituto.

6.8.2.9.2. O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdos impróprios e de relacionamentos.

6.8.2.9.3. O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.

6.8.2.9.4. É vedado qualquer tipo de download. Como também o upload de qualquer software licenciado ao PREVINI ou de dados de propriedade do instituto ou de seus segurados, sem expressa autorização do gerente responsável pelo software ou pelos dados.

6.8.2.9.5. Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

6.8.2.9.5. Não é permitido:

- Download de músicas, jogos, filmes, programas etc.;
- Utilização de meios alternativos para burlar o sistema de controle de acesso a Internet da instituição;
- Acesso a sites com conteúdo impróprio, pornográficos e afins;
- Utilização de programas de downloads P2P, como Limewire, Kazaa, Ares, Emule, uTorrent, biTorrent, entre outros;
- Ligação de aparelhos a fim de redistribuir o acesso à rede wireless a terceiros;

- Se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais.
- Divulgar sua conta de usuário e sua senha de acesso para qualquer pessoa. Estas informações são de caráter pessoal e intransferível.
- Utilizar o serviço para fins ilícitos e proibidos.
- Utilizar o serviço para transmitir ou divulgar material ilícito, proibido ou difamatório que viole a privacidade de terceiros, ou que seja abusivo, ameaçador, discriminatório, injurioso ou calunioso.
- Acessar conteúdo pornográfico e jogos on-line.
- Utilizar o serviço para transmitir/divulgar material que incentive discriminação ou violência.
- Transmitir e/ou divulgar qualquer material que viole direitos de terceiros, incluindo direitos de propriedade intelectual.
- Obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao serviço.
- Interferir ou interromper o serviço, as redes ou os servidores conectados ao serviço.
- Usar de falsa identidade ou utilizar dados de terceiros para obter acesso ao serviço.
- Tentar enganar ou subverter as medidas de segurança dos sistemas e da rede de comunicação.
- Utilizar o serviço para intimidar, assediar, difamar ou aborrecer qualquer pessoa.
- Utilizar serviço de proxy para burlar sites com acesso não autorizado.
- Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos.
- Utilizar o acesso à internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade Internet.
- Acessar sites pornográficos ou quaisquer outros sites que seu conteúdo não seja informativo ou educacional.
- Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais do PREVINI.
- Violar ou tentar violar os sistemas de segurança.
- Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais do PREVINI.
- Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e worms, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional.
- Utilizar os recursos computacionais do PREVINI para ganho indevido.
- Utilizar os recursos computacionais do PREVINI para intimidar, assediar, difamar ou aborrecer qualquer pessoa.
- Consumir inutilmente os recursos computacionais do PREVINI de forma intencional.

- Desenvolver qualquer outra atividade que desobedeça às normas apresentadas acima.

6.8.2.10. Recomendações sobre o uso do Correio Eletrônico (E-Mail)

6.8.2.10.1. É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico do PREVINI.

6.8.2.10.2. É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem do PREVINI perante seus servidores e a comunidade em geral e que possam causar prejuízo moral e financeiro.

6.8.2.10.3. Evitar utilizar o e-mail da empresa para assuntos pessoais.

6.8.2.10.4. Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

6.8.2.10.5. Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

6.8.2.10.6. Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

6.8.2.10.7. Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

6.8.2.11. Antivírus

6.8.2.11.1. Antivírus dos servidores e estações são atualizados automaticamente.

6.8.2.11.2. A varredura por vírus é feito diariamente nas estações e nos servidores.

6.8.2.12. Uso de Softwares de Mensageria

6.8.2.12.1. Recomenda-se a utilização do Software Softprevi – Actuary como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio.

6.8.2.12.2. A instalação de software de mensageria e a liberação do acesso são restritas e sua utilização deve ser justificada à Gerência de TI.

6.8.2.12.3. O uso de sistemas de mensageria é aceitável apenas quando for utilizado como ferramenta de produtividade para comunicação online, no exercício de sua função. Enquanto o uso responsável dos sistemas de mensageria é estimulado, o seu abuso deve ser evitado.

6.8.2.12.4. Sistemas de mensageria possuem histórico de riscos associados à malwares (p.ex. vírus, worms etc), de forma que deve ser utilizado com zelo e cuidado.

6.8.2.12.5. O uso de sistemas de mensageria em redes de relacionamento pessoais deve ser evitado no ambiente corporativo, por conta da natural assíncronia das mensagens instantâneas oriundas de terceiros sem finalidades laborais, o que usualmente torna-se contraproducente.

6.8.2.12.6. O grande problema de se utilizar este tipo de software é que, uma vez conectado, o computador fica altamente vulnerável. As portas de entrada/saída ficam abertas, sem qualquer restrição de leitura ou gravação. Desta forma, vírus que exploram esse tipo de vulnerabilidade não encontram empecilhos para se instalarem e iniciarem os processos danosos, não só para aquele dispositivo, mas para todos os que a ele estiverem conectados ou que estiverem em rede.

6.8.2.12.7. Exemplos de softwares de Mensageria: mIRC, Scoop Script, Avalanche, Full Throttle, MSN Messenger, Yahoo Messenger, Skype, etc.

6.8.2.13. Controle de Acesso a VPN

6.8.2.13.1. O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

6.8.2.13.2. É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

6.8.2.13.3. O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações das empresas abrangidas neste procedimento.

6.8.2.13.4. Nunca deixar sessões VPN abertas. Cada vez que o usuário deixar o seu equipamento conectado via VPN, deve executar logoff ou bloquear seu equipamento.

6.8.2.13.5. Manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

6.8.2.14. Controle de Acesso Lógico (Baseado em Senhas)

6.8.2.14.1. Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

6.8.2.14.2. Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.

6.8.2.14.3. Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.

6.8.2.14.4. Não incluir senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função.

6.8.2.14.5. A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso.

6.8.2.14.6. A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário.

6.9. REDE SEM FIO (WI-FI)

Essa rede permite maior flexibilidade e mobilidade, visando oferecer aos funcionários e prestadores de serviços do PREVINI acesso à Internet, através de equipamentos próprios que suportem esta tecnologia.

6.9.1. *Cobertura de Acesso:* 3º Andar, 2º Andar e 1º Andar

6.9.2. *Redes Disponíveis (SSID):* Funcionarios.PREVINI e PREVINI.convidado

A rede **Funcionarios.PREVINI** disponível apenas e somente para funcionários e estagiários do PREVINI. Esse acesso é feito pela amarração do endereço MAC da placa de rede de cada equipamento dos funcionários. Qualquer equipamento que tente acessar essa rede mesmo que tenha obtido a senha de acesso, não logrará êxito caso o MAC do dispositivo não esteja cadastrado/autorizado pela TI.

A rede **PREVINI.convidado** disponível apenas para convidados. O acesso é autorizado por funcionário do PREVINI onde é informada a senha de acesso, em seguida será necessário informar um número/código de Voucher. Esses vouchers são gerados pela equipe de TI do PREVINI onde são permitidos acessos a Internet. Os Vouchers normalmente são válidos apenas por 8 horas e não tem limite de velocidade de acesso. O tempo de validade e limite de velocidade podem ser alterados pela equipe de TI caso seja necessário.

Os Vouchers são disponibilizados e ficam sob a guarda da Chefia de Gabinete que tem a responsabilidade de identificar e tomar nota dos dados pessoais do usuário, bem como, dia e hora da entrega do voucher.

Importante ressaltar que os acessos da rede de convidados, tem permissão de acesso somente a Internet, não sendo permitido acesso para qualquer rede interna do PREVINI.

A rede de Funcionários só é permitida apenas acesso a Internet, não sendo permitido acesso a qualquer rede interna do PREVINI.

6.9.3. *Requisitos de Hardware:* Para acessar a rede Wi-Fi do PREVINI é necessário, como requisito mínimo, um dispositivo computacional equipado com PLACA DE REDE sem fio compatível com a Norma IEEE 802.11 a/b/g e Suporte às Normas de segurança padrão IEEE 802.1x.

6.9.4. *Configuração de Acesso:* A configuração do dispositivo Wireless para acesso à rede é de inteira responsabilidade do usuário, o PREVINI não se responsabiliza por eventuais danos que possam ocorrer. Ao acessar a rede, uma senha de segurança e um voucher de acesso são solicitados e o usuário deverá também ler e aceitar os Termos de Uso. Essa senha e voucher estão disponíveis na Chefia de Gabinete.

6.9.5. *Termos de Uso:* Ao acessar a rede sem fio, você reconhece que é maior de idade, leu e entendeu e concorda em ficar vinculado a este contrato.

