Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

Categorias	Cód.
SEGURANÇA	1.1
SEGURANÇA	1.2
SEGURANÇA	1.3
SEGURANÇA	1.4
SEGURANÇA	1.5
SEGURANÇA	1.6

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.7

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.8
SEGURANÇA	1.9

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.10

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.11
SEGURANÇA	1.12
SEGURANÇA	1.13

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.14

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.15
SEGURANÇA	1.16
SEGURANÇA	1.17
SEGURANÇA	1.18

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.19
SEGURANÇA	1.20

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.21
SEGURANÇA	1.22

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.23
SEGURANÇA	1.24

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.25

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.26
SEGURANÇA	1.27
SEGURANÇA	1.28

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.29
SEGURANÇA	1.30

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.31
SEGURANÇA	1.32

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.33
SEGURANÇA	1.34

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.35
SEGURANÇA	1.36
SEGURANÇA	1.37

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.38
SEGURANÇA	1.39
SEGURANÇA	1.40
SEGURANÇA	1.41
SEGURANÇA	1.42

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.43
SEGURANÇA	1.44
SEGURANÇA	1.45

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

SEGURANÇA	1.46
SEGURANÇA	1.47
SEGURANÇA	1.48
SEGURANÇA	1.49
SEGURANÇA	1.50

Categorias	**Cód.**
CONTINUIDADE DE SERVIÇO	2.1
CONTINUIDADE DE SERVIÇO	2.2

Ambiente:	
Analista:	
Data da Realização:	
Sistema Operacional:	

CONTINUIDADE DE SERVIÇO	2.3
CONTINUIDADE DE SERVIÇO	2.4
CONTINUIDADE DE SERVIÇO	2.5
CONTINUIDADE DE SERVIÇO	2.6
CONTINUIDADE DE SERVIÇO	2.7
CONTINUIDADE DE SERVIÇO	2.8
CONTINUIDADE DE SERVIÇO	2.9
CONTINUIDADE DE SERVIÇO	2.10
CONTINUIDADE DE SERVIÇO	2.11
Categorias	**Cód.**
DESEMPENHO NAGIOS	3.1
DESEMPENHO NAGIOS	3.2
DESEMPENHO NAGIOS	3.3
DESEMPENHO NAGIOS	3.4
DESEMPENHO NAGIOS	3.5
DESEMPENHO NAGIOS	3.6
DESEMPENHO NAGIOS	3.7
Categorias	**Cód.**
DOCUMENTAÇÃO DO PROJETO	4.1
DOCUMENTAÇÃO DO PROJETO	4.2
DOCUMENTAÇÃO DO PROJETO	4.3
Categorias	**Cód.**
CADASTRO	5.1
CADASTRO	5.2

Check-List de Auditoria

CABEÇALHO

Itens	Auditoria
1.1 Definir o propósito do sistema operacional para a instalação mínima de pacotes. Antes da instalação, deve-se ter em mente qual serviço será executado pelo sistema operacional para que a instalação seja feita com o mínimo de pacotes e recursos possíveis, garantindo que não existirão arquivos e recursos desnecessários instalados	Conforme
1.2 Definir o particionamento do disco do sistema operacional. É recomendando a utilização de partições com filesystem tipo LVM e que as partições de alocação de dados (exemplo: /var e /home), partição de boot (/boot) e outras padrões do sistema operacional sejam criadas separados (/), desta forma, caso aconteça ocupação de 100% de uma partição que não seja a principal, o sistema operacional continuará funcional.	Conforme
1.3 Instalar o sistema operacional com o timezone adequado. O timezone deve ser configurado adequadamente pois esta configuração é essencial para a tratativa de incidentes de segurança e para análise de falha.	Conforme
1.4 Habilitar SELinux (Security-Enhanced Linux). O SELinux implementa vários níveis de segurança adicionais ao kernel do sistema operacional e deve ser habilitado. O modo que deve ser habilitado é o "enforcing", habilita ou na instalação ou atráves do arquivo /etc/selinux/config através da opção: SELINUX = enforcing	Não se Aplica
1.5 Implementar senha no gerenciador de boot (grub ou lilo). É recomendado que se implemente senha no gerenciador de boot do sistema operacional para que se tenha um nível de segurança adicional no acesso local (senha padrão definida pela equipe administração linux CTI)	Conforme
1.6 Realizar a atualização de patches de segurança e dos aplicativos do sistema operacional. O sistema operacional deve atualizado após a instalação. O sistema operacional sempre deve estar atualizado. É necessário que sejam criadas rotinas (automatizadas ou manuais) para fazer a atualização dos patches de segurança e dos aplicativos. Isto se faz necessário em virtude da velocidade com que são lançados exploits para exploração de vulnerabilidades recém-descobertas nos aplicativos e sistema operacional. Para evitar problemas em rotinas automatizadas, excluir das atualizações os pacotes do kernel (estes deverão ser atualizados manualmente). Para excluir no yum os pacotes relacionados ao kernel, inserir a seguinte linha no arquivo /etc/yum.conf: exclude=kernel*	Conforme

Check-List de Auditoria

CABEÇALHO

1.7 Desativar IPV6. Desabilitar nas configurações da interface de rede.	Conforme

Check-List de Auditoria

CABEÇALHO

1.8 Adequar o runlevel de inicialização do sistema para o modo adequado (sem interface gráfica). O sistema operacional deve estar programado para sempre entrar em execução com o nível de runlevel adequado (sem interface gráfica e outros recursos não necessários como o xfs).	Conforme
1.9 Especificar os servidores NTP do ambiente para o sincronismo do relógio do sistema operacional (10.32.9.230 - 10.32.8.1). O sincronismo do relógio é imprescindível para se fazer correlação de eventos ou tratar incidentes de segurança. O sincronismo do relógio deve estar sempre funcionando no sistema operacional. O sistema operacional deve possuir rotinas para fazer a sincronização do relógio periodicamente. O ideal é que o período máximo de intervalo entre as sincronizações seja de 30 minutos para que o relógio esteja sempre confiável. Para realizar esta configuração, logar com o usuário root e executar os seguintes comandos: chkconfig crond on service crond start crontab -e Inserir as seguintes linhas no crontab do usuário root: ########## Check List de Seguranca ################## 0,30 * * * * /usr/sbin/ntpdate -u 10.32.9.230 0,30 * * * * /usr/sbin/ntpdate -u 10.32.8.1 0,30 * * * * /sbin/hwclock --systohc ## RHEL instalar o pacote chrony vim /etc/chrony.conf server 10.99.113.11 iburst server 10.32.9.230 iburst server 10.32.8.1 iburst systemctl restart chronyd.service	Conforme

Check-List de Auditoria

CABEÇALHO

1.10 Configurar no kernel do sistema operacional, parâmetros de segurança relacionados a rede .
 	
Alguns parâmetros de rede podem ser modificados no kernel para garantir um nível adicional de segurança nos serviços oferecidos pela rede.
São exemplos de parâmetros para serem alterados no /etc/sysctl.conf:
net.ipv4.tcp_syncookies = 1 : habilita o mecanismo de cookies para a proteção de ataques do tipo "syn flood"
net.ipv4.tcp_max_syn_backlog = 1024 : configura o número máximo de requisições SYN que o servidor manterá na memória antes de receber o SYN_ACK do cliente
net.ipv4.icmp_echo_ignore_broadcasts = 1 : desabilita pacotes ICMP para endereços de broadcast
net.ipv4.ip_forward = 0 : desabilita o roteamento de pacotes entre as interfaces de rede do sistema
 	
OBS.: Se houver necessidade de habilitar o roteamento, checar no documento de apoio outros parâmetros que devem ser configurados.
 	
