A empresa é a Idle Corp. ela trabalha na produção de jogos idles, ela trabalha com a engine Unity e possui cinco computadores para a produção desses jogos.

Segurança da informação:

A ISO 27000 se concentra na proteção dos ativos de informação da organização, que podem incluir:

* Dados: Código-fonte dos jogos, scripts, designs, arquivos de áudio e vídeo, dados de jogadores e muito mais.
* Softwares: A engine Unity, ferramentas de desenvolvimento, softwares de controle de versão e outros softwares utilizados na criação dos jogos.
* Hardwares: Computadores, servidores, dispositivos de armazenamento e outros hardwares que suportam o desenvolvimento e a operação dos jogos.

A ISO 27000 fornece um conjunto de controles de segurança para proteger esses ativos contra diversos tipos de ameaças, como:

* Malware: Vírus, Worms, Trojans e outros softwares maliciosos que podem corromper ou roubar dados.
* Ataques cibernéticos: Hackers que podem invadir sistemas de computador para roubar dados, causar danos ou interromper operações.
* Erros humanos: Acessos não autorizados, perda acidental de dados ou falhas na configuração de sistemas.

De acordo com a ISO 27000

* Integridade**:** Garante que os dados e informações sejam precisos e confiáveis, livres de alterações não autorizadas. No contexto da Idle Corp., isso significa que o código-fonte dos jogos, os designs e os dados dos jogadores não podem ser corrompidos ou manipulados.
* Confidencialidade**:** Assegura que os dados e informações sejam acessíveis apenas por pessoas autorizadas. Na Idle Corp., isso significa que apenas os desenvolvedores autorizados têm acesso ao código-fonte dos jogos, e que os dados dos jogadores são protegidos contra acesso não autorizado.
* Disponibilidade**:** Garante que os dados e informações estejam acessíveis aos usuários autorizados quando necessário. Para a Idle Corp., isso significa que os jogos e seus serviços online estão sempre disponíveis para os jogadores, sem interrupções ou indisponibilidades.

Para tratar da integridade, da confiabilidade e disponibilidade, é necessário entender o que é ameaça, vulnerabilidade e probabilidade.

* Uma **vulnerabilidade** é uma falha ou fraqueza em um sistema ou processo que pode ser explorada por uma **ameaça**. Na Idle Corp., as vulnerabilidades podem incluir falhas de software, erros de configuração, senhas fracas ou práticas inadequadas de segurança por parte dos funcionários.
* Uma **ameaça** é um evento ou ação que pode explorar uma vulnerabilidade e causar danos à segurança da informação. Para a Idle Corp, as ameaças podem incluir ataques cibernéticos, malware, erros humanos, desastres naturais ou falhas de hardware.
* A **probabilidade** é a chance de uma **ameaça** se concretizar e causar danos à segurança da informação. Ao avaliar os riscos, a Idle Corp deve considerar a probabilidade de cada tipo de ameaça, como a frequência de ataques cibernéticos na indústria de jogos ou a chance de falhas de hardware nos computadores.

Para garantir que a empresa esteja segura certas responsabilidades tem de ser garantidas:

* Diretoria: Aprovar e revisar as políticas e procedimentos de segurança da informação;
* Gestor de Segurança da Informação: Implementar e gerenciar o programa de segurança da informação;
* Colaboradores: Cumprir as políticas e procedimentos de segurança da informação.

Com a aprovação da diretoria tem de garantir que essas normas sejam passadas a todos membros da empresa para ter a unificação da segurança de forma a não expor a empresa a ameaças internas e externas.

* Toda a equipe deve receber treinamento para não expor a empresa por erros humanos.
* A implementação e o cumprimento de novas regras estabelecidas devem ser monitorados para garantir a segurança, através de auditorias internas, análise de logs, entrevistas com os colaboradores, etc.
* Essa política também deve ser revisada pelo menos uma vez por ano, visto