"O serviço de rede sem fio é fornecido pelos proprietários e é completamente a seu critério. Seu acesso à rede pode ser bloqueado, suspenso ou encerrado a qualquer momento por qualquer motivo.

Você concorda em não usar a rede sem fio para qualquer finalidade que seja ilegal e assumir total responsabilidade por seus atos.

É expressamente proibido mostrar, armazenar ou transmitir textos, imagens ou sons que possam ser considerados ofensivos ou abusivos; utilizar o acesso a Internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade de Internet; provocar interferências em serviços de outros usuários ou o seu bloqueio parcial ou total; acessar sites pornográficos ou quaisquer outros sites que seu conteúdo não seja informativo ou educacional; violar os sistemas de segurança de rede; utilizar os recursos computacionais para fins comerciais ou políticos, tais como mala direta (spans) ou propaganda política.

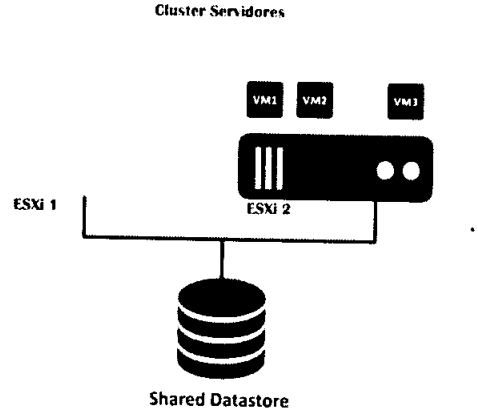
A rede sem fio é fornecida sem garantias de qualquer tipo, expressas ou implícitas."

6.10. PLANO DE CONTINGÊNCIA

6.10.1. Com o avanço da tecnologia, é praticamente impossível encontrar empresas e ou órgãos que não dependam do bom funcionamento do ambiente operacional para o sucesso do seu negócio. Falhas em sistemas podem causar diversos danos, principalmente quando afetam os nossos segurados. Por isso, cada vez mais, é comum ver organizações adotando a redundância em TI. Em sua tradução, o termo "Redundância" significa um "discurso que se baseia na utilização de diferentes palavras para expressar um mesmo pensamento ou ideia" — de acordo com o Dicionário Online de Português. Porém, o termo é usado em TI com outro propósito. Ele indica a duplicação de componentes críticos, aumentando a confiabilidade e

segurança de um sistema, bem como sua disponibilidade. Os componentes que podem receber essa proteção são normalmente relacionados a dados, como os backups. Porém, seu uso também pode ser interessante em clusters. Dessa forma, com o uso da redundância, são construídos clusters de alta disponibilidade. Nesse modelo, quando um nó falha, a tarefa é enviada para outro nó (ou dispositivo), mantendo o sistema funcionando de forma ininterrupta. A redundância em TI é essencial para a alta disponibilidade de **sistemas, redes e dados**. Com a repetição de componentes críticos para o funcionamento de um serviço, a confiabilidade dele é aprimorada, pois caso aconteça uma falha que possa desabilitar o sistema primário, um sistema secundário assume a responsabilidade. O objetivo da redundância em TI é garantir a utilização ininterrupta de serviços e evitar a perda de dados. Isso é feito com fontes de energia alternativas, múltiplos locais de armazenamento de dados e outros dispositivos redundantes.

6.10.2. Atualmente no PREVINI utilizamos 02 (dois) clusters, um para redundância de servidores virtuais e outro para redundância de desktops virtuais. O PREVINI utiliza para gerenciamento dos Hosts de seu datacenter uma ferramenta chamada VMware ESXi que atualmente se encontra na versão 6.7, através dessa ferramenta podemos gerenciar o Cluster de Servidores que é composto por 2 Servidores físicos com o Sistema Operacional ESXi.



Para ficar mais claro, podemos verificar na imagem acima que quando um servidor físico (ESXi1) apresentar falhas, teoricamente os servidores virtuais (VM) gerenciado por esse servidor (ESXi1) também poderiam apresentar falhas, mas em se tratando de um cluster de servidores, podemos utilizar um serviço chamado de HA (High Availability) para fazer com que todas as VM (Virtual Machine) possam migrar automaticamente para o outro servidor (ESXi2) e fazendo com que os serviços disponibilizados não pare. Nessa situação, os dois servidores recebem o tráfego de forma igualmente distribuída. Porém, em momentos de falha em um deles, o dispositivo redireciona o seu tráfego para o servidor que continua funcionando. Dessa

forma, a operação se mantém normal, permitindo que o erro seja reparado sem custos para a organização. Isso ocorre também para o cluter de desktops virtuais.

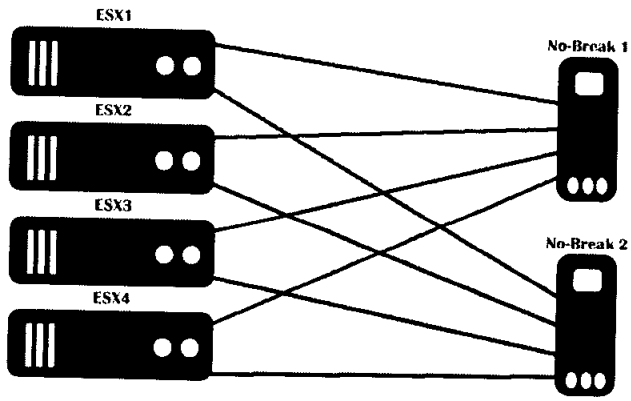
6.10.3 A redundância pode ser aplicada a diversos componentes de um sistema com o objetivo de garantir que sua disponibilidade seja mantida em momentos de problemas que levariam a pausa do funcionamento.

6.10.4. Um sistema pode ser redundante em diversos dos seus componentes. Para isso, basta que ele tenha pelo menos dois recursos diferentes integrados e capazes de se substituírem. As formas mais comuns de redundância em TI são nas fontes de energia, nas redes, na memória RAM e nos dados.

6.10.4.1. Fontes de energia:

6.10.4.1.1. A redundância em fontes de energia consiste, na maior parte das vezes, em nobreaks e baterias que podem garantir a continuidade do trabalho em um local mesmo se houver indisponibilidade ou intermitência na rede elétrica.

6.10.4.1.2 No PREVINI atualmente utilizamos servidores físicos onde todos eles são providos de fontes de energia redundante, isso significa que caso uma fonte apresente problema, a outra fonte supri a necessidade para que o servidor não pare de funcionar, até que a fonte que apresentou falha seja trocada.



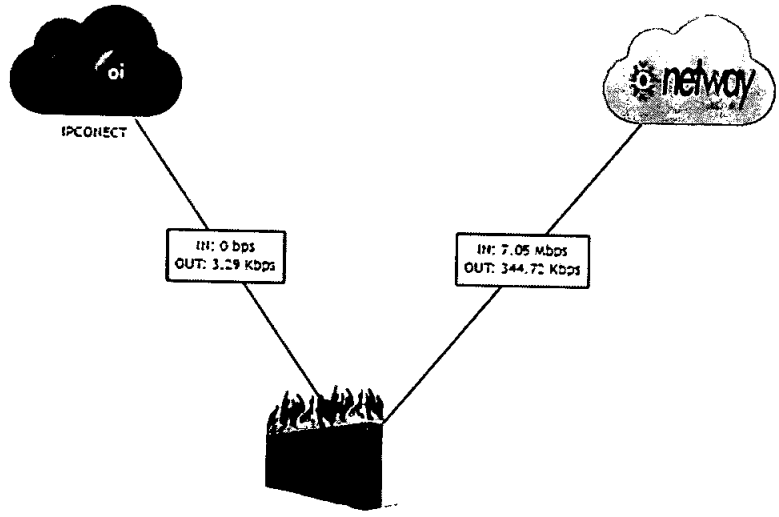
Utilizamos 02 (dois) no-breaks onde interligamos fonte de energia de cada servidor em nobreaks diferentes, conforme ilustrado no desenho acima. Assim podemos garantir que além

da redundância das fontes de energia de cada servidor, podemos contar com a redundância de no-breaks.

6.10.4.2. Redes:

6.10.4.2.1. A redundância de rede envolve a repetição de equipamentos modulares de fornecimento de rede e, pelo menos, duas conexões diferentes com a internet. A ideia é garantir a conexão mesmo no caso de falha de um componente ou serviço. Logo, se o provedor de internet do PREVINI sofre alguma falha, precisamos de uma opção alternativa para continuar operando, o que pode ser, por exemplo, uma conexão com outro provedor. Em alguns casos, é interessante que essa conexão secundária ou terciária seja sem fio, para situações em que o problema é físico, como a queda de um poste na região em que passam todos os cabos de provedores.