### Parametros Seguranca Check List #### 	
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 1024
net.ipv4.ip_forward = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
##############################
 	
RHEL7
/etc/sysctl.d/100-backlog.conf (CRIAR SE NAO TIVER)
 	
# Check List de Seguranca - PACELO 	
net.ipv4.tcp_max_syn_backlog = 1024
net.ipv4.tcp_syncookies = 1
net.ipv4.ip_forward = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
	Conforme

Check-List de Auditoria

CABEÇALHO

1.11 Desabilitar serviços desnecessários. O sistema operacional deve "ouvir" apenas nas portas que estejam em produção e sejam realmente necessárias, visto que o principal ponto de comunicação da rede com o sistema operacional é através das portas dos serviços. Deve ser realizada uma análise pelo administrador do ambiente a fim de identificar quais dos serviços podem ou não serem desabilitados. São exemplos de serviços que geralmente foram instalados por padrão e que, quase sempre podem ser desabilitados: Serviços iniciados via /etc/xinet.d: chargen, chargen-udp, cups-lpd, cups, daytime, daytime-udp, echo, echo-udp, eklogin, ekrb5-telnet, finger, gssftp, imap, imaps, ipop2, ipop3, krb5-telnet, klogin, kshell, ktalk, ntalk, pop3s, rexec, rlogin, rsh, rsync, servers, services, sgi_fam, talk, telnet, tftp, time e time-udp Serviços iniciados via /etc/rc.d/rc*.d: vsftp, apmd, avahi-daemon, canna, cups-config-daemon, FreeWnn, gpm, hidd, hpoj, hplip, innd, irda, isdn, kdcrotate, lvs, mars-nwe, messagebus, oki4daemon, privoxy, rstatd, rusersd, rwalld, rwhod, spamassassin, wine, nfs, nfslock, autofs, ypbind, ypserv, yppasswdd, portmap, smb, netfs, lpd, apache, httpd, tux, snmpd, named, postgresql, mysqld, webmin, kudzu, squid, cups, ip6tables, iptables, pcmcia, bluetooth e mDNSResponder Para configurar use chkconfig ou setup.	Conforme
1.12 Eliminar serviços que não implementam segurança adequada na comunicação ou na autenticação. Todos os serviços que não possuem nível adequado de segurança e que não implementam criptografia na comunicação devem ser removidos ou substituídos por serviços com um nível adequado de segurança (exemplo: Telnet, FTP, Rlogin, Rsh, Rcp, IMAP, POP, etc)	Conforme
1.13 Desabilitar a utilização do recurso CTRL+ALT+DEL no sistema operacional. Este recurso deve ser desabilitado no sistema operacional para evitar que o comando CTRL+ALT+DEL quando digitado no sistema operacional faça o servidor reiniciar. Para desabilitar o CTRL+ALT+DEL, editar o arquivo /etc/inittab e comentar a seguinte linha: #ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now RHEL7 systemctl disable ctrl-alt-del.target	Conforme

Check-List de Auditoria

CABEÇALHO

1.14 Remover ferramentas de compilação. Todas as ferramentas de compilação existentes no sistema devem ser removidas. Ferramentas de compilação são utilizadas por invasores para compilar códigos no sistema operacional com o objetivo de obterem o acesso de super usuário (root). Exemplo de ferramentas de compilação: gcc, gcc3, gcc3-c++, gcc3-g77, gcc3-java, gcc3-objc, gcc-c++, gcc-chill, gcc-g77, gcc-java, gcc-objc, bin86, dev86, cc, flex, bison e nasm. O comando a seguir, ajuda a identificar ferramentas de compilação instaladas no ambiente: rpm -qa | egrep "^gcc|java|bin86|dev86|cc|flex|bison|nasm"	Conforme

Check-List de Auditoria

CABEÇALHO

1.15 Implementar sulogin (single user login). O sulogin exige autenticação no modo "single" de inicialização. Esta configuração é necessária para se elevar o nível de segurança através do acesso local no servidor onde está instalado o sistema operacional. Para habilidar o sulogin, basta acrescentar a seguinte linha ao arquivo /etc/inittab: ~~:S:wait:/sbin/sulogin RHEL7 já é padrão	Conforme
1.16 Habilitar sistema de auditoria no sistema operacional (Auditd). O sistema de auditoria do Linux é necessário para análises de segurança em casos de comprometimento do sistema e em tratativas de falhas no sistema. Para instalar e executar o Laus, utilizar os seguintes comandos: chkconfig auditd on service auditd start As regras inseridas na instalação padrão, já oferecem níveis adequados de auditoria.	Conforme
1.17 Definir umask padrão para 077. O umask 077 manterá a criação padrão dos arquivos e diretórios no sistema operacional com o nível de acesso apenas para criador do arquivo ou diretório. Para configurar o umask, inserir a seguinte linha nos arquivos /etc/profile e /etc/csh.login: ####### CHECK LIST DE SEGURANCA ######### umask 077 ##	Não se Aplica
1.18 Limitar acesso ao usuário "root" via comando "su" apenas para o grupo "wheel". Este parâmetro fará uma restrição dos usuários que podem se tornar root no sistema operacional. Este modificação é mais uma camada para se elevar o nível de segurança do sistema. Somente usuários que pertencerem ao grupo "wheel" e possuírem a senha do root conseguirão ter acesso root através do comando "su". Para realizar esta configuração, descomentar a seguinte linha no arquivo /etc/pam.d/su: auth required pam_wheel.so use_uid	Não se Aplica

Check-List de Auditoria

CABEÇALHO

1.19 Implementar banner de aviso para os terminais locais e remotos do sistema. Banners com notificações de segurança no momento do acesso são sempre necessários e recomendados por institutos internacionais como mecanismo adicional de segurança informando que o acesso ao ambiente é restrito e monitorado. Os banners devem ser inseridos nos arquivos: /etc/issue, /etc/issue.net e /etc/motd ********** Permitido o uso somente para pessoas autorizadas ********** Individuos que utilizarem este equipamento sem autorizacao, ou em operacoes que excedam o nivel de autorizacao permitido, estarao sujeitos a penalizacoes e rigores da legislacao aplicavel. Qualquer um que utilize este sistema concorda previamente com o monitoramento e esta ciente que se atividades ilicitas e/ou criminais forem reveladas a partir deste, podera ser objeto de processo judicial e/ou criminal. **********	Conforme
1.20 Impedir que o usuário root possa se logar através do serviço de FTP e sempre que possível, configurar shell não válida para os usuários que são exclusivos para FTP. Se o serviço de FTP precisa estar rodando no servidor, garantir que o usuário root não possa se conectar através do FTP e criar shell não válida para os usuários de FTP de maneira que eles não possam se logar no ambiente utilizando outro meio. Considerar também o enjaulamento do serviço de FTP e os diretórios para navegação dos usuários. As seguintes configurações devem ser realizadas: 1) Inserção do usuário root no arquivo /etc/vsftpd/ftpusers para que ele não possa se logar no serviço de FTP 2) Adotar o comando usermod -s /sbin/nologin nome_do_usuario para atribuir shell não válida para usuários de FTP 3) Insrerir as seguintes linhas no arquivo /etc/vsftpd/vsftpd.conf para configurar o enjaulamento dos usuários: chroot_list_enable=YES chroot_list_file=/etc/vsftpd/chroot_list 4) Inserir no arquivo /etc/vsftpd/chroot_list, o nome dos usuários que serão enjaulados	Conforme

Check-List de Auditoria

CABEÇALHO

1.21 Manter serviço de correio restrito ao equipamento local (quando o servidor não for um mail server). Caso o servidor não seja um servidor de correio, o serviço de email deve estar restrito à interface loopback do sistema operacional, permitindo apenas que e-mails originados do próprio sistema sejam entregues. Para efetuar essa configuração: 1) Editar o arquivo /etc/mail/sendmail.mc alterando a seguinte linha: DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl 2) Gerar um novo arquivo /etc/mail/sendmail.cf: m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf 3) Reiniciar o serviço do sendmail: service sendmail restart	Não se Aplica
1.22 Instalar o pacote sysstat para verificação de histórico de utilização de recursos de I/O e CPU. O pacote sysstat é necessário para que se tenha um histórico semanal (armazenado em /var/log/sa/sar*) sobre a utilização dos recursos de I/O e CPU no sistema operacional para análises futuras de capacidade, falhas e segurança. Para instalar e executar o sysstat: yum install sysstat chkconfig sysstat on service sysstat start	Conforme

