**Proteção da Console**

**1. Proteção da BIOS**

O BIOS é um software básico, necessário para a inicialização da placa-mãe, responsável por checar os dispositivos instalados, e carregar o sistema operacional, o que pode ser feito a partir do HD, CD-ROM/DVD-ROM, floppy disk, pen-drive, ou qualquer outra mídia disponível. O BIOS inclui também o Setup, o software que permite configurar as diversas opções oferecidas pela placa-mãe. O processador é programado para procurar e executar o BIOS sempre que o computador for ligado, processando-o da mesma forma que outro software qualquer.

Para armazenar as configurações feitas no Setup utilizamos o CMOS (Complementary Metal-Oxide Semicondutor). Como as configurações do Setup representam um pequeno volume de informações, ele é bem pequeno em capacidade. Assim como a memória RAM principal, ele é volátil, de forma que as configurações são perdidas quando a alimentação elétrica é cortada. Por isso, toda placa-mãe inclui uma bateria, que mantém as configurações quando o micro é desligado.

Desta forma é importante proteger este software que é iniciado toda vez que o computador é ligado, pois ele é a porta de entrada para todos os outros softwares contidos nas mídias instaladas (como sistema operacional, controlador de disco com suporte a gerenciamento de RAID, entre outros).

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

**2. Proteção nos gerenciadores de boot**

Gerenciadores de Boot são softwares capazes de iniciar o processo de carregamento do(s) sistema(s) operacional(is) em um computador. São de extrema importância em casos de computadores com mais de um sistema operacional instalado, pois os gerenciadores tem a função de permitir ao usuário a escolha do sistema a ser carregado.

Os principais gerenciadores de Boot existentes são: LILO (Linux Loader) e GRUB (GRand Unifield Bootloader) para sistemas GNU/Linux, NTLDR (New Tecnology Loader) para a família MS Windows e BTX Loader para família BSD.

Aqui devemos proteger a edição do nosso gerenciador de Boot para que uma pessoa com acesso a console não possa alterar a senha de root ou de qualquer outro usuário, passando como parâmetro para o Kernel o argumento “init=/bin/sh rw”.

Para assegurarmos que essa técnica não seja usada contra nossos sistemas, você deverá definir uma senha para o gerenciador de Boot.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

**3. Segurança nos terminais**

Quando falamos em segurança, a primeira coisa que vem à mente é um possível ataque remoto. Então, os nossos servidores que não estão conectados à Internet não estão correndo nenhum perigo, certo? Errado, aliás, dois fatores estão errados. Não está conectado diretamente à Internet, não quer dizer que está totalmente seguro, pois, se um cracker conseguir passar pelo nosso firewall, ele vai conseguir acesso às outras máquinas que estão conectadas à rede interna e não necessariamente conectada diretamente à Internet.

Outro fator é funcionários mal-intencionados, com acesso local (físico) aos servidores. Muitas vezes quem entende de tecnologia costuma subestimar as pessoas com cargos mais braçais. Ledo engano, pois esse pessoal tem computadores em suas casas e mesmo sem intenções maliciosas podem causar problemas ao ver um terminal em sua frente. Além disso, se por um descuido da equipe de TI, um funcionário mal-intencionado conseguir acesso ao Datacenter, se passando por não entender nada de informática, pode na verdade ser um espião industrial com conhecimentos superior aos seus!

**3.1 - Remoções dos Shell desnecessárias**

Vamos remover os Shell válidas de todos os usuários que não vão executar oficialmente login no sistema, por meio de um terminal local (tty) ou via SSH. Isso garante que se uma aplicação for executada por um usuário como www-data, que é usado para subir o serviço de WEB, e for comprometido, esse usuário não poderá efetuar login.

Observação: crie um usuário que utilizaremos para administrar o servidor (sem permissões privilegiadas) e atribua uma senha para esse usuário.

**3.2 - Acessos aos Terminais da Console**

Por questões de segurança não é interessante deixarmos o login habilitado em todos os terminais de texto. Por isso, vamos desabilitar alguns terminais, deixando somente dois disponíveis. Você poderá escolher quais terminais você deseja bloquear.