6.10.4.2.2. No PREVINI dispomos de 02 (dois) links de internet redundantes, é de extrema importância que esses links sejam de operadoras diferentes. Utilizamos um link de fibra ótica (Oi Telemar) e um link via rádio frequência (NetWay Telecom).



Quando uma operadora apresenta falha na comunicação, outro link entra em ação de forma automática sem que os usuários percebam.

Gateways

Name	RTT	RTTsd	Loss	Status
WANGW	0.0ms	0.0ms	100%	Offline
WAN_NETWAYGW	4.0ms	3.4ms	0.0%	Online

6.10.4.3. Memória RAM:

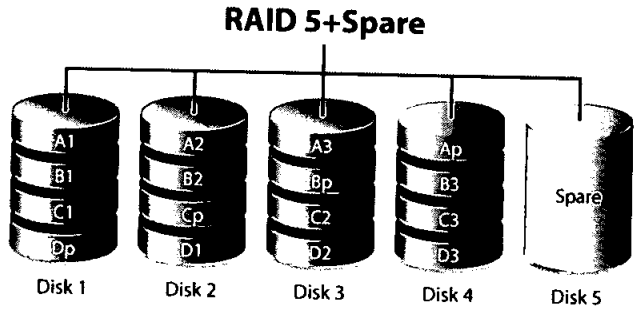
6.10.4.3.1 A redundância também pode ser usada na memória RAM dos dispositivos do PREVINI, garantindo que, quando um problema surge em um de seus componentes, os demais deem conta do recado. Um ponto importante é entender que a velocidade do dispositivo pode ser impactada, caso o total de memória disponível para as operações não seja alta, sobrecarregando as atividades.

6.10.4.3.2 Os servidores do PREVINI trabalham com sobra de memória para justamente poder receber serviços de outro servidor que apresentou falha de memória, algo que é muito comum em um ambiente virtualizado. Importante ressaltar que todas as memórias dos servidores são ECC (Error Correction Check) o que garante ainda mais possíveis erros de memória.

6.10.4.3. Dados:

6.10.4.3.1. As redundâncias nos dados são feitas com técnicas e equipamentos que vão garantir que eles sobrevivam a qualquer tipo de desastre e estejam sempre disponíveis.

6.10.4.3.2. O PREVINI utiliza em sua estrutura um equipamento chamado "Storage" sendo um dos principais componentes de datacenters, atualmente a storage funciona com RAID 5 de Hardware. Caso qualquer um dos discos venha a falhar, as controladoras são capazes de calcular e recuperar em tempo real os dados contidos no disco defeituoso, permitindo assim que o sistema continue operando mesmo sem um dos discos.



6.10.4.3.3. Uma das finalidades de um Storage também é expandir a capacidade e performance de armazenamento sem que tenha um impacto direto na produção. Em outras palavras, seria permitir um armazenamento inteligente de dados.

6.10.4.4. Backup:

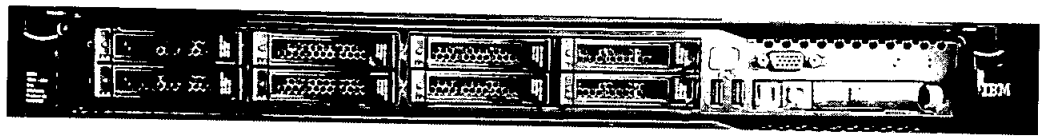
6.10.4.4.1 O PREVINI trabalha com uma política de backups consistente e, pelo menos, dois locais de armazenamento diferentes. Uma boa política de backups é aquela que faz cópias de segurança dos dados em intervalos curtos que possam ser medidos em horas. Dessa forma, se algum tipo de falha afeta os sistemas principais de uma empresa, boa parte do trabalho ainda pode ser recuperada nos backups. Como existe a possibilidade dos dados corrompidos ou malwares prejudicarem um backup, é muito recomendável que existam também cópias de datas um pouco mais antigas, que possam ser acessadas nesses casos. Em relação aos locais de armazenamento, é extremamente recomendável que eles sejam distantes o bastante para garantir a segurança dos dados em catástrofes naturais: mesmo se a cidade em que um datacenter está instalado for devastada por uma inundação, os dados sobreviverão em outro local geograficamente afastado. Outra técnica importante é contar com, pelo menos, um backup armazenado na nuvem, o que garante disponibilidade e segurança de dados maior do que datacenters físicos.

No PREVINI tomamos todo o cuidado com o Backup e a aplicação de boas práticas conforme descrito no passo a passo de toda a funcionalidade de backup desde a instalação da aplicação até a restauração de algum dado ou informação, conforme descrito abaixo:

Instalação do ARCserve

A aplicação é totalmente licenciada, instalada por parceiros e foi homologada pelo setor de T.I. do PREVINI. Atualmente sendo executado em um servidor IBM System x3550 M3 (imagem

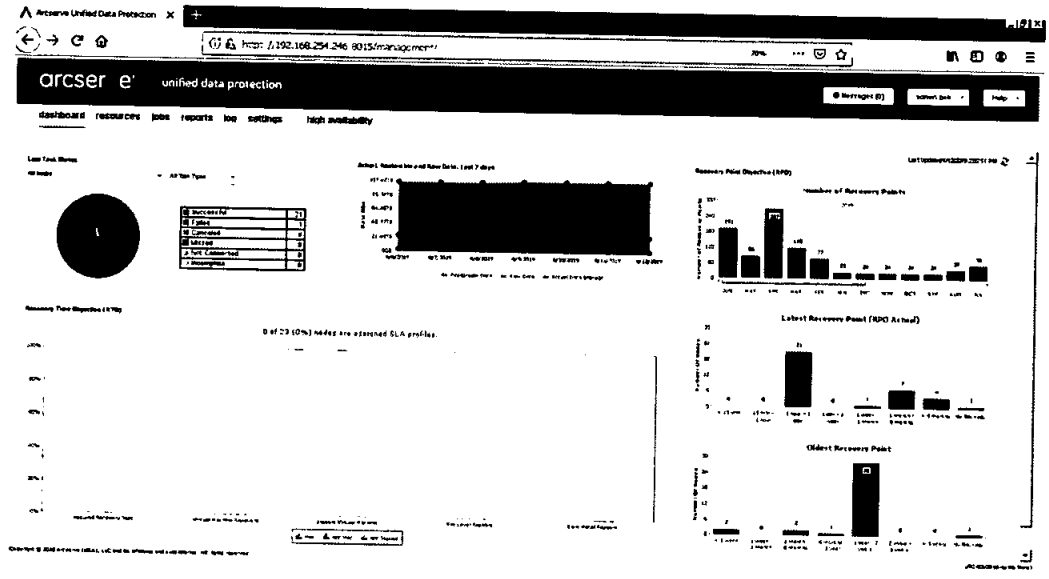
abaixo) com 96 GB de memória RAM, 8 discos SAS em Raid 5 (redundância), 2 (duas) fontes de energia redundantes funcionando sobre a plataforma Microsoft Windows Server 2008 R2.



A solução Arcserve UDP permite expandir com facilidade as topologias para continuidade dos negócios localmente ou por longas distâncias (e em vários locais), inclusive provedores de nuvem e de serviços. A instalação é feita com alguns cliques. A aplicação utiliza um recurso de deduplicação (processo de analisar identificar e remover duplicidade nos dados, diminuindo assim a quantidade de informação a ser manipulada e armazenada).