Check-List de Auditoria

CABEÇALHO

1.23 Habilitar recurso de contabilização de processos "psacct" no sistema operacional. Este recurso fará com que todos os comandos executados pelos usuários sejam gravados no sistema operacional para futuras análises e auditoria. O sistema deve estar sempre com este processo instalado e em execução, além de possuir rotinas que façam backup destas informações (/var/account). Para instalar e executar a auditoria de processos, utilizar os seguintes comandos: yum install psacct chkconfig psacct on service psacct start OBS: Os seguintes comandos estarão disponíveis após habilitada a auditoria: ac: mostra a quantidade de tempo (em horas) que um usuário ficou logado no sistema. lastcomm: mostra os últimos comandos executados por um usuário. sa: mostra um resumo dos últimos comandos utilizados. accton: habilita ou desabilita a auditoria.	Conforme
1.24 Replicar os log's do sistema operacional para um servidor centralizado (10.32.15.62). Os log's do sistema devem ser replicados em tempo real para uma base centralizada, pois, em casos de comprometimento do equipamento, o atacante tentará adulterar ou remover os log's locais do servidor. Deverá ser inserida a seguinte linha no arquivo /etc/syslog.conf: ########## REPLICAR SERVIDOR DE LOG ########## *.* @10.32.15.62 ##	Não se Aplica

Check-List de Auditoria

CABEÇALHO

1.25 Manter os níveis adequados de severidade na configuração de syslog. As severidades do syslog devem ser mantidas adequadamente, pois garantem que as informações relacionadas à cada situação estejam nos arquivos adequados do sistema para análise de segurança e auditoria. No mínimo, as seguintes linhas devem estar presentes no arquivo /etc/syslog.conf: ## # Log all kernel messages to the console. # Logging much else clutters up the screen. #kern.* /dev/console # Log anything (except mail) of level info or higher. # Don't log private authentication messages! *.info;mail.none;authpriv.none;cron.none /var/log/messages # The authpriv file has restricted access. authpriv.* /var/log/secure # Log all the mail messages in one place. mail.* -/var/log/maillog # Log cron stuff cron.* /var/log/cron # Everybody gets emergency messages *.emerg * # Save news errors of level crit and higher in a special file. uucp,news.crit /var/log/spooler # Save boot messages also to boot.log local7.* /var/log/boot.log	Conforme

Check-List de Auditoria

CABEÇALHO

1.26 Manter os arquivos de log com as permissões mais restritivas possível. Os logs do sistema operacional gerados pelo syslog, ou logs com informações confidenciais de aplicações instaladas devem possuir o nível adequado de permissão. Somente os usuários utilizados pelas respectivas aplicações devem ser os proprietários dos arquivos de log e a permissão de leitura destes logs devem ser a mais restritiva possível.	Conforme
1.27 Gravar data e hora no bash history. Implementar no /etc/profile sendo configurado para todos os usuários do sistema. ############ CHECK LIST DE SEGURANCA ############ HISTTIMEFORMAT="%c -> " TMOUT=1800 export HISTTIMEFORMAT TMOUT ##	Conforme
1.28 Garantir que informações dos comandos last, lastb e lastlog estejam funcionando. Os comandos last, lastb e lastlog devem estar funcionando perfeitamente. Estes comandos invocam arquivos binários que contém informações de acesso ao sistema. last: mostra a listagem dos últimos usuários que logaram no sistema, incluindo a hora do login, hora do logout, endereço IP, etc. lastb: mostra o mesmo conteúdo do comando last, acrescentando o conteúdo do arquivo (touch /var/log/btmp) que contém todas as tentativas de login sem sucesso. lastlog: mostra o conteúdo do arquivo /var/log/lastlog que contém o registro do último login dos usuários.	Conforme

Check-List de Auditoria

CABEÇALHO

1.29 Desabilitar core dumps. Arquivos de core armazenam informações que estavam em uma determinada área da memória em um momento de erro. Se a informação não está criptografada ou protegida, os arquivos de core podem revelar informações confidenciais. Desta forma, core dumps devem ser habilitados apenas quando houver necessidade de se fazer "debug" de erros em programas. Para desabilitar core dumps, inserir as seguintes linhas no arquivo /etc/security/limits.conf: ## ############ CHECK LIST DE SEGURANCA ############## * soft core 0 * hard core 0 ##	Conforme
1.30 Habilitar a complexidade da senha. É recomendável que o sistema exiga complexidade da senha atribuída aos usuários. A recomendação é que a senha tenha um tamanho mínimo, que seja composta por caracteres maisúsculos, minúsculos, dígitos e caracteres especiais. Para realizar esta configuração, editar o arquivo /etc/pam.d/system-auth e inserir os parâmetros minlen (tamanho mínimo), lcredit (número mínimo de caracteres minúsculos), ucredit (número mínimo de caracteres maiúsculus), dcredit (número mínimo de dígitos) e ocredit (número mínimo de caracteres especiais) na seguinte linha (considerando que o número de caracteres de cada grupo seja 1 e que o tamanho mínimo da senha seja 8). Cada sistema operacional tem a configuração do pam.d especifica, nesse caso é necessário ficar atento, abaixo segue um exemplo da configuração no Red Hat 5.8. password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1	Não se Aplica

Check-List de Auditoria

CABEÇALHO

1.31 Habilitar o recurso para bloquear usuários após "n" tentativas de login incorretas. Este recurso é necessário para proteger o usuário em casos de ataques de dicionário ou força bruta, pois caso aconteçam "n" tentativas de acesso repetidamente com usuário e senha inválidos o sistema irá bloquear a conta do usuário durante um período configurável (recomendado 15 minutos). Para realizar esta configuração, editar o arquivo /etc/pam.d/system-auth e inserir as linhas, considerando que "deny=5" (5 tentativas) e que o período em que a conta ficará bloqueada é "unlock_time=1800" (30 minutos). Cada sistema operacional tem a configuração do pam.d especifica, nesse caso é necessário ficar atento, abaixo segue um exemplo da configuração no Red Hat 5.8. auth required pam_tally2.so deny=5 onerr=fail unlock_time=1800 account required pam_tally.so Caso tenha autenticação via IPA ou LDAP, a policita pode ser habilitada la em vez de ser local.	Não se Aplica
1.32 Habilitar no sistema operacional para que não sejam aceitas as "n" senhas utilizadas anteriormente. Este recurso deve ser implementado para que um determinado usuário não faça rodízio de senhas conhecidas e utilizadas recentemente no ambiente. O sistema deve exigir que as "n" últimas senhas utilizadas não sejam reaproveitadas. Para realizar esta configuração, editar o arquivo /etc/pam.d/system-auth e inserir o parâmetro remember=n na seguinte linha (considerando que "n"=15): Cada sistema operacional tem a configuração do pam.d especifica, nesse caso é necessário ficar atento, abaixo segue um exemplo da configuração no Red Hat 5.8. password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok remember=15 Caso tenha autenticação via IPA ou LDAP, a policita pode ser habilitada la em vez de ser local.	Não se Aplica

Check-List de Auditoria

CABEÇALHO

1.33 Configurar política de segurança relacionada ao login. Habilitar tempo máximo de validade da senh, a senha poderá ser utiliza por no máximo 90 dias. Habilitar tempo mínimo de validade da senha, o usuário precisará esperar pelo menos 1 dia para alterá-la novamente. Habilitar recurso para notificação antecipada da expiração da senha, será informado ao usuário que sua senha está prestes à expirar, apresentado 15 dias antes. Minimo tamanho de senha aceitavel. vim /etc/login.defs ############ CHECK LIST DE SEGURANCA ########## PASS_MAX_DAYS 90 PASS_MIN_DAYS 1 PASS_MIN_LEN 6 PASS_WARN_AGE 15 ## Habilitar recurso para bloquear a conta do usuário após "n" dias de expiração da senha. Após a data da expiração da senha, o usuário terá 2 dias para alterar sua senha antes da conta ser bloqueada vim /etc/default/useradd INACTIVE=2	Conforme
1.34 Desativar autenticação de usuários sem senha (/etc/ssh/sshd_config). Não permitir que usuários com senha em branco acessem o equipamento através do SSH. Parâmetro configurado: PermitEmptyPasswords no	Conforme

