Faculdade Senac Goiás

Ismael Derick Brito Cardoso

João Vitor Vieira Felicio

Rone Augusto Oliveira Jacob

Governança de Tecnologia da Informação

Plano de Segurança da Informação

Inicialmente, deve se possuir a percepção de que a segurança da informação deve respeitar os seguintes critérios: autenticidade, não repúdio, privacidade e auditoria. Também deve possuir a percepção de que a segurança da informação deve abranger três aspectos básicos:

- **A confidencialidade**, onde somente pessoas devidamente autorizadas pela empresa devem possuir o acesso à informação.
- **A integridade**, onde somente poderão ser realizadas alterações, supressões e adições autorizadas pela empresa, devem ser realizadas nas informações.
- **A disponibilidade**, pois a informação deve estar disponível, apenas para as pessoas autorizadas sempre que necessário ou demandado.

Política de Segurança

A Política de Segurança da Informação deve ser uma declaração formal da organização, acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores, com o propósito de estabelecer diretrizes a serem seguidas, no ato à adoção de procedimentos e mecanismos relacionados à segurança da informação.

Pessoal

Independentemente domei-o ou da forma existente, a informação está presente no trabalho de todos os profissionais, e desta forma, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações, destacando, por exemplo, diretores coordenadores, servidores e terceirizados, devem assumir atitude proativa no que diz respeito à proteção das informações, todos os servidores devem compreender as ameaças externas que podem afetar a segurança das informações da organização, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, entre outros, bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.

Proibições

Todo tipo de acesso à informação referente a empresa, que não for explicitamente autorizado é proibido. Informações confidenciais, não devem ser transportadas em qualquer meio (pen-drive, papel, drive) sem as devidas autorizações e proteções. As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não protegido. As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não protegido.

Somente softwares homologados pelos especialistas da empresa, poderão ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia da empresa. As políticas para uso de internet e correios eletrônicos devem ser rigorosamente seguidas, e arquivos de origem desconhecida nunca devem ser abertos ou executados. Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.

Obrigações

A área de Gestão de Segurança da Informação deve realizar, de forma sistemática, a avaliação dos riscos de incidentes relacionados à segurança da informação. A análise dos riscos deve atuar como ferramenta de orientação ao Comitê Gestor da Segurança da Informação, principalmente, no que diz respeito à identificação dos principais riscos aos quais as informações da empresa estarão expostas e priorização de ações voltadas à mitigação dos riscos apontados, tais como a implantação de novos controles, criação de novas regras e procedimentos ou a reformulação de sistemas. O escopo da análise ou da avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc. Todos os profissionais e servidores da empresa deverão ter ciência de que, o uso das informações e dos sistemas de informação, podem ser monitorados, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos ou legais.

Infraestrutura

Banco de dados

O Banco de Dados SQL do Azure é um serviço de banco de dados de nuvem dimensionável e inteligente que oferece a mais ampla compatibilidade com o mecanismo do SQL Server e até 212% de retorno sobre o investimento.

Segurança de rede

O Banco de Dados SQL do Microsoft Azure fornece um serviço de banco de dados relacional para aplicativos na nuvem e empresariais. Para ajudar a proteger os dados do cliente, os firewalls impedem o acesso de rede ao servidor de banco de dados até que ele seja concedido explicitamente com base no endereço IP ou na origem do tráfego de rede virtual do Azure.

Regras de firewall de IP.

As regras de firewall de IP permitem acesso a bancos de dados com base no endereço IP de origem de cada solicitação. Para saber mais, confira Overview of Azure SQL Database and SQL Data Warehouse firewall rules (Visão geral de regras de firewall do Banco de Dados SQL do Azure e do SQL Data Warehouse).

Regras de firewall de rede virtual

Os pontos de extremidade de serviço de rede virtual estendem a conectividade de rede virtual por meio do backbone do Azure e permitem que o Banco de Dados SQL do Azure identifique a sub-rede de rede virtual da qual o tráfego é originado. Para permitir que o tráfego alcance o Banco de Dados SQL do Azure, use as marcas de serviço do SQL para permitir o tráfego de saída por meio de Grupos de Segurança de Rede.

Power BI

Power BI por ser simples e rápida, com capacidade de criar análises rápidas de uma planilha do Excel ou um banco de dados local. Mas o Power BI também é robusto e empresarial, pronto para ampla modelagem e análise em tempo real, bem como desenvolvimento personalizado. Ele pode ser sua ferramenta de visualização e o pessoal de relatório e também servem como o mecanismo de decisão e análise para projetos de grupo, divisões ou empresas inteiras.