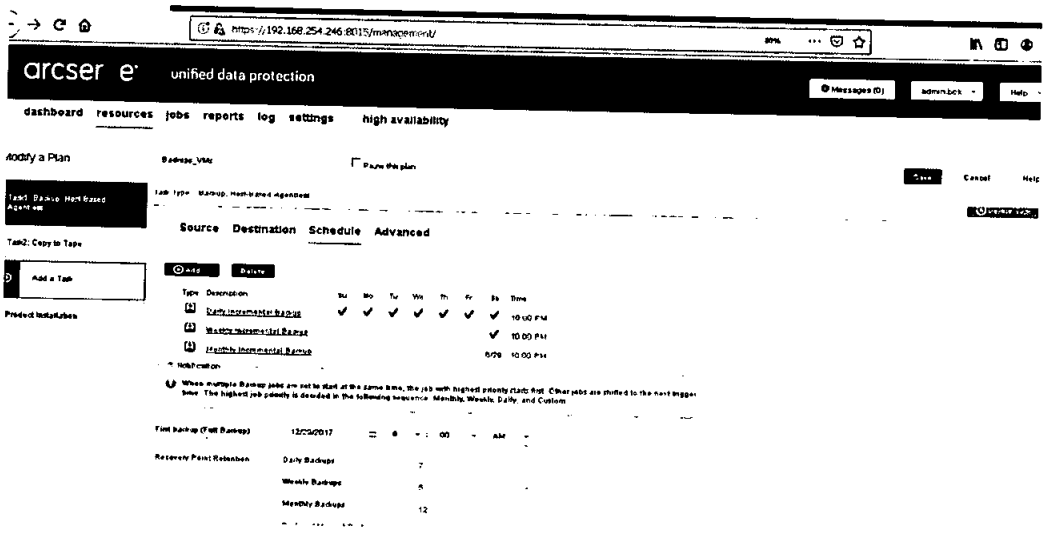
A aplicação ARCSERVE funciona através de navegadores WEB pela da porta HTTPS (443). Para acessar a aplicação deve ser informa usuário e senha (imagem abaixo), garantindo assim segurança no acesso da aplicação.

Ao acessar a aplicação, podemos visualizar a tela que chamamos de "dashboard", onde são mostrados diversos gráficos a respeito dos planos de backups. Nessa tela podemos verificar os status de backups (Successful, Failed, Canceled, Missed, Not Connected e Incomplete) o que facilita na tomada de decisões quando necessário.

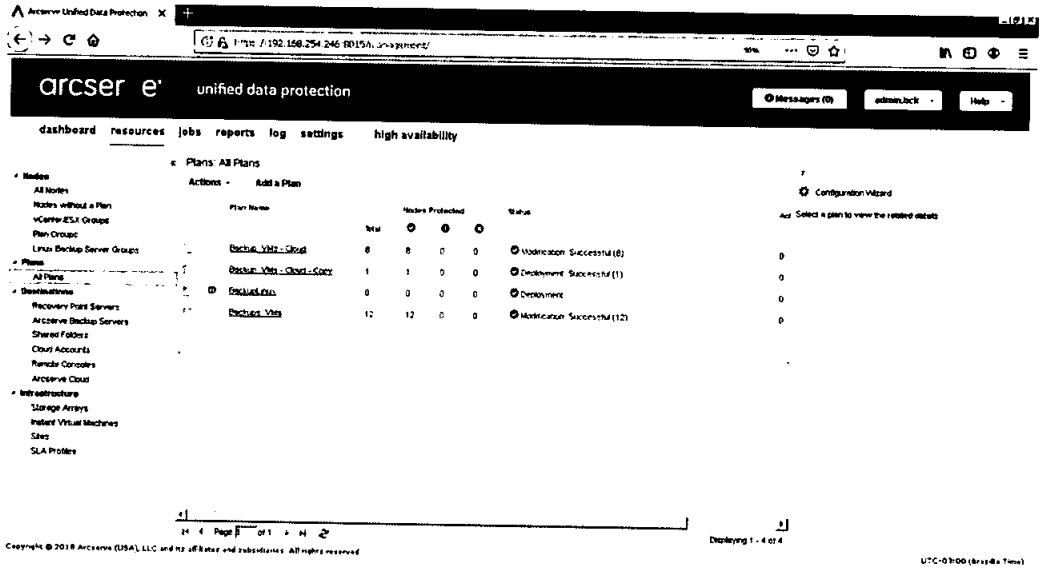


Ao acessar a opção resources podemos visualizar diversas configurações e principalmente a área de planos de backups (all plans) criados e a possibilidade de criar mais planos, caso seja necessário.

Os backups são feitos de forma incremental diariamente e seu inicio sempre a partir das 22:00h.

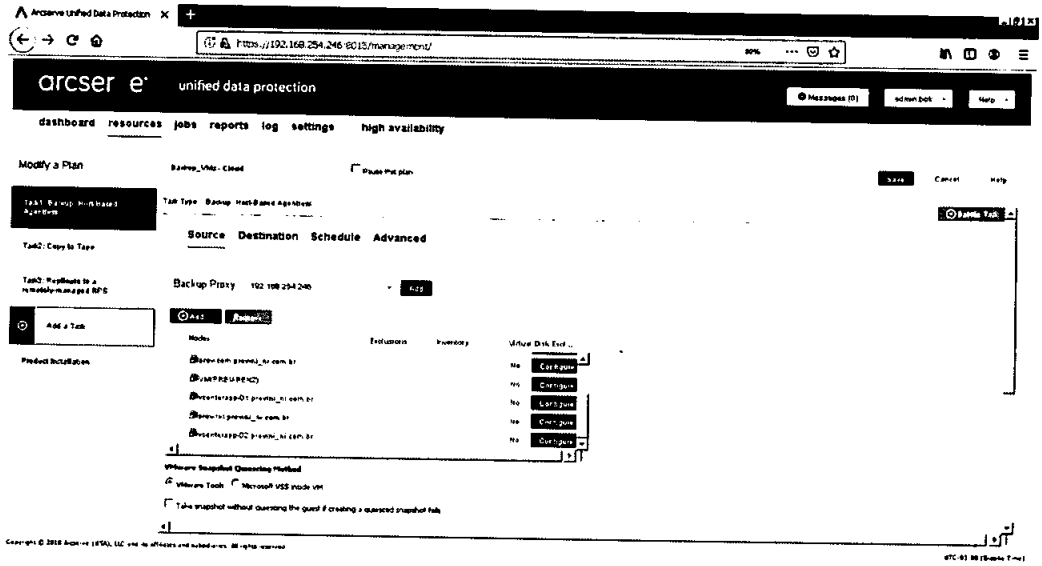


Para a nossa estrutura atual utilizamos basicamente 2 (dois) planos de backup (Backup VMs – Cloud e Backups VMs) conforme pode ser visto na tela abaixo:



- Backup VMs – Cloud: Esse plano foi criado para execução de backup de servidores mais importantes, são eles:

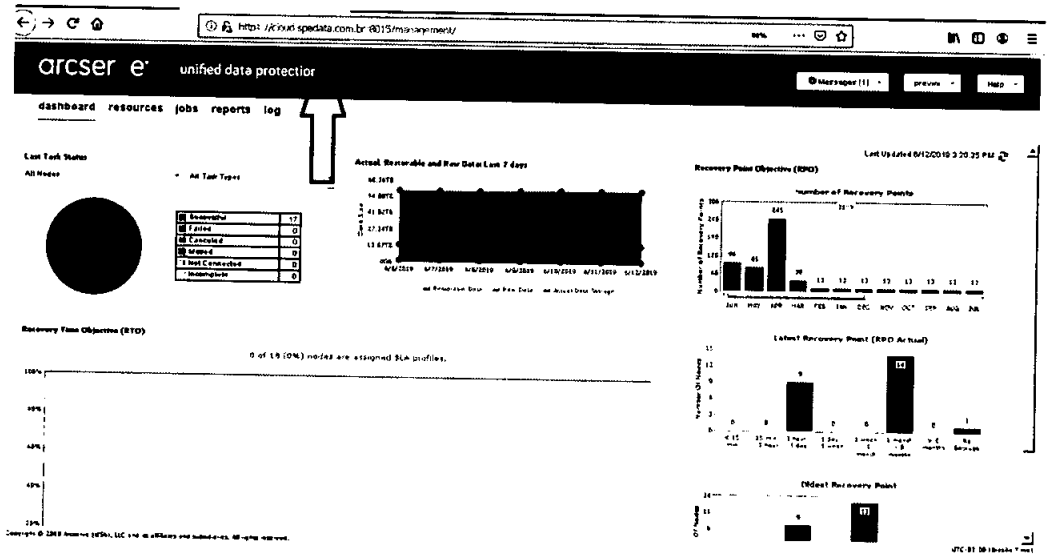
  - PREV-NET3 (Firewall)
  - PREV-SEC (Security Vmware)
  - PREV-CON (Connection Vmware)
  - PREV-COM (Compose Vmware)
  - PREV-BEN2 (Banco Postgres Softprevi)
  - PREV-BEM-APL (Servidor de Aplicação Softprevi)
  - PREV-SRV (Servidor de Arquivos ADDC)
  - PREV-TEL (Telefonia – Bilhetagem)
  - VcenterApp1 (Vcenter Servidores Virtuais)
  - VcenterApp2 (Vcenter VDI)



Após execução do backup em disco, são feitos de forma redundante os backup em fitas através de uma controladora IBM TS3100 Tape Library.