Check-List de Auditoria

CABEÇALHO

1.35 Não permitir login direto com o usuário root no protocolo SSH (/etc/ssh/sshd_config). Permissão de acesso direto com super usuário no sistema eleva o risco de comprometimento do servidor além de não garantir a rastreabilidade adequada em incidentes de segurança e falhas. Parâmetro configurado: PermitRootLogin no Caso precise de root deixar PermitRootLogin yes e habilitar o /etc/security/acess.conf - : root : ALL EXCEPT 10.11.148.53 rsyslogprd 10.32.14.13 usrv07 tty1 172.23.4.1 172.23.16.1 127.0.0.1 LOCAL + : ALL : cron crond * é necessário habilitar no PAM, a linha é a do meio (pam_access) e deve estar entre nologin e auth. /etc/pam.d/sshd account required pam_nologin.so account required pam_access.so account include password-auth	Conforme
1.36 Habilitar recurso "Privilege Separation" no protocolo SSH (/etc/ssh/sshd_config). Este recurso faz a separação dos processos do SSH. Isso possibilita que o processo seja executado com usuário não privilegiado e enjaulado no disco do sistema operacional. Parâmetro configurado: UsePrivilegeSeparation yes RHEL7 UsePrivilegeSeparation sandbox # Default for new installations.	Conforme
1.37 Habilitar apenas a versão 2 do protocolo SSH (/etc/ssh/sshd_config). Foram descobertas várias falhas de segurança na implementação da versão 1 do protocolo SSH. A versão 2 implementa criptografia e mecanismos de segurança mais robustos. Parâmetro configurado: Protocol 2	Conforme

Check-List de Auditoria

CABEÇALHO

1.38 Desabilitar "Port Forwarding" no protocolo SSH (/etc/ssh/sshd_config). Port Forwarding é um mecanismo utilizado para fazer redirecionamento de portas no sistema operacional. Esta opção deve ser mantida sempre desabilitada pois um atacante pode utilizá-la para abrir shell's reversas e outros recursos indesejáveis no sistema. Parâmetros que devem ser configurados: AllowTcpForwarding no GatewayPorts no X11Forwarding no	Conforme
1.39 Habilitar recurso "Strict Mode" no protocolo SSH (/etc/ssh/sshd_config). Este recurso faz com que seja necessário manter um nível mais restritivo de permissões no diretório home do usuário criado no servidor que está recebendo a conexão SSH. Esta configuração eleva o nível de segurança do protocolo. Parâmetro configurado: StrictModes yes	Conforme
1.40 Atribuir banner de segurança que informe "acesso restrito e monitorado" antes do logon do usuário (/etc/ssh/sshd_config). É recomendado que seja apresentado um banner de alerta informando que o acesso é restrito, monitorado e se atividades ilícitas forem registradas, os logs poderão ser utilizados perante a Lei. OBS .: Para máquinas com configuração de Oracle RAC é recomendando desabilitar essa opção no momento de configuração do RAC, caso contrario poderá dar erro ao montar o OCFS2. Parâmetro configurado: Banner /etc/issue.net	Conforme
1.41 Restringir acesso ao ssh apenas ao grupo de usuários de administração do SO (AllowUsers) (/etc/ssh/sshd_config). A opção AllowUsers, especifica e controla quais usuários podem acessar o servidor via ssh. Vários usuários podem ser especificados, separados por espaços.	Não se Aplica
1.42 Desabilitar subsystem sftp do protocolo SSH (caso não seja utilizado) (/etc/ssh/sshd_config). O SFTP é um subsystem externo ao SSH que permite a transferência de arquivos utilizando o protocolo SSH. Caso não haja necessidade de utilização de transferência de arquivos através de SFTP deve-se desabilitar o subsystem para diminuir possibilidades de exploração de vulnerabilidades no protocolo ou vazamento de informações confidenciais. Parâmetro configurado: #Subsystem sftp /usr/libexec/sftp-server	Não se Aplica

Check-List de Auditoria

CABEÇALHO

1.43 Bloquear logon de usuários que não possuem senha definida (/etc/ssh/sshd_config). Não permitir que usuários com senha em branco acessem o equipamento através do SSH. Parâmetro configurado: PermitEmptyPasswords no	Conforme
1.44 Manter somente o usuário root com UID 0. Somente o usuário root deve ter o UID 0. Se existirem outros usuários com a mesma permissão do super usuário, a rastreabilidade de eventos poderá se tornar impossível, pois, os logs apontarão apenas o acesso do root. Um comando que pode facilitar a identificação de usuários com UID 0 é: getent passwd | awk -F: '$3 == "0" { print $1 }'	Conforme
1.45 Manter as permissões corretas para os arquivos do sistema e logs. Os arquivos contendo logs das aplicações e do sistema operacional, além de outros arquivos do sistema, devem manter suas permissões no nível mais restritivo suportado pelas aplicações evitando que seu conteúdo seja revelado ou alterado de maneira não autorizada. chmod 400 /var/spool/cron chmod 400 /etc/shadow chmod 400 /etc/crontab chmod 600 /etc/securetty chmod 640 /etc/syslog.conf chmod 640 /etc/rsyslog.conf chmod 640 /etc/sysctl.conf chmod 640 /var/log/wtmp chmod 640 /var/log/lastlog chmod 664 /etc/security/limits.conf chmod 664 /etc/csh.login chmod 644 /etc/group chmod 644 /etc/passwd	Conforme

Check-List de Auditoria

CABEÇALHO

1.46 Impedir que existam usuários com senhas em branco. O sistema não deve possuir usuários com senhas "vazias", pois usuários sem senhas elevam muito o nível de exposição do sistema, possibilitando a um invasor entrar no sistema sem necessitar de uma senha válida. Comando abaixo verifica usuários que não possuem uma senha definida (favor desconsiderar os usuarios de servicos do SO): cat /etc/shadow | awk -F: '$2 == "!!" { print $1 }'	Conforme
1.47 Utilizar a última versão estável do agente de monitoramento escolhido (Nagios_plugin). Instalar o Nagios Plugin.	
1.48 Adequar o serviço do agente escolhido para iniciar automáticamente junto com os outros serviços do sistema operacional (rc.local/wwtask - Trauma0). Instalar o Trauma0	
1.49 Garantir que os agentes estejam configurados de forma correta de acordo com os procedimentos. Garantir que os agentes do Trauma0 e Nagios Plugin estejam configurados corretamente.	

1.50 Adequação do SYSSTAT.
 	
vim /etc/cron.d/sysstat
 	
# run system activity accounting tool every 10 minutes 	
*/10 * * * * root /usr/lib64/sa/sa1 1 1
# generate a daily summary of process accounting at 23:53 	
53 23 * * * root /usr/lib64/sa/sa2 -A
 	
vim /etc/sysconfig/sysstat
 	
# How long to keep log files (days), maximum is a month 	
HISTORY=30
COMPRESSAFTER=2
	Conforme

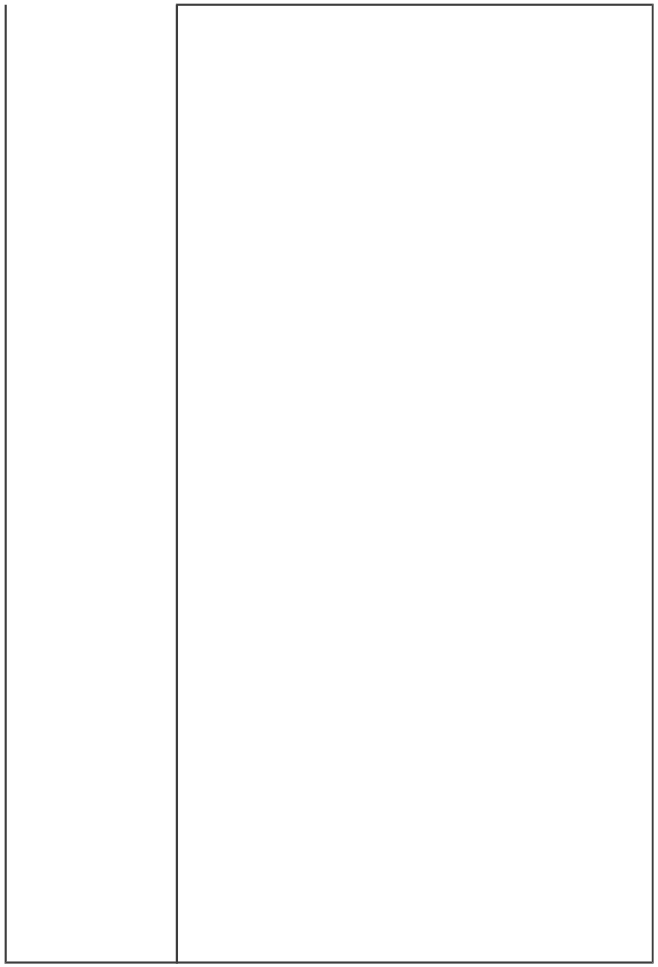
Itens	**Auditoria**
2.1 Definição da administração de Sistema Operacional	Conforme
2.2 Cadastramento no Servidor LDAP (a definir)	Conforme