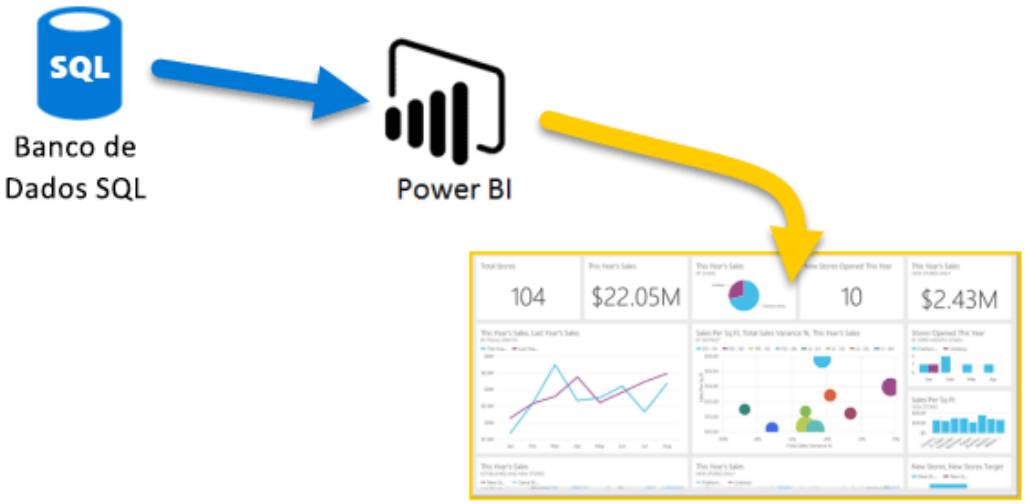
Azure e Power BI

Com os serviços do **Azure** e o **Power BI**, podemos transformar seus esforços de processamento de dados em análises e relatórios que fornecem informações em tempo real sobre a sua empresa. Se o processamento de dados é baseado em nuvem ou local, simples ou complexo, de única fonte ou altamente escalonado, armazenado ou em tempo real, o Azure e o Power BI têm a conectividade interna e a integração para dar vida aos seus esforços de business intelligence.

Banco de Dados SQL do Azure e Power BI

Iniciaremos uma conexão simples com um Banco de Dados SQL do Azure e criar relatórios para monitorar o progresso de sua empresa. Com o Power BI Desktop, é possível criar relatórios que identificam tendências e indicadores chave de desempenho que promovem a sua empresa.

.



Transferência de dados.

O AWS DataSync é um serviço de transferência de dados que facilita a automação da movimentação de dados entre o armazenamento local e o Amazon S3 ou o Amazon Elastic File System (Amazon EFS). O DataSync processa automaticamente muitas das tarefas relacionadas a transferências de dados que podem retardar as migrações ou sobrecarregar as operações de TI, incluindo executar suas próprias instâncias, processar criptografia, gerenciar scripts, otimizar redes e validar integridade de dados. Você pode usar o DataSync para transferir dados online com velocidade até 10 vezes maior que as ferramentas de código aberto. O DataSync usa um agente de software local para conexão a armazenamento ou sistemas de arquivos existentes usando o protocolo Network File System (NFS) para que você não precise criar scripts nem modificar aplicativos para trabalhar com APIs da AWS. Você pode usar o DataSync para copiar dados usando o AWS Direct Connect ou links de Internet para a AWS. O serviço oferece migrações de dados uma única vez, fluxos de trabalho de processamento de dados recorrentes e replicação automatizada para proteção e recuperação de dados. É fácil começar a usar o DataSync: implante o agente DataSync no local, conecte-o a um sistema de arquivos ou uma matriz de armazenamento, selecione o Amazon EFS ou o S3 como armazenamento na AWS e comece a mover os dados. Você paga apenas pelos dados copiados.

Armazenamento

O AWS Backup é um serviço de backup gerenciado que facilita a centralização e automatização do backup de dados entre os serviços da AWS na nuvem e no local usando o AWS Storage Gateway. Usando o AWS Backup, você pode configurar políticas de backup e monitorar atividades de backup de forma centralizada para recursos da AWS como volumes do Amazon EBS, bancos de dados do Amazon RDS, tabelas do Amazon DynamoDB, sistemas de arquivos do Amazon EFS e volumes do AWS Storage Gateway. O AWS Backup automatiza e consolida tarefas de backup que antes eram realizadas separadamente em cada serviço, eliminando a necessidade de criar scripts personalizados e processos manuais. Com apenas alguns cliques no console do AWS Backup, você pode criar políticas de backup que automatizam o gerenciamento da programação e da retenção dos backups. O AWS Backup oferece uma solução de backup gerenciada e baseada em políticas para simplificar o gerenciamento de backups e permitir o cumprimento de requisitos de conformidade de backup normativos e corporativos.