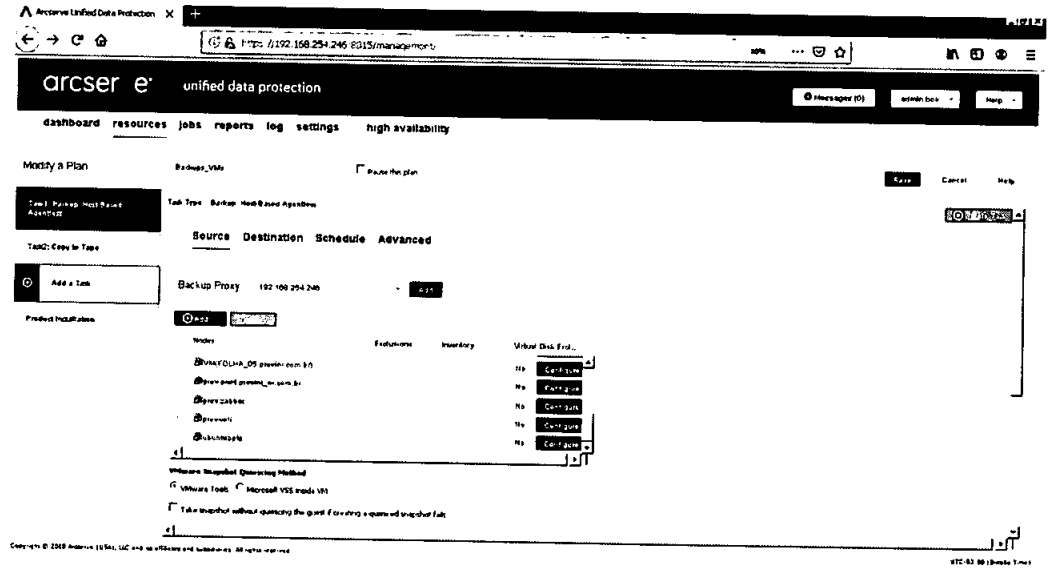
Após a conclusão do backup nas fitas, automaticamente inicia-se um serviço de réplica em nuvem.

Essa "nuvem" é disponibilizada através de contrato de serviço com a empresa SPE Data Informática (https://cloud.spedata.com.br:8015/management/), onde foram homologadas as devidas politicas de segurança de acesso tanto do lado de nossa instituição, quanto do lado da empresa contratada. Essa medida garante possíveis falhas contra desastre no prédio da instituição.

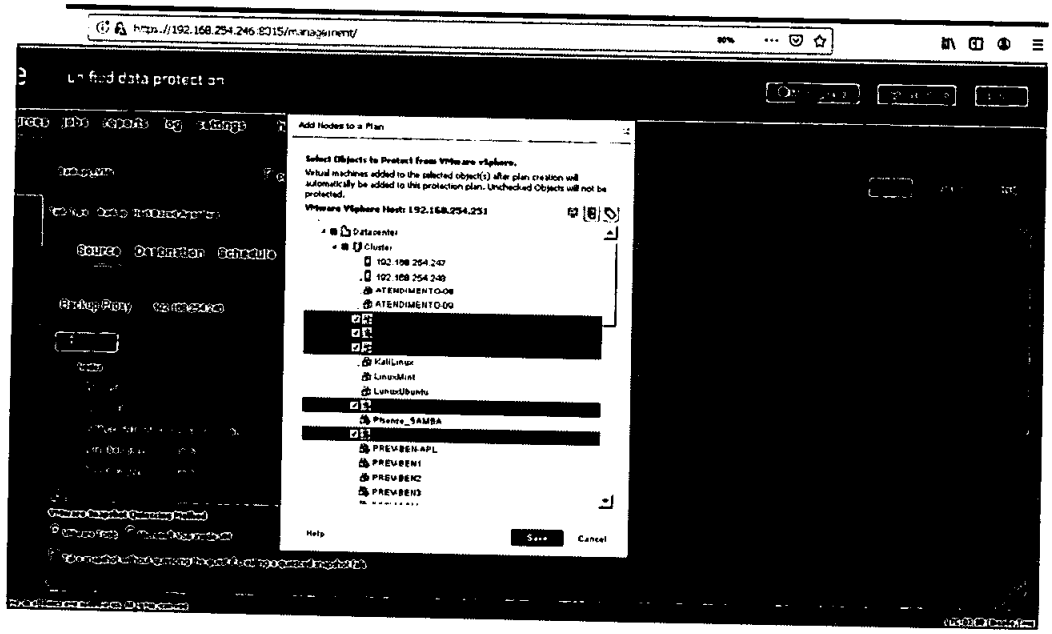


- Backup VMs: Esse plano foi criado para execução de backup de diversos servidores, são eles:

  - PROXYUDP (Restauração de BKP Linux)
  - PREV-WEB (Intranet)
  - PREV-BEN (Backup Imagens Softprevi)
  - PREV-FIN (Financeiro SIOP)
  - PREV-FIN2 (Financeiro Beta)
  - PREV-FIN3 (Financeiro Aplicação Modernização)
  - PREV-FIN4 (Financeiro Banco Modernização)
  - PREV-ZABBIX (Monitoramento)
  - PREV-WIFI (Gerenciador Wifi)
  - PREV-PPTP (VPN com a Prefeitura)

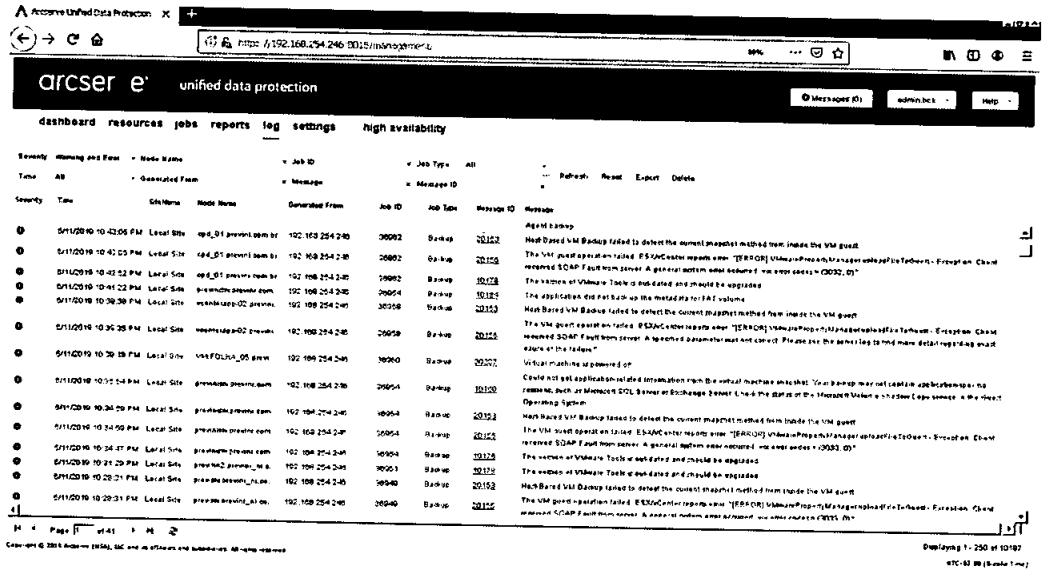


Caso seja necessária a modificação de um plano de backup existente e inclusão de um novo servidor no backup, basta clicar no plano com o botão direito do cursor (mouse) escolher a opção Modify na tela seguinte, clicar no botão Add e escolher a opção Add Nodes from a vCenter/ESX(i), na tela seguinte deverá ser informado o endereço e as credenciais do Vcenter, na tela seguinte, basta escolher o servidor que deseja incluir no plano de backup e clicar em Save.