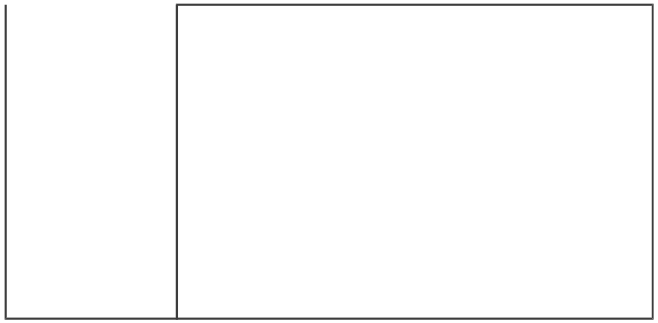
Check-List de Auditoria

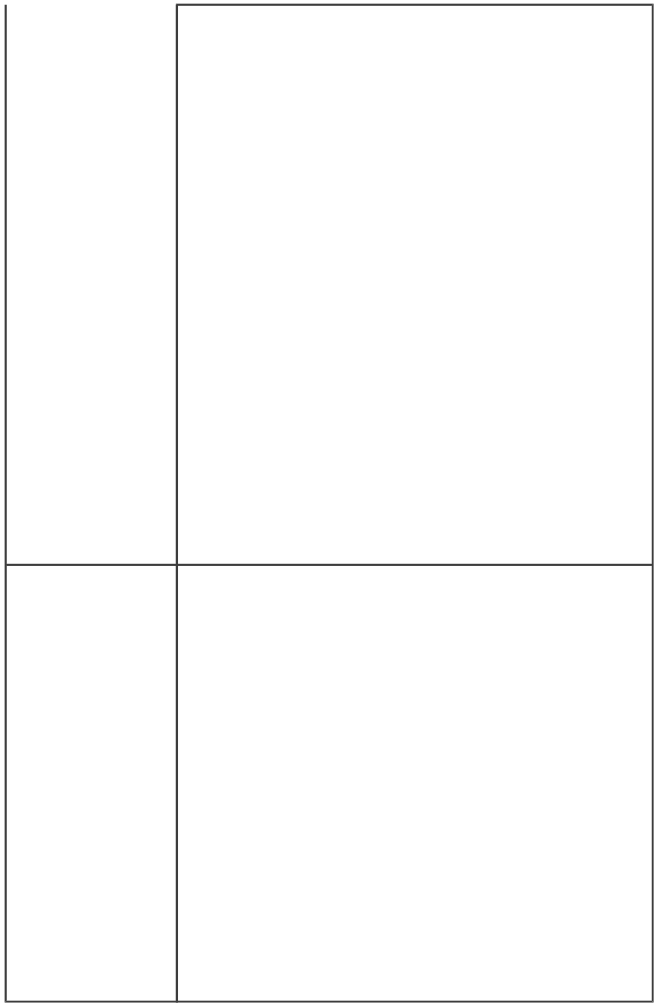
CABEÇALHO

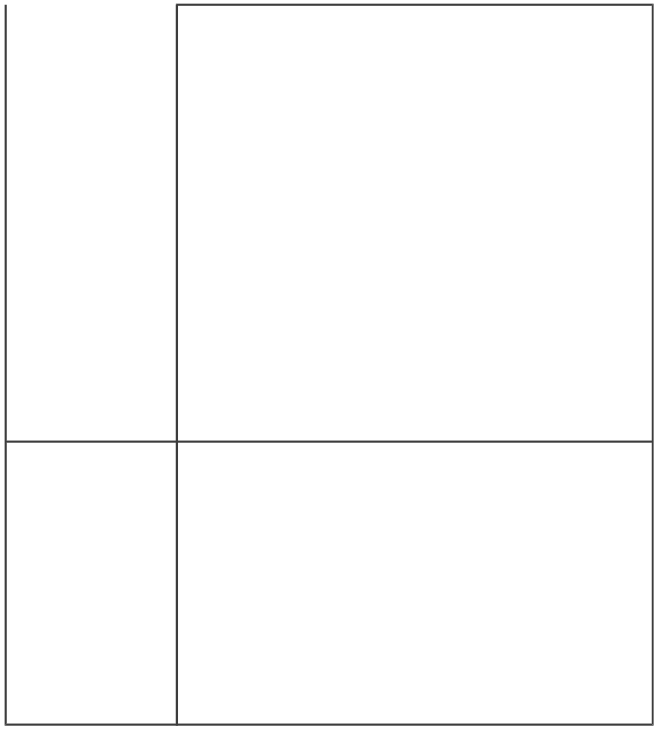
2.3 Utilizar sudo sempre que necessário	Conforme
2.4 Agente de virtualização, caso o servidor seja virtual (Xentools, Vmtools).	Conforme
2.5 Instalação da última versão do dataprotector ou netbackup no servidor.	Não Conforme
2.6 Verificar a configuração dos DNS	Conforme
2.7 Garantir a última versão do Sistema Operacional caso aplicação não necessite de um específico.	Conforme
2.8 Alterar parâmetro "per_source" do xinetd para permitir várias instancias do Data Protector vim /etc/xinetd.d/omni per_source = UNLIMITED	Não se Aplica
2.9 Incluir nas rotinas de backup. Diário 30 dias /etc - Backup inclemental diariamente de segunda a sábado. Semanal 30 dias /etc - Backup full realizado toda semana no domingo Diário 30 dias /var - Backup inclemental diariamente de segunda a sábado. Semanal 30 dias /var - Backup full realizado toda semana no domingo	Não se Aplica
2.10 Eliminar usuários genéricos	Conforme
2.11 Efetuar antecipadamente a configuração de horário de verão no sistema operacional	Não se Aplica
Itens	**Auditoria**
3.1 CPU	Conforme
3.2 Memória Física	Conforme
3.3 Memória Swap	Conforme
3.4 Consumo de Disco	Conforme
3.5 Taxa de utilização de Disco	Conforme
3.6 Utilização de Rede	Conforme
3.7 Sistema UP/DOWN	Conforme
Itens	**Auditoria**
4.1 Formulário de Instalação da Aplicação (caso aplicação instalada e configurada pela Adminitração Linux CTI)	Conforme
4.2 Formulário de Instalação do Sistema Operacional	Conforme
4.3 Detalhamento Tecnico	Conforme
Itens	**Auditoria**
5.1 Cadastro do servidor no monitoramento (NAGIOS).	Conforme
5.2 Cadastro do servidor no CMDB.	Conforme