**3.3 - Reboot**

Caso seu sistema tenha teclado conectado, por default, qualquer um poderá reinicializar o sistema sem efetuar login. Por medidas de segurança é bom ter o controle dos acessos, inclusive de quem reinicia a máquina. Para desativar o uso do Ctrl+Alt+Del, como forma de reiniciar o sistema sem a necessidade de login, devemos editar o arquivo/etc/inittab.

**Observação:** Isso também evitará que um servidor Linux em um mesmo rack que outro servidor com sistema operacional Windows® possa ser reiniciado por engano, pois o CTRL+ALT+DEL no Windows® tem outro contexto, o de apresentar a tela de login e não de reiniciar o sistema operacional.

Enquanto alguns promovem o CTRL+ALT+DEL, outros não gostam de usá-lo tanto assim.

O Linux é um sistema muito estável, porém como qualquer outro software, poderá falhar em algum momento, onde nem CTRL+ALD+DEL poderá te ajudar. Neste momento você poderá usar um recurso de Kernel chamado “Magic SysRq key”. Com ele você poderá desligar o sistema sem comprometer o seu filesystem (coisa que um desligamento forçado, pressionando o botão de liga/desliga faz).

Suas principais funções são:

• ALT+SysRq+r 🡪 Tira o teclado e o mouse do controle do Servidor X. Isso pode ser útil quando o seu Servidor X estiver travado, você pode mudar para um terminal e matar o X ou verificar o log.

• ALT+SysRq+k 🡪 Mata todos os processos que estão rodando no momento. Não faça isso no console onde está rodando o X, pois ele poderá travar.

• ALT+SysRq+b 🡪Um reboot sem desmontar o sistema (Esse é o perigo).

• ALT+SysRq+o 🡪 Desliga via APM.

• ALT+SysRq+s 🡪 Executa um sync em todos os sistemas de arquivos montados.

• ALT+SysRq+u 🡪 Remonta todo o sistema de arquivos montado como read-only.

• ALT+SysRq+m 🡪 Joga todas as informações da memória para o terminal.

• ALT+SysRq+e 🡪Envia um SIGTERM para todos os processos exceto o init.

• ALT+SysRq+i 🡪 Envia um SIGKILL para todos os processos exceto o init.

• ALT+SysRq+l 🡪 Envia um SIGKILL para todos os processos inclusive o init (O sistema não funcionará mais após esta sequência ser pressionada).

Aqui entre uma questão do que é mais importante, gerenciamento, facilidades ou segurança? Pois com este recurso habilitado não adianta nada termos desabilitado o CTRL+ALT+DEL se este recurso pode ser usado para reiniciar a máquina com o pressionamento das teclas ALT+SysRq+b.

**3.4 - Bloqueios do terminal por inatividade**

Quando abandonamos a console de um sistema em que estamos trabalhando é importante que ele tenha algum recurso que desconecte automaticamente após um período inativo ou ainda uma forma de bloqueamos a console na necessidade de nos ausentamos. Para isso podemos usar a variável global TMOUT e o programa vlock respectivamente.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 032: Análise crítica dos direitos de acesso de usuário.

9.2.5 – Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários a intervalos regulares. (ABNT, NBR 27002, 2013, p.28).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33)

. Controle 039: Controle de acesso ao código fonte de programas.

9.4.5 - Convém que o acesso ao código fonte de programas seja restrito. (ABNT, NBR 27002, 2013, p.34).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

**4 - Restringindo acesso a console de usuários sem senhas (senhas nulas)**

Conformidade com a Norma NBR ISO/IEC 27001:2013

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31).

. Controle 037: Sistemas de gerenciamento de senha.

9.4.3 - Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade. (ABNT, NBR 27002, 2013, p.33).

**5 - Bloqueando o login do root na console**

Por questões de segurança não é bom que o usuário root tenha acesso direto ao sistema (nem local, nem remoto). O ideal é “logarmos” como um usuário comum e, quando for necessário fazer alguma tarefa administrativa, usamos o comando su para nos tornarmos root ou usamos comando sudo para executar algum comando como root.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 039: Controle de acesso ao código fonte de programas.