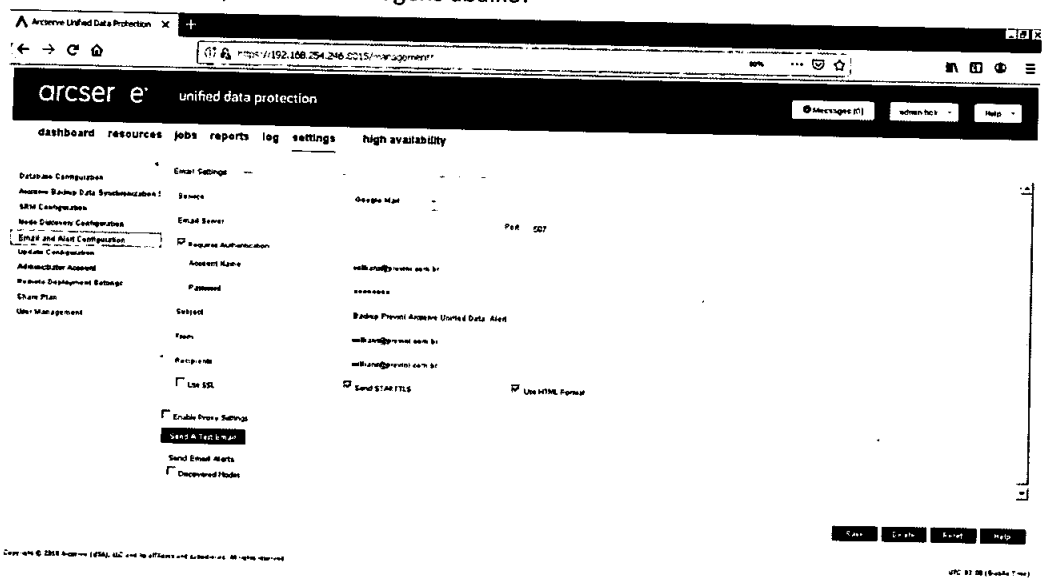


São feitos replicas de backups mensalmente também para um disco externo, onde esse disco fica armazenado fisicamente fora do prédio da instituição, assim garantindo também falhas contra desastres no prédio.

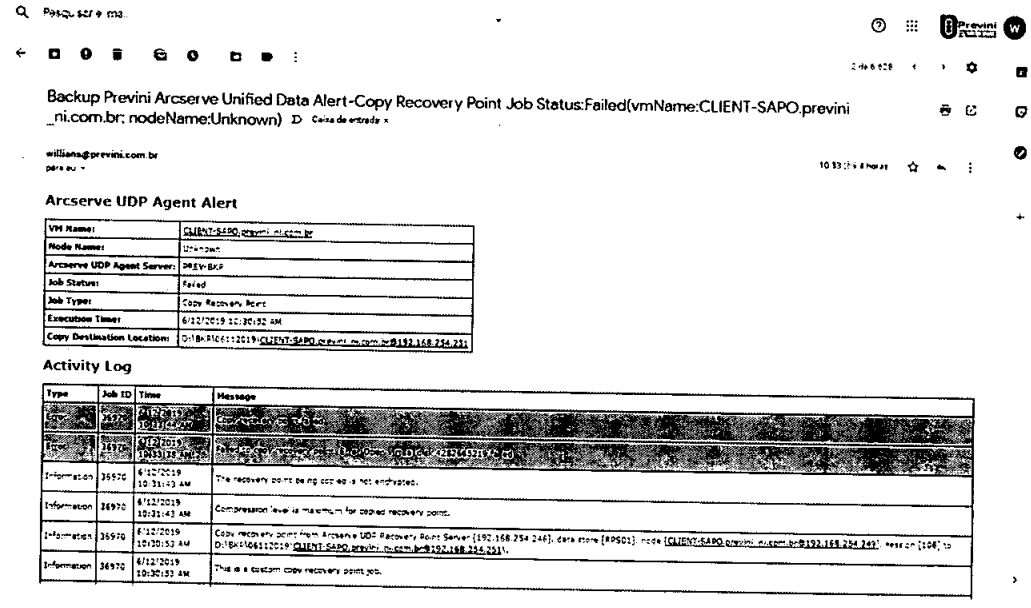
Ao acessar a opção de Log, podemos verificar todos os procedimentos de backup e também podemos verificar alertas e erros, o que facilita na administração dos backups.



Na opção Settings, podemos também configurar envio de alertas de erros e relatórios de conclusão de backup conforme imagens abaixo:



Abaixo podemos visualizar como exemplo um alerta enviado por e-mail a respeito de um erro ao tentar executar um backup:



Backup Previni Arcserve Unified Data Alert-Copy Recovery Point Job Status:Failed(vmName:CLIENT-SAPO.previni _ni.com.br; nodeName:Unknown)

williams@previni.com.br

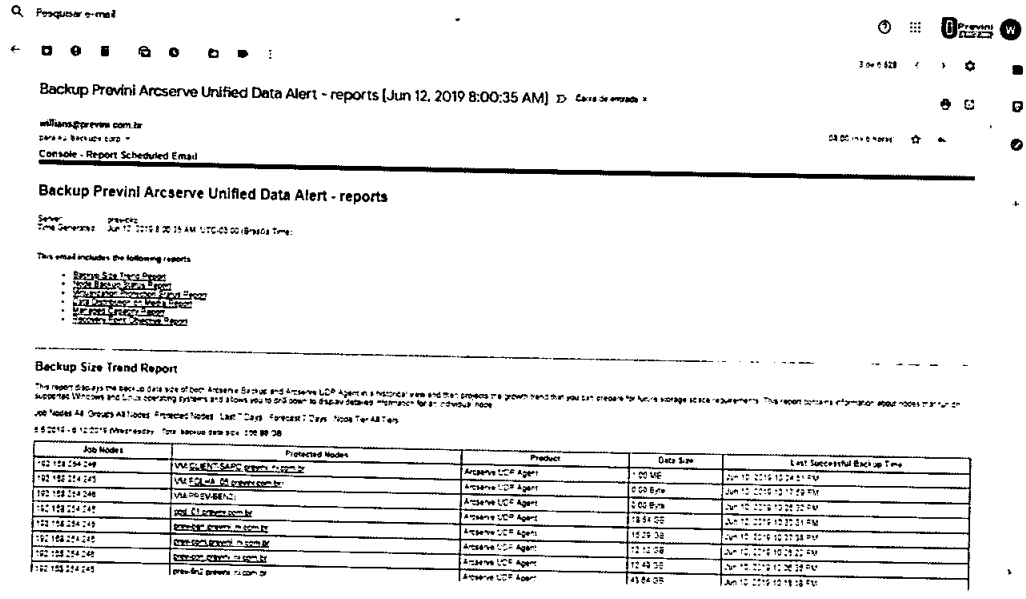
Arcserve UDP Agent Alert

VM Name:	CLIENT-SAPO.previni-ni.com.br
Node Name:	Unknown
Arcserve UDP Agent Server:	PREV-BKP
Job Status:	Failed
Job Type:	Copy Recovery Point
Execution Time:	6/12/2019 10:30:02 AM
Copy Destination Location:	D:\BackUp\06112019\CLIENT-SAPO.previni-ni.com.br@192.168.254.251

Activity Log

Type	Job ID	Time	Message
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
Information	36970	6/12/2019 10:31:43 AM	The recovery points being copied is not encrypted.
Information	36970	6/12/2019 10:31:43 AM	Compression level is maximum for copied recovery points.
Information	36970	6/12/2019 10:30:53 AM	Copy recovery point from Arcserve UDP Recovery Point Server [192.168.254.246], data store [RPSD1], node [CLIENT-SAPO.previni-ni.com.br@192.168.254.249], session [104], to D:\BackUp\06112019\CLIENT-SAPO.previni-ni.com.br@192.168.254.251\.
Information	36970	6/12/2019 10:30:53 AM	This is a custom copy recovery point job.

