Segurança Física de acesso aos dados

Leograf

A Segurança Física tem como objetivos específicos:

- ✓ **Proteger edificações e equipamentos;**
- ✓ **Prevenir perda, dano ou comprometimento dos ativos;**
- ✓ **Manter a continuidade das atividades dos negócios;**
- ✓ **Reduzir as ameaças que coloquem em risco o bom funcionamento dos sistemas.**

Sistema de Proteção contra Descargas Atmosféricas (SPDA) e Aterramento

As edificações onde encontram-se instalações de processamento, estão protegidas por um sistema contra descargas atmosféricas (para-raios) e tem sistema de aterramento eficiente, observando-se o seguinte:

- ✓ Todo sistema de proteção recebe manutenção preventiva e inspeção anualmente.
- ✓ A função do para-raios é proteger edificações e pessoas, não abrangendo necessariamente,equipamentos eletroeletrônicos.
- ✓ A inspeção e medição do sistema de aterramento deve ser anual, conforme a norma vigente.

Fornecimento de energia

Os equipamentos devem estar protegidos contra falhas de alimentação elétrica, observando-se as especificações do fabricante do equipamento quanto ao fornecimento de energia:

- ✓ Uso de no-break em equipamentos que suportam atividades críticas e para todos os componentes do Backbone Leograf.
- ✓ Uso de grupo-gerador em instalações estratégicas e áreas do núcleo e de distribuição da rede Leograf.
- ✓ Iluminação de emergência e interruptores elétricos de emergência que permitam o desligamento de equipamentos em caso de necessidade.

Segurança Ambiental

A Segurança Ambiental tem por objetivo adotar medidas que evitem risco às instalações e equipamentos por ocorrência dos seguintes fatores:

- ✓ Incêndio;
- ✓ Fumaça;
- ✓ Poeira;
- ✓ Vibração;
- ✓ Umidade;
- ✓ Sensores de controle destes fatores integrados a um sistema que permita a monitoração remota, assim como o disparo de alarmes.
- ✓ Restrições à comida, bebida e fumo dentro das Instalações de Processamento.

Segurança do acesso às instalações

A Segurança das instalações com relação ao acesso físico tem como objetivos específicos:

- ✓ Prevenir e controlar o acesso não autorizado a informações e instalações físicas da empresa;
- ✓ Prevenir perda, dano ou comprometimento dos ativos;
- ✓ Evitar a exposição ou roubo de informação.

Controle de Acesso

As instalações de processamento ou outras áreas de segurança são equipadas com controles de entrada apropriados, de forma que somente pessoal autorizado tenha acesso liberado. O controle de acesso depende dos requisitos de segurança próprios da área considerada e pode se dar através de:

- ✓ Controle de entrada (métodos de acesso físico);
- ✓ Crachás de identificação e acesso com procedimentos pelos quais o acesso é concedido pode ser modificado ou excluído,
- ✓ Liberações de acesso para colaboradores, através de identificação de perfil e área de trabalho.
- ✓ Restrições de acesso baseadas no status do funcionário e horas de operação
- ✓ Bloqueio de acessos físico para colaboradores, quando demissão ou afastamento temporário
- ✓ Pontos de contato para acesso;

Segurança do acesso à instalação:

Sistemas de segurança adotados:

- ✓ O Controle de Acesso utiliza como validação um sistema de cartão com PIN (Personal Identification Number), seja para funcionários, colaboradores ou visitantes. Eventualmente, em locais mais críticos, pode-se optar também pela validação biométrica (impressão digital, por exemplo);O fornecimento dos cartões de acesso deve ser através do gerente responsável pela segurança;
- ✓ O extravio ou roubo de cartões de acesso deve ser informado imediatamente à segurança;
- ✓ Os cartões de acesso devem ser mantidos pelos seus respectivos proprietários todo o tempo,e nunca devem ser emprestados para qualquer pessoa ou deixados desprotegidos;
- ✓ Todas as portas externas são bloqueadas fora do horário comercial normal;
- ✓ Qualquer pessoa dentro de uma área de segurança deverá dispor de identificação de acordo com a função por ela exercida;
- ✓ Os funcionários não podem permitir a estranhos o acesso aos re-

cursos de rede.