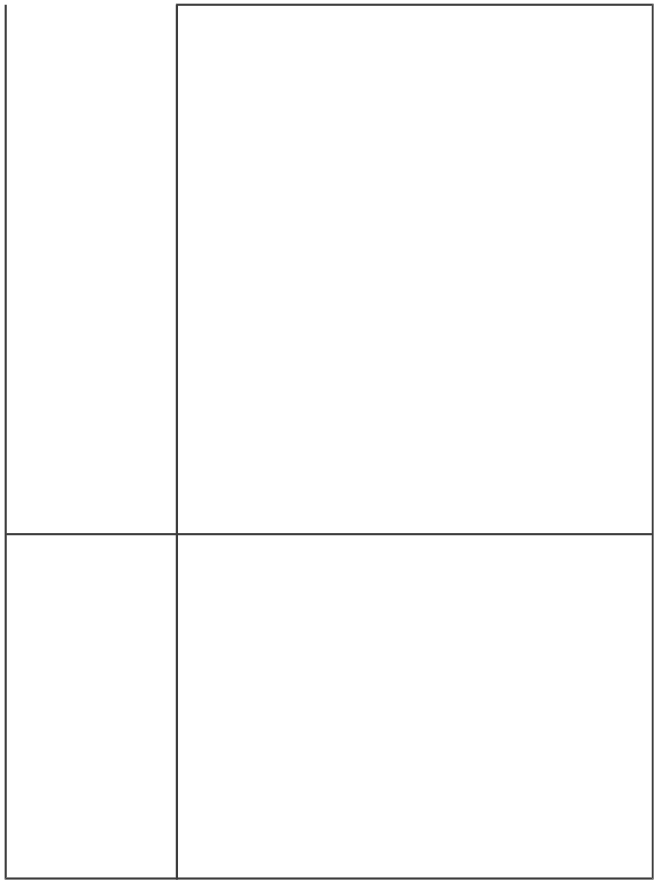
Critico	Observação

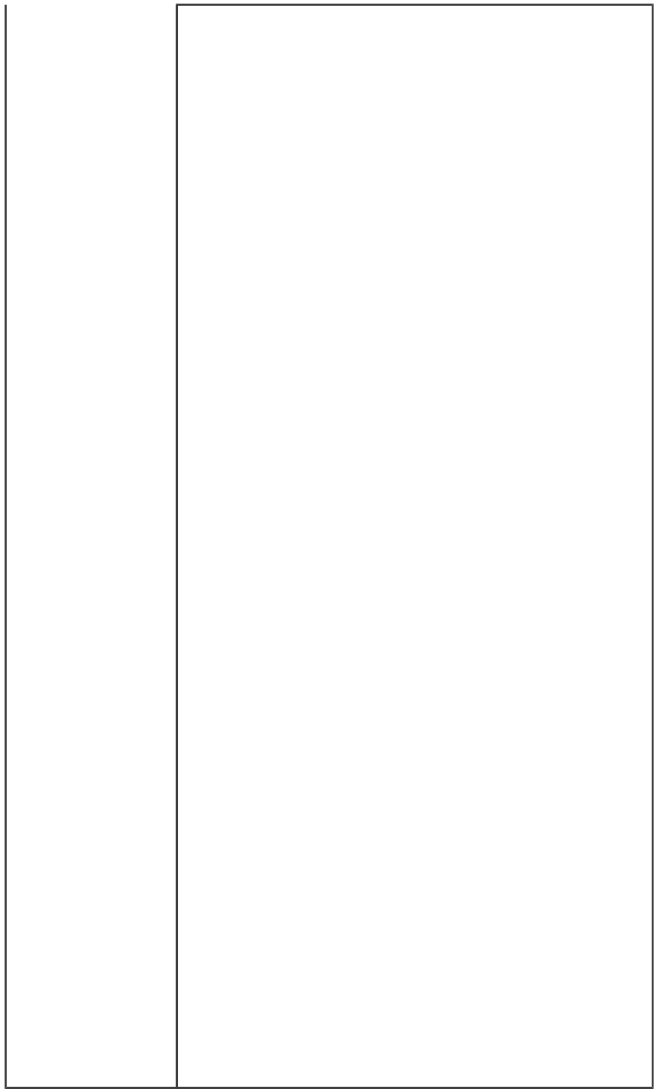


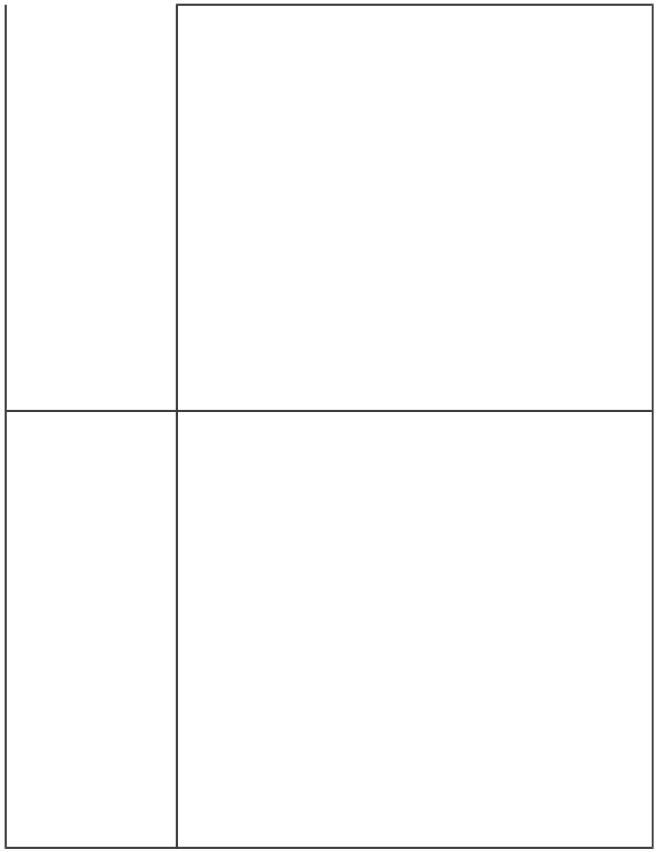


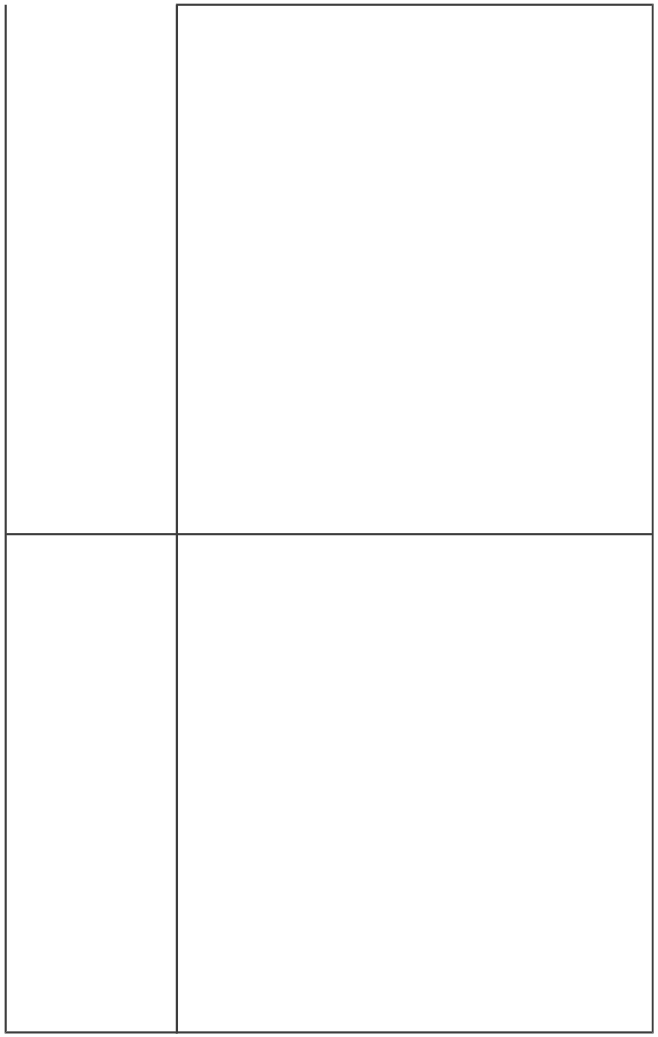


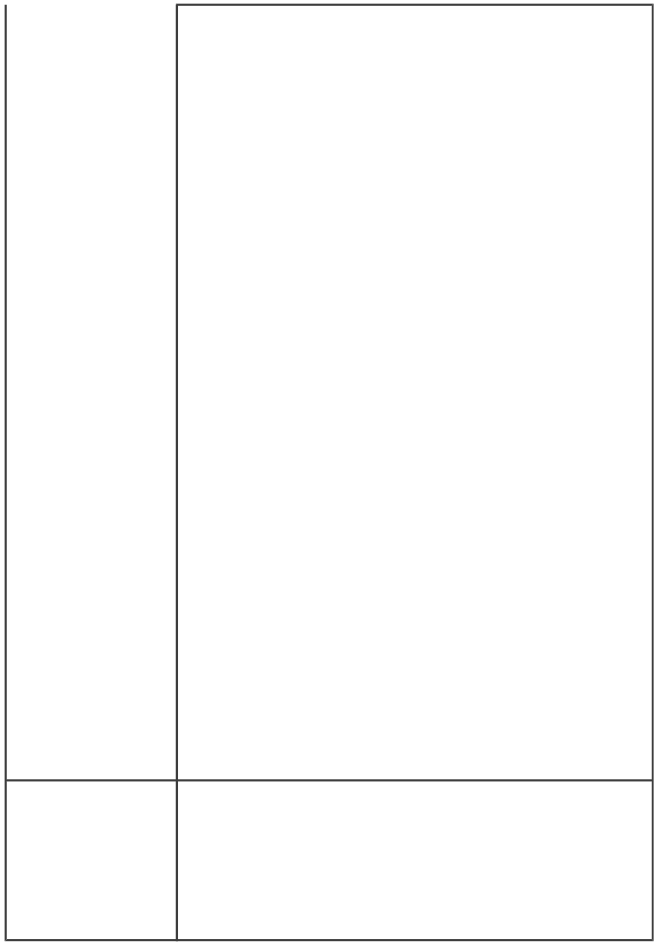












Critico	Observação

Impeditivo	

Critico	Observação

Critico	Observação

Critico	Observação

Categorias	Cód.
SEGURANÇA	**1.1**
SEGURANÇA	**1.2**
SEGURANÇA	**1.3**
SEGURANÇA	**1.4**
SEGURANÇA	**1.5**
SEGURANÇA	**1.6**
SEGURANÇA	**1.7**
SEGURANÇA	**1.8**