Abaixo podemos verificar um relatório de conclusão de backup recebido por email:



Backup Previni Arcserve Unified Data Alert - reports [Jun 12, 2019 8:00:35 AM]

williams@previni.com.br

Console - Report Scheduled Email

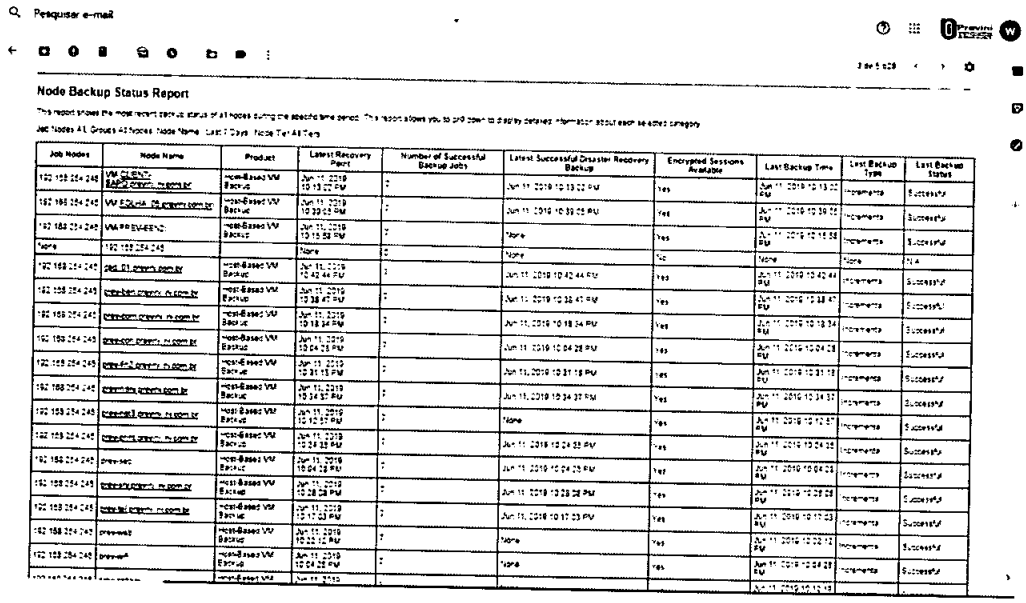
Backup Previni Arcserve Unified Data Alert - reports

This email includes the following reports:

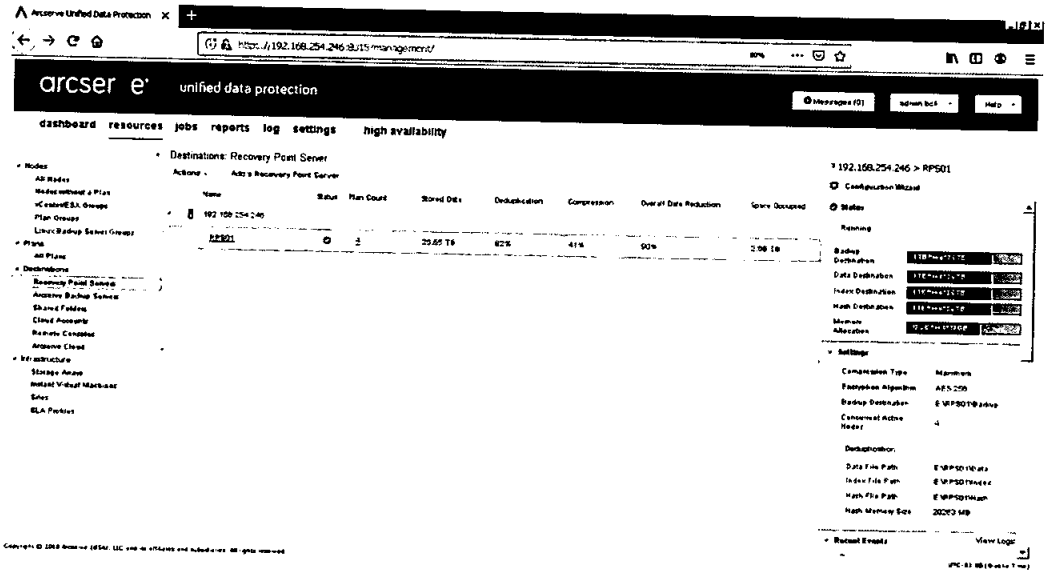
- Backup Size Trend Report
- Node Backup Status Report
- Protected Nodes Summary Report
- VM Summary by Host Report
- Backup Summary Report
- Recovery Point Summary Report

Backup Size Trend Report

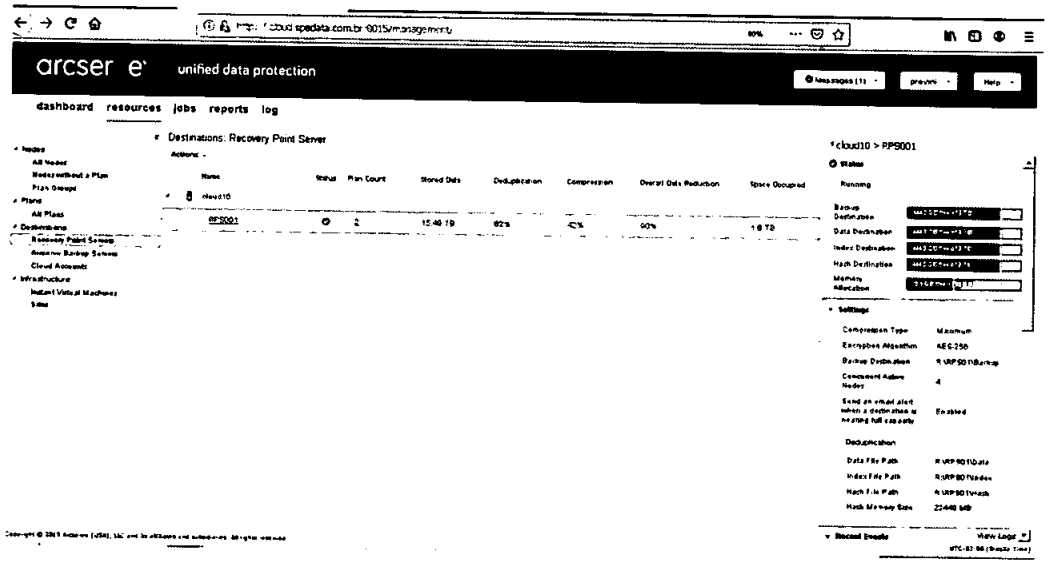
Job Nodes	Protected Nodes	Product	Data Size	Last Successful Backup Time
192.168.254.249	VM:CLIENT-SAPO.previni-ni.com.br	Arcserve UDP Agent	1.00 MB	Jun 12, 2019 10:24:31 PM
192.168.254.245	VM:FOLHA_04.previni.com.br	Arcserve UDP Agent	0.00 Byte	Jun 12, 2019 10:17:59 PM
192.168.254.246	VM:PREV-BENEF	Arcserve UDP Agent	0.00 Byte	Jun 12, 2019 10:20:20 PM
192.168.254.245	pos_01.arcserve.com.br	Arcserve UDP Agent	19.54 GB	Jun 12, 2019 10:31:31 PM
192.168.254.249	previnet.previni-ni.com.br	Arcserve UDP Agent	15.29 GB	Jun 12, 2019 10:31:58 PM
192.168.254.245	prev-sql.previni-ni.com.br	Arcserve UDP Agent	12.12 GB	Jun 12, 2019 10:25:22 PM
192.168.254.249	previsql.previni-ni.com.br	Arcserve UDP Agent	12.48 GB	Jun 12, 2019 10:36:38 PM
192.168.254.245	prev-fin2.previni-ni.com.br	Arcserve UDP Agent	41.84 GB	Jun 12, 2019 10:18:38 PM



Atualmente podemos verificar que o total de espaço utilizado em nosso RPS01 LOCAL (servidor de backup no instituto) é de 2.66 TB conforme demonstrado em imagem abaixo:

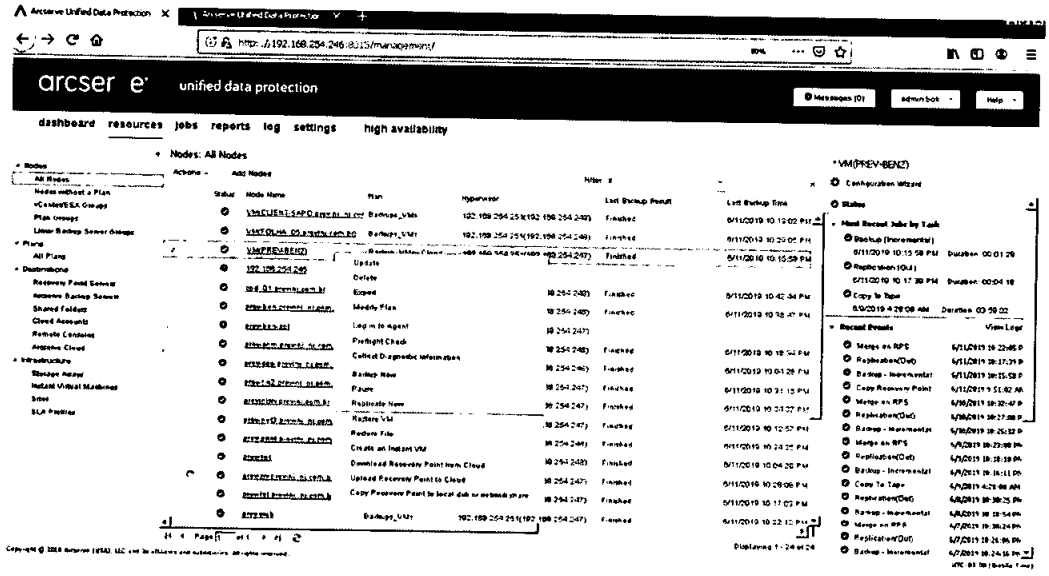


Atualmente podemos verificar que o total de espaço utilizado em nosso RPS01 REMOTO (servidor de backup em nuvem) é de 1.6 TB conforme demonstrado em imagem abaixo:

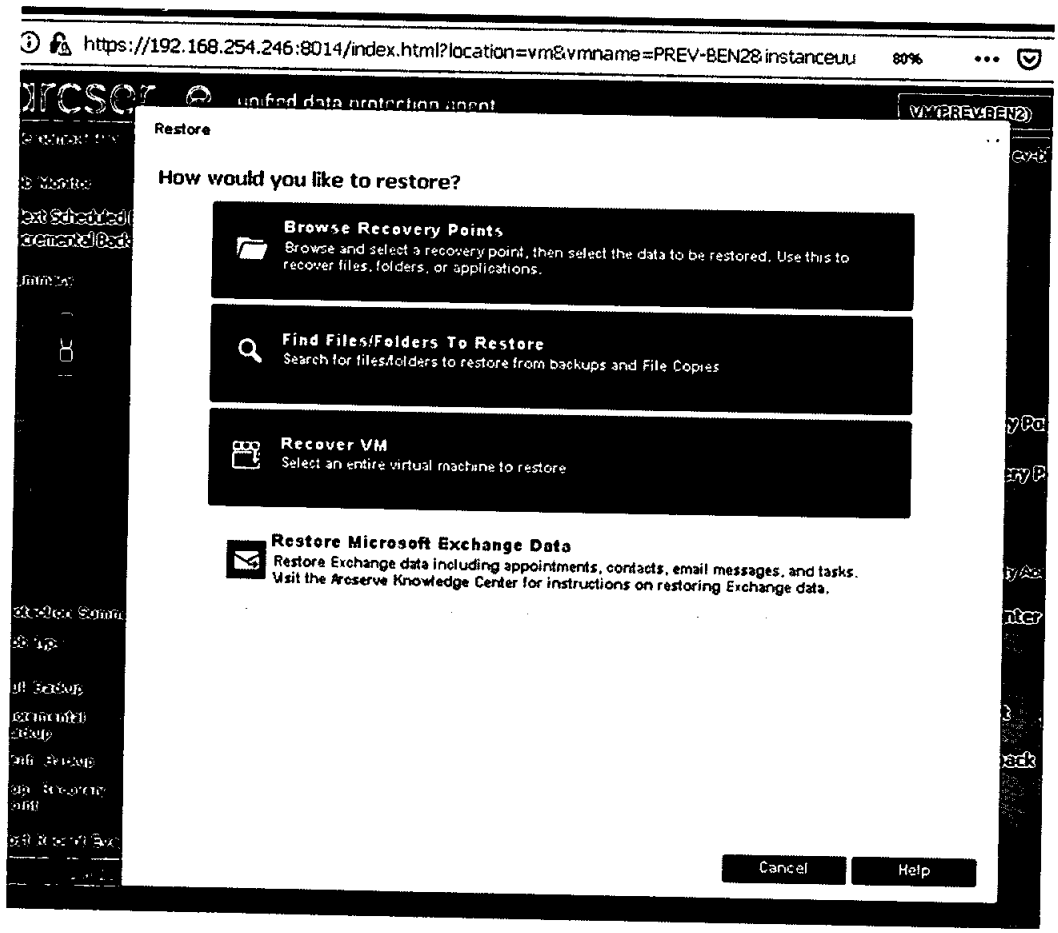


Restaurando um servidor de backup

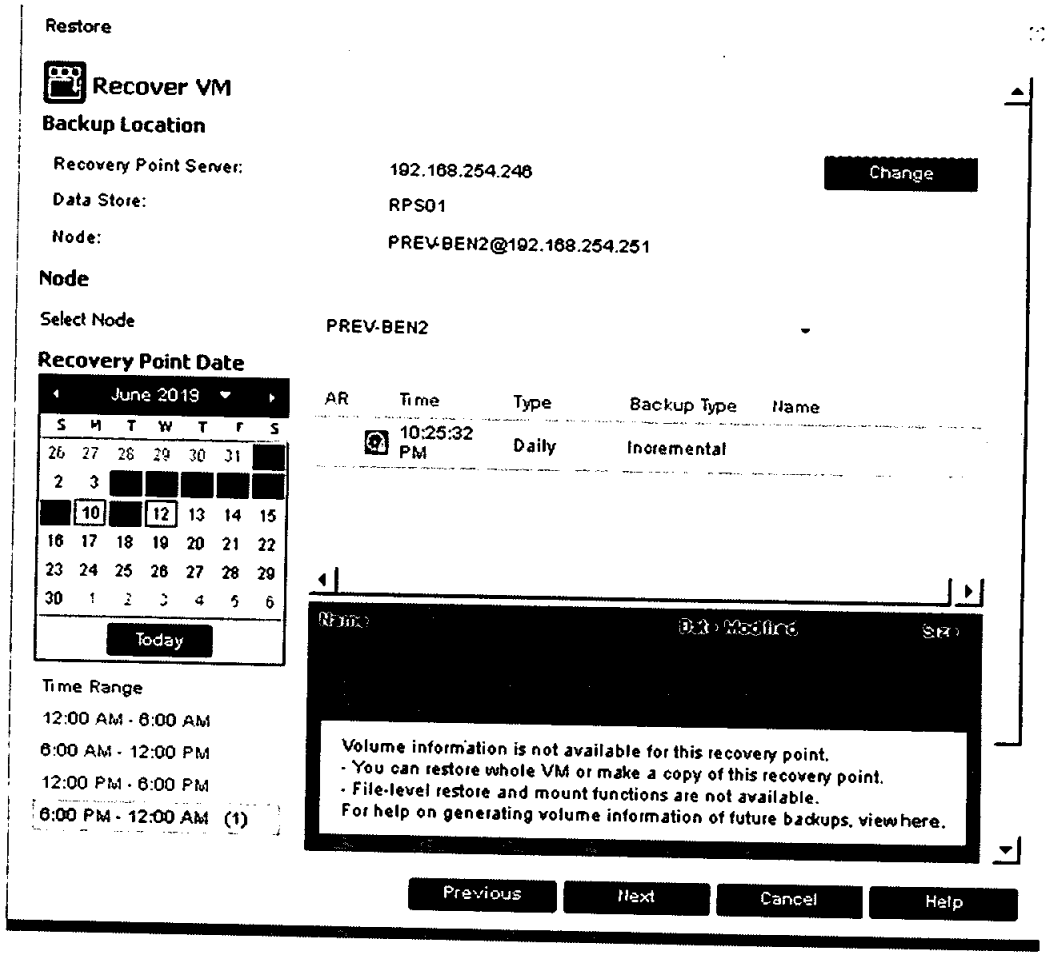
Para restaurar um servidor, basta abrir a opção resources e depois clicar em All Nodes, escolher o servidor que deseja restaurar e clicar na opção Restore VM.



Esolher a opção Recover VM

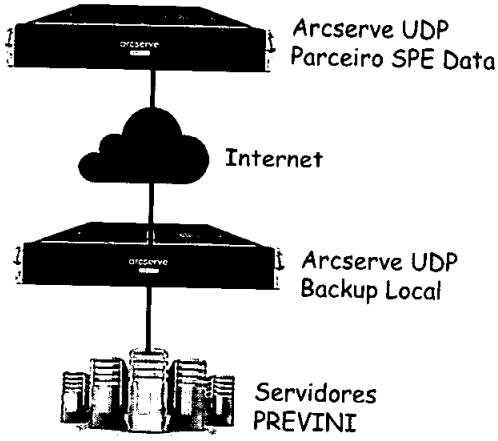


Escolher o ponto de restauração no calendário ao lado esquerdo e clicar em Next.



Ao final, o backup do servidor VM completo será restaurado.

Mapa da replicação do backup:



6.11. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

6.11.1. Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

6.11.2. O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

6.12. VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.

Nova Iguaçu, 05 agosto de 2019.

Anderson da Silva Moreira
Matrícula n° 60/200.036-6
Diretor Presidente

Willians de Azevedo Correa
Matrícula n° 11/100.040-5
Gerente da Divisão de Informática