9.4.5 - Convém que o acesso ao código fonte de programas seja restrito. (ABNT, NBR 27002, 2013, p.34).

. Controle 063: Registro de eventos.

12.4.1 - Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.54).

. Controle 065: Registro de eventos (log) de administrador e operador.

12.4.3 - Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (log) protegidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.56).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

**6 - Limitando os usuários que podem logar na console**

Aqui iremos ver como restringir o número de usuários que podem fazer login no console.

**Conformidade com a Norma NBR ISO/IEC 27001:2013**

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 032: Análise crítica dos direitos de acesso de usuário.

9.2.5 – Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários a intervalos regulares. (ABNT, NBR 27002, 2013, p.28).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 039: Controle de acesso ao código fonte de programas.

9.4.5 - Convém que o acesso ao código fonte de programas seja restrito. (ABNT, NBR 27002, 2013, p.34).

. Controle 063: Registro de eventos.

12.4.1 - Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.54).

. Controle 065: Registro de eventos (log) de administrador e operador.

12.4.3 - Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (log) protegidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.56).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

**7 - Limitando login consecutivos nos terminais**

Para evitarmos que um único usuário seja usado por diversas pessoas, podemos restringir o número de login consecutivos que este usuário pode fazer.

Conformidade com a Norma NBR ISO/IEC 27001:2013

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 034: Uso da informação de autenticação secreta.

9.3.1 - Convêm que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta. (ABNT, NBR 27002, 2013, p.30).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 039: Controle de acesso ao código fonte de programas.

9.4.5 - Convém que o acesso ao código fonte de programas seja restrito. (ABNT, NBR 27002, 2013, p.34).

. Controle 063: Registro de eventos.

12.4.1 - Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.54).

. Controle 065: Registro de eventos (log) de administrador e operador.

12.4.3 - Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (log) protegidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.56).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

**8 - Usuários com permissão de elevar seus privilégios para root (administrador)**

Para evitar que usuários que não tenha permissão de uso dos comandos su/sudo possam elevar seus privilégios para outros usuários do sistema, vamos criar um grupo e adicionar somente usuários que poderão usar o comando su e outro para usuários que possam usar o sudo.

Além disso, os usuários que utilize o comando su, devem ter seus acessos registrados, para fins de auditoria e análise forense em caso de abusos.

Conformidade com a Norma NBR ISO/IEC 27001:2013

. Controle 030: Gerenciamento de direitos de acesso privilegiados.

9.2.3 - Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados. (ABNT, NBR 27002, 2013, p.27).

. Controle 032: Análise crítica dos direitos de acesso de usuário.

9.2.5 – Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários a intervalos regulares. (ABNT, NBR 27002, 2013, p.28).

. Controle 034: Uso da informação de autenticação secreta.

9.3.1 - Convêm que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta. (ABNT, NBR 27002, 2013, p.30).

. Controle 035: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso. (ABNT, NBR 27002, 2013, p.31).

. Controle 036: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações, sejam controlados por um procedimento seguro de entrada no sistema (log-on). (ABNT, NBR 27002, 2013, p.31).

. Controle 038: Uso de programas utilitários privilegiados.

9.4.4 - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, NBR 27002, 2013, p.33).

. Controle 039: Controle de acesso ao código fonte de programas.

9.4.5 - Convém que o acesso ao código fonte de programas seja restrito. (ABNT, NBR 27002, 2013, p.34).

. Controle 063: Registro de eventos.

12.4.1 - Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.54).

. Controle 065: Registro de eventos (log) de administrador e operador.

12.4.3 - Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (log) protegidos e analisados criticamente, a intervalos regulares. (ABNT, NBR 27002, 2013, p.56).

. Controle 070: Controles de auditoria de sistemas de informação.

12.7.1 - Convém que as atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio. (ABNT, NBR 27002, 2013, p.60).

. Controle 078: Análise e especificação dos requisitos de segurança da informação.

14.1.1 - Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. (ABNT, NBR 27002, 2013, p.67).

. Controle 099: Avaliação e decisão dos eventos de segurança da informação.

16.1.4 - Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação. (ABNT, NBR 27002, 2013, p.86).