Segurança Lógica

Diretrizes – CID

Nossa política de segurança é baseada na norma NBR ISO IEC 27001. Nosso SGSI - Sistema de Gestão de Segurança da Informação - foi projetado para assegurar com a finalidade adequada e proteger os ativos de informação e prover a confiança aos usuários dos serviços da escola.

Seguindo as três

Políticas De Acesso

Políticas de Segurança para acesso físico

Trata-se de políticas para evitar o acesso de desconhecidos à escola e suas salas restritas de forma a garantir a segurança de informações privilegiadas de terceiros a infraestrutura.

1. Caso for visitante, o mesmo deverá deixar seus dados de identificação hora de entrada, com o segurança que fará inserção dos dados no sistema de controle de visistantes;

2. Caso for funcionário terá um smartcard (cartão de identificação magnética) com foto que servirá como cartão de ponto automático;

3. Caso for aluno terá um smartcard com foto que ao passar pela catraca eletrônica implicará em presença automática no sistema de controle de frequência;

4. Caso for funcionário e necessite entrar na escola fora do expediente, deve ser autorizados pela segurança e ter em posse seu cartão de identificação, caso seja aluno ou visitante se torna impossível o acesso à escola;

5. O acesso a sala dos servidores da escola será permitido aos membros das áreas de Segurança, responsáveis da área de TI e visitantes desde que acompanhado por um responsável em todo o período em que permanecerem na sala;

6. Serão utilizados sistemas de detecção de intrusos, via câmeras de segurança, para monitorar os acessos às dependências físicas.

Políticas de Segurança para controle de acesso lógico

Trata-se de políticas para evitar o acesso de desconhecidos mau intencionado a informações privilegiadas ou uso indevido de colaboradores ou alunos.

1. O compartilhamento de senha de acesso é absolutamente proibido. Caso ocorra de um titular divulgar sua senha a outros, será ele responsável pela infração cometida, estando passível de advertência;

2. Caso o usuário desconfie que sua senha não seja mais segura, poderá solicitar ao departamento de TI a alteração desta;

3. As senhas de funcionários têm validade de 60 dias, depois deste período é obrigatória à troca da senha;

4. Quando o funcionário errar o nome de usuário ou senha será exibido uma mensagem de erro. Toda via o funcionário erre três vezes seguidas seu acesso será bloqueado e somente o administrador da rede poderá liberar o uso novamente.

Políticas Para Uso De Senhas

A senha é de acesso é pessoal e intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo. Porém para maximizar a segurança em relação às senhas criamos políticas quanto a durabilidade e formação de senhas:

1. Senha com data para expiração a senha possui prazo de validade com 60 dias, obrigando o colaborador ou usuário a renovar sua senha, não atendendo aos alunos;

2. É vetada a repetição da senha. Através de regras uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos;

3. É obrigatório a composição o número mínimo de 8 (oito) caracteres alfanuméricos e caracteres especiais;

O sistema de autenticação é Case Sensitive, portanto será obrigatório a utilização de caracteres maiúsculos, minúsculos e números, bem como a utilização de caracteres especiais como: @ # $ % & \*.

Políticas De Uso Da Internet

São definidas regras para boa utilização da internet, sendo essa uma ferramenta importante não só para o estudo como para fins administrativos.

1. O acesso à internet será livre para pessoas que possui privilégios como o diretor da escola entre outros;

2. A internet deve ser utilizada para fins corporativos, o enriquecimento intelectual de seus colaboradores ou como ferramenta para busca de informações que venham contribuir para o desenvolvimento de seus trabalhos;

3. O uso para fins pessoais, mediante ao consentimento do responsável pelo setor, fica restrito à consulta de movimentação bancária e ao acesso ao e-mail pessoal, estando vedadas práticas abusivas tais como a circulação de correntes, material pornográfico entre outros;

4. A realização de downloads deve realizada somente em casos de extrema necessidade. Além disso, estará limitada a arquivos de no máximo 10 MB (Mega Byte), pois downloads de arquivos de tamanho superior podem congestionar o fluxo de tráfego e comprometer o tráfego da rede.

5. É terminantemente proibida a execução de jogos, músicas ou rádios online, visto que esta prática congestiona a banda de

internet, dificultando a execução de serviços que necessitam deste recurso.

Realização De Downloads

Uso, Execução E/Ou Acesso De Jogos, Rádios On-Line, Softwares De Comunicação Instantânea, Redes Sociais.

Políticas De Uso De E-Mail

Os Sites De Conteúdo Inapropriado.

Backup

Todos os dias as empresas produzem uma serie de dados o que é perfeitamente normal e compreensível. O backup é essencial para manter e assegurar as informações importantes para a empresa. Estamos sempre passíveis de situações onde possa ocorrer a perda inesperada de informações como em uma tragédia de campo natural ou até mesmo um incêndio criminoso. Pensando em uma política para backup criamos uma tabela:

Políticas de Backup

Domingo Completo Horário

Segunda-feira Diferencial 00:00

Terça-feira Diferencial 00:00

Quarta-feira Diferencial 00:00

Quinta-feira Diferencial 00:00

Sexta-feira Diferencial 00:00

Sábado Diferencial 00:00

Tabela 19: Políticas para Backup

Optamos pelo backup completo aos domingos para que seja feito o backup na íntegra de todos os arquivos e diretórios existentes no

servidor. Para os dias de semana e aos sábados, optamos pelo backup diferencial, visando a facilidade no caso necessite de restauração