- ✓ Os visitantes ou funcionários sem permissão deverão ganhar autorização e identificação especial para ter acesso e permanecer nos locais de segurança, devendo estar explícito qual o propósito de adentrar ao local, quais as atividades que serão desenvolvidas e a quais recursos estas pessoas terão acesso;

- ✓ Serviços de terceiros ou Visitantes em Instalações de Processamento devem ser agendados previamente, fornecido o nome das pessoas que executarão o serviço, assim como o detalhamento da atividade a ser desenvolvida;

- ✓ Tanto para o caso de terceiros quanto para visitantes, uma pessoa da Unidade/Depto deve sempre acompanhar o trabalho, de forma que um estranho nunca fique sozinho nas instalações;

- ✓ Circuito Fechado de TV nas áreas consideradas estratégicas, havendo registro da imagem local por meio de câmeras de vídeo, sendo armazenadas em mídia, com backups diários e guarda por 30 dias, de forma a poderem ser resgatadas em caso de alguma ocorrência ou auditoria;

Segurança para o Sistema de Telefonia

Semelhante às Instalações de Processamento, o sistema de telefonia requer cuidados e procedimentos que visem a segurança:

- ✓ O acesso físico ao hardware do sistema de telefonia e aos terminais de configuração de sistema é restritivo aos administradores do sistema de telefonia e ao pessoal da companhia provedora do serviço;

- ✓ A instalação de modems deve ser coordenada pelo grupo responsável, a fim de fornecer a segurança necessária e infraestrutura de rede para manter a segurança.

Segurança dos equipamentos

A segurança dos equipamentos está diretamente relacionada aos procedimentos de instalação e proteção, atentando-se ao seguinte:

- ✓ A instalação de equipamentos deve seguir o procedimento recomendado pelo fabricante e/ou normas específicas existentes, na falta destes, deverá ser consultado o setor responsável pela instalação elétrica da Unidade;

- ✓ Equipamentos de servidores, firewall e roteadores instalados em área restrita;
- ✓ A instalação, manutenção e atualização de equipamentos no Backbone da Leograf é de responsabilidade de pessoal devidamente capacitado de TI.

- ✓ Controle e Inventário periódico de ativos referente hardware e software, através do Open Audit.

Segurança de equipamentos instalados fora da Leograf

Os equipamentos instalados fora dos limites da Leograf e interligados a ela, devem ter autorização expressa do responsável pela administração do backbone da Leograf para poder manter a conexão.

Manutenção de equipamentos

Em relação à manutenção dos equipamentos, deve-se observar o seguinte:

- ✓ A manutenção de equipamentos deve ser de acordo com intervalos e especificações do fabricante.
- ✓ Apenas profissionais autorizados podem fazer manutenção nos equipamentos, ou seja, o próprio fabricante, empresas autorizadas por ele e equipe de manutenção de redes da Leograf. Mantidos registros de todas as falhas feitas ou ocorridas em toda manutenção preventiva e corretiva.

- ✓ Equipamentos enviados para manutenção de terceiros e que possuem meios de armazenamento (disco rígido, fitas, etc.) devem ter seus itens checados para assegurar que toda informação sensível, sigilosa e software licenciado foi removido ou sobreposto antes da alienação do equipamento. Um hardware sobressalente está disponível caso a criticidade do equipamento seja alta;

- ✓ Dispositivos de armazenamento danificados, assim como equipamentos, devem sofrer uma avaliação de riscos para verificar se eles devem ser destruídos, reparados ou descartados.

Segurança lógica de acesso aos dados

Segurança lógica e Segurança da informação

Tão importante quanto a segurança física é a segurança da informação.

- ✓ Utilização de cofre para a guarda das mídias contendo as cópias de Segurança (back-up). Este cofre é resistente a incêndio, umidade, interferências eletromagnéticas, poeira, fumaça e vandalismo; O acesso às mídias de back-up deve ser restrito ao pessoal autorizado;

- ✓ O acesso ao aplicativo de back-up deve ser restrito ao pessoal autorizado;
- ✓ Equipamentos, informações ou software não devem ser retirados da organização sem autorização; Uso de criptografia para guarda de arquivos, sejam internos da Leograf ou Dados de Clientes;
- ✓ Toda informação, quer em mídia eletro-eletrônica ou papel, deve ficar sempre guardada em locais apropriados e de acesso restrito, especialmente fora dos horários de trabalho normal;

- ✓ Semanalmente back-up completo dos sistemas e, diariamente, à noite a cópia incremental, ou seja, o que foi modificado; Back-ups em mídia, com colocação em cofre, e backups automáticos on-line com Data Center Konics.

- ✓ A restauração deve ocorrer da última cópia completa até as cópias com as alterações incrementais (Layered Over), até o momento do evento.

- ✓ Identificação de perfil de usuários para acesso e recebimento de informações, através de:

- Processo formal de alçada;

- Processo de mapeamento de acessos de acordo com a função exercida pelo colaborador, com controle de autoridade formal e responsabilidade.

- ✓ Identificação do tipo de informações: Confidencial (informações

apenas para uso dos usuários identificados e dados de clientes), Restritas (informações apenas para áreas definidas) e públicas para todos os usuários da empresa.