SEGURANÇA	**1.9**
SEGURANÇA	**1.10**
SEGURANÇA	**1.11**
SEGURANÇA	**1.12**
SEGURANÇA	**1.13**
SEGURANÇA	**1.14**
SEGURANÇA	**1.15**

SEGURANÇA	**1.16**
SEGURANÇA	**1.17**
SEGURANÇA	**1.18**
SEGURANÇA	**1.19**
SEGURANÇA	**1.20**
SEGURANÇA	**1.21**
SEGURANÇA	**1.22**
SEGURANÇA	**1.23**
SEGURANÇA	**1.24**
SEGURANÇA	**1.25**
SEGURANÇA	**1.26**
SEGURANÇA	**1.27**
SEGURANÇA	**1.28**
SEGURANÇA	**1.29**
SEGURANÇA	**1.30**
SEGURANÇA	**1.31**
SEGURANÇA	**1.32**
SEGURANÇA	**1.33**
SEGURANÇA	**1.34**
SEGURANÇA	**1.35**
SEGURANÇA	**1.36**
SEGURANÇA	**1.37**
SEGURANÇA	**1.38**
SEGURANÇA	**1.39**
SEGURANÇA	**1.40**
SEGURANÇA	**1.41**
SEGURANÇA	**1.42**
SEGURANÇA	**1.43**
SEGURANÇA	**1.44**
SEGURANÇA	**1.45**
SEGURANÇA	**1.46**
SEGURANÇA	**1.47**
SEGURANÇA	**1.48**
SEGURANÇA	**1.49**
SEGURANÇA	**1.50**
Categorias	**Cód.**
CONTINUIDADE DE SERVIÇO	**2.1**

CONTINUIDADE DE SERVIÇO	**2.2**
CONTINUIDADE DE SERVIÇO	**2.3**
CONTINUIDADE DE SERVIÇO	**2.4**
CONTINUIDADE DE SERVIÇO	**2.5**
CONTINUIDADE DE SERVIÇO	**2.6**

CONTINUIDADE DE SERVIÇO	**2.7**
CONTINUIDADE DE SERVIÇO	**2.8**
CONTINUIDADE DE SERVIÇO	**2.9**
CONTINUIDADE DE SERVIÇO	**2.10**
CONTINUIDADE DE SERVIÇO	**2.11**
Categorias	**Cód.**
DESEMPENHO NAGIOS	**3.1**
DESEMPENHO NAGIOS	**3.2**
DESEMPENHO NAGIOS	**3.3**
DESEMPENHO NAGIOS	**3.4**
DESEMPENHO NAGIOS	**3.5**
DESEMPENHO NAGIOS	**3.6**
DESEMPENHO NAGIOS	**3.7**
Categorias	**Cód.**
DOCUMENTAÇÃO DO PROJETO	**4.1**
DOCUMENTAÇÃO DO PROJETO	**4.2**
DOCUMENTAÇÃO DO PROJETO	**4.3**
Categorias	**Cód.**
CADASTRO	**5.1**
CADASTRO	**5.2**

Itens	Conforme
Antes da instalação, deve-se ter em mente qual serviço será executado pelo sistema operacional para que a instalação	1
É recomendando a utilização de partições com filesystem tipo LVM e que as partições de alocação de dados (exemplo: /var e /home), partição de boot (/boot) e outras padrões do sistema operacional sejam criadas separados (/), desta	1
O timezone deve ser configurado adequadamente pois esta configuração é essencial para a tratativa de incidentes de	1
O SELinux implementa vários níveis de segurança adicionais ao kernel do sistema operacional e deve ser habilitado. O	0
É recomendado que se implemente senha no carregador de boot do sistema operacional para que se tenha um nível de	1
Velocidade com que são lançados exploits para exploração de vulnerabilidades recém-descobertas nos aplicativos e sistema operacional	1
	1
O sistema operacional deve estar programado para sempre entrar em execução com o nível de runlevel adequado (sem	1

########## Check List de Seguranca #################	1
net.ipv4.tcp_syncookies = 1	1
imap, imaps, ipop2, ipop3, krb5-telnet, klogin, kshell, ktalk, ntalk, pop3s, rexec, rlogin, rsh, rsync, servers, services,	1
Todos os serviços que não possuem nível adequado de segurança e que não implementam criptografia na comunicação	1
Para desabilitar o CTRL+ALT+DEL, editar o arquivo /etc/inittab e comentar a seguinte linha:	1
usuário (root).	1
Exemplo de ferramentas de compilação: gcc, gcc3, gcc3-c++, gcc3-g77, gcc3-java, gcc3-objc, gcc-c++, gcc-chill, gcc-	1

Para instalar e executar o Laus, utilizar os seguintes comandos:	1
Para configurar o umask, inserir a seguinte linha nos arquivos /etc/profile e /etc/csh.login:	0
mais uma camada para se elevar o nível de segurança do sistema. Somente usuários que pertencerem ao grupo "wheel" e possuírem a senha do root conseguirão ter acesso root através do comando "su"	0
indivíduos que utilizarem este equipamento sem autorizacao, ou em operacoes que excedam o nivel de	1
As seguintes configurações devem ser realizadas:	1
1) Editar o arquivo /etc/mail/sendmail.mc alterando a seguinte linha: DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl	0
	1
yum install psacct	1
Deverá ser inserida a seguinte linha no arquivo /etc/syslog.conf:	0
authpriv.* /var/log/secure	1
Os logs do sistema operacional gerados pelo syslog, ou logs com informações confidenciais de aplicações instaladas	1
############ CHECK LIST DE SEGURANCA ############	1
last: mostra a listagem dos últimos usuários que logaram no sistema, incluindo a hora do login, hora do logout	1
mínimo), lcredit (número mínimo de caracteres minúsculos), ucredit (número mínimo de caracteres maiúsculos), dcredit (número mínimo de dígitos) e ocredit (número mínimo de caracteres especiais) na seguinte linha (considerando que o	1
linha (considerando que "n" =15):	0
	0
	1
Não permitir que usuários com senha em branco acessem o equipamento através do SSH.	1
- : root : ALL EXCEPT 10.11.148.53 rsyslogprd 10.32.14.13 usrv07 tty1 172.23.4.1 172.23.16.1 127.0.0.1 LOCAL	1
+ : ALL : cron crond	1
Foram descobertas várias falhas de segurança na implementação da versão 1 do protocolo SSH. A versão 2 implementa criptografia e mecanismos de segurança mais robustos	1
indesejáveis no sistema.	1
Este recurso faz com que seja necessário manter um nível mais restritivo de permissões no diretório home do usuário criado no servidor que está recebendo a conexão SSH. Esta configuração eleva o nível de segurança do protocolo	1
atividades ilícitas forem registradas, os logs poderão ser utilizados perante a Lei.	1
A opção AllowUsers, especifica e controla quais usuários podem acessar o servidor via ssh. Vários usuários podem ser	0
haja necessidade de utilização de transferência de arquivos através de SFTP deve-se desabilitar o subsystem para	0
Não permitir que usuários com senha em branco acessem o equipamento através do SSH.	1
rastreabilidade de eventos poderá se tornar impossível, pois, os logs apontarão apenas o acesso do root.	1
chmod 600 /etc/securetty	1
	1
	0
operacional (rc.local/wwtask - fraum0).	0
	0
# generate a daily summary of process accounting at 23:53	1
53 23 * * * root /usr/lib64/sa/sa2 -A	