Contas de Acesso

Sobre o acesso aos sistemas, conforme Normas de Acesso para Usuários, segue:

- ✓ Cada usuário possui uma conta individual. Não deve haver contas coorporativas ou contas compartilhadas por mais de um usuário; Orientações sobre definição e utilização de senhas, em Normas para Usuários; A empresa mantém um sistema unificado de contas dos usuários dos Sistemas integrantes da Leograf, sejam Coorporativos, sejam de Internet;

- ✓ Novo funcionário da empresa receberá uma conta única para acessar os sistemas, incluindo o acesso remoto, quando necessários à execução de suas funções;

- ✓ A solicitação de abertura de contas em quaisquer dos sistemas se dará pelo preenchimento de um documento e devidamente aprovado pelo Gestor do Departamento.

- ✓ A autorização e o nível da conta será concedida pelo proprietário e/ou administrador do sistema, ou se for o caso, pelo administrador de rede;

- ✓ Contas de usuários que venham a se desligar da Leograf, tais como funcionários e prestadores de serviço, serão canceladas imediatamente da data do desligamento , a partir de documento do RH e Gestor da área de atuação do colaborador desligado;

- ✓ Funcionários em férias, terão suas senhas bloqueadas para acesso físico e lógico na Leograf;
- ✓ O Setor de Pessoal da empresa ao qual esteja vinculado um funcionário demitido ou afastado, deve comunicar o responsável de segurança da Unidade para as providências.

- ✓ **Segurança para Redes**

A segurança para a rede sob o aspecto da segurança lógica deve considerar filtros e protocolos habilitados nos ativos.

- ✓ Regras de proteção nos seus roteadores e/ou firewall para proteger as redes de forma restritiva (método de exceção);

- ✓ Para os roteadores do Backbone Leograf, os filtros e regras obrigatórios e estudados para cada caso, além de serem aprovadas pela Área de TI;

- ✓ O acesso lógico aos equipamentos de rede (roteadores, switches, servidores, ou outros) deve sempre ser protegido por senhas não padrão (default ou inicial), quer para suporte, configuração ou gerenciamento e, preferencialmente, a partir de um número restrito de equipamentos;

- ✓ As senhas de acesso lógico aos equipamentos (devem ser) trocadas periodicamente, a cada 90 dias ou quando o administrador ou funcionário que as detenha venha a se desligar da Empresa ou da função;

- ✓ Os responsáveis mantêm um registro (Log) para as alterações de configuração dos equipamentos de rede;

- ✓ Uso de aplicativos de gerenciamento para os equipamentos de rede e servidores, que notifiquem o administrador em casos de anomalias;

- ✓ Para o caso do gerenciamento SNMP, não deve estar habilitado se não estiver em uso, do contrário, garantir acesso estritamente aos administradores responsáveis;

- ✓ Utilização de antivírus que monitorem as mensagens de correio eletrônico;
- ✓ As informações de configuração dos equipamentos devem estar armazenadas em servidores administrativos, nunca em servidores públicos ou de produção;

- ✓ Os equipamentos de rede tem back-up de sua configuração em servidores administrativos, semanalmente ou quando alterações de configuração;
- ✓ Os equipamentos devem ter habilitados somente os protocolos necessários;

Segurança de acesso remoto

- ✓ A permissão para o acesso remoto é fornecida pela área de TI da Leograf com autorização da diretoria executiva da empresa;
- ✓ A autenticação deve ser necessariamente através de senhas, combinada com recurso de identificação de chamada;
- ✓ Não deverá ser permitido múltiplo acesso simultâneo para o mesmo usuário, a menos em casos analisados e autorizados pelos gerentes responsáveis.

Segurança para servidores

Plano de contingência para a recuperação de desastres.

- ✓ Os servidores configurados para suportar apenas os serviços necessários;
- ✓ Os servidores fisicamente seguros, permitindo acesso restrito;
- ✓ Os administradores dos servidores devem estar atentos a atualizações e correções de vulnerabilidades dos sistemas operacionais e software;

Segurança para notebooks e Smartphone

- ✓ Os notebooks devem utilizar criptografia para evitar acesso não autorizado caso sejam roubados;
- ✓ Os usuários jamais devem deixar sessões abertas, efetuando o logout quando ele não estiver em uso;
- ✓ Orientação aos usuários que dados importantes sejam protegidos por senhas e criptografia;
- ✓ É instruído que o usuário que utilize senhas diferentes para os sistemas e equipamentos, defendendo-se em caso de roubo de alguma senha;
- ✓ Estes equipamentos portáteis devem estar presos fisicamente através de cabos, correntes ou outro dispositivo de segurança, ou ainda, trancados em gavetas ou armários quando fora de uso;

Leograf

LEOGRAF GRÁFICA E EDITORA LTDA.

RUA BENEDITO GUEDES DE OLIVEIRA, 587

SÃO PAULO - SP

FONE: (11) 3933-3888 - FAX: 3932-1986