Itens	Conforme
2.1 Definição da administração de Sistema Operacional	1

2.2 Cadastramento no Servidor LDAP (a definir)	1
2.3 Utilizar sudo sempre que necessário	1
2.4 Agente de virtualização, caso o servidor seja virtual (Xentools, Vmtools).	1
2.5 Instalação da última versão do dataprotector ou netbackup no servidor.	0
2.6 Verificar a configuração dos DNS	1

2.7 Garantir a última versão do Sistema Operacional caso aplicação não necessite de um específico.	1
vim /etc/xinetd.d/omni	0
Diario 30 dias /etc - Backup incremental diariamente de segunda a sabado. **Semanal 30 dias /etc - Backup full realizado toda semana no domingo**	0
2.10 Eliminar usuários genéricos	1
2.11 Efetuar antecipadamente a configuração de horário de verão no sistema operacional	0
Itens	**Conforme**
3.1 CPU	1
3.2 Memória Física	1
3.3 Memória Swap	1
3.4 Consumo de Disco	1
3.5 Taxa de utilização de Disco	1
3.6 Utilização de Rede	1
3.7 Sistema UP/DOWN	1
Itens	**Conforme**
4.1 Formulário de Instalação da Aplicação (caso aplicação instalada e configurada pela Adminitração Linux CTI)	1
4.2 Formulário de Instalação do Sistema Operacional	1
4.3 Detalhamento Tecnico	1
Itens	**Conforme**
5.1 Cadastro do servidor no monitoramento (NAGIOS).	1
5.2 Cadastro do servidor no CMDB.	1

Não Conforme	Não se Aplica	Críticos
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0

0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0

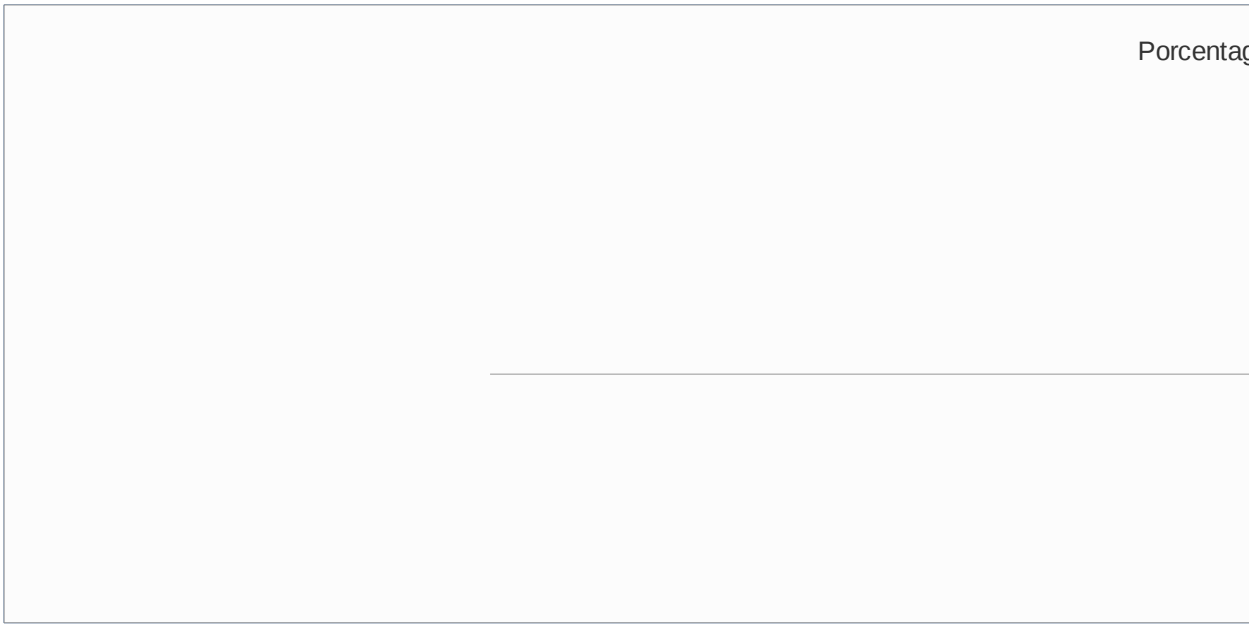
0	0	0
0	1	0
0	1	0
0	0	0
0	0	0
0	1	0
0	0	0
0	0	0
0	1	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	1	0
0	1	0
0	1	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	1	0
0	1	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
Não Conforme	**Não se Aplica**	**Críticos**
0	0	0

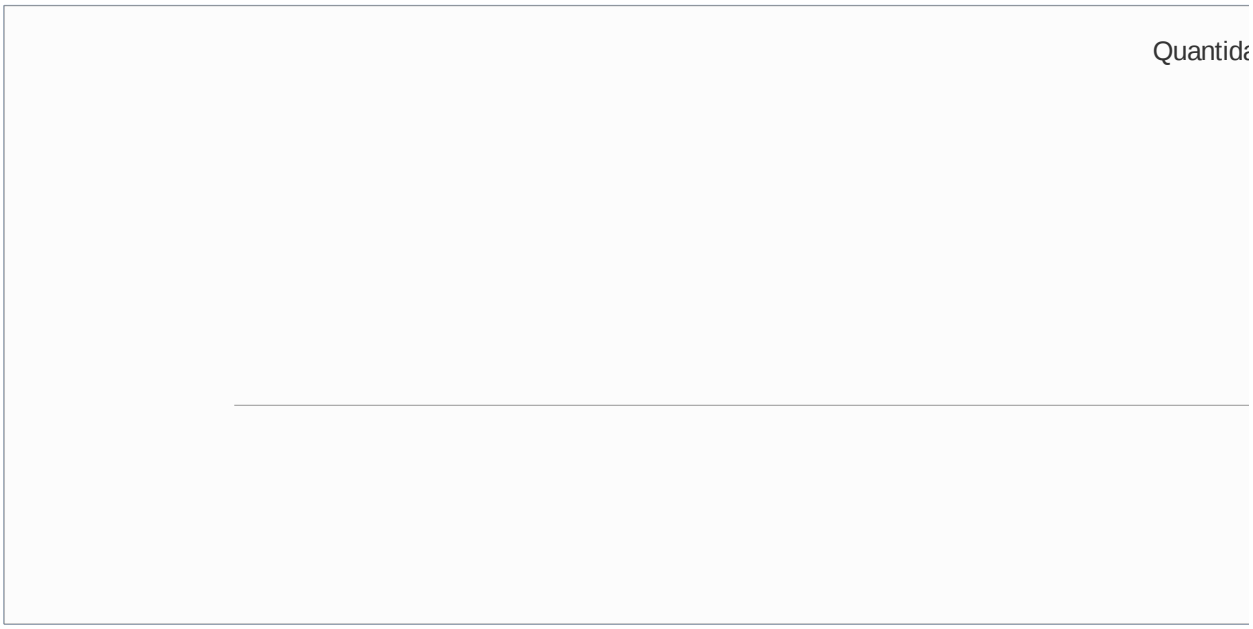
0	0	0
0	0	0
0	0	0
1	0	0
0	0	0

0	0	0
0	1	0
0	1	0
0	0	0
0	1	0
Não Conforme	**Não se Aplica**	**Críticos**
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
Não Conforme	**Não se Aplica**	**Críticos**
0	0	0
0	0	0
0	0	0
Não Conforme	**Não se Aplica**	**Críticos**
0	0	0
0	0	0

CONSOLIDAD

	Conformes	% Conformes	Não Conf.
SEGURANÇA	37	80,43	0
CONTINUIDADE DE SERVIÇO	7	63,64	1
DESEMPENHO	7	100,00	0
DOCUMENTAÇÃO DO PROJETO	3	100,00	0
CADASTRO	2	100,00	0
TOTAL	**56**	**81,16**	**1**





O POR GRUPO DE ITENS

% Não Conformes	Não Aplica	% Não se Aplica	Total X Itens	Críticos
0,00	9	19,57	46	0
9,09	3	27,27	11	0
0,00	0	0,00	7	0
0,00	0	0,00	3	0
0,00	0	0,00	2	0
1,45	**12**	**17,39**	**69**	**0**

gem C/NC/NA e Críticos

ade C/NC/NA e Críticos

% Criticos x Não Conformidade
0,00
0,00
0,00
0,00
0,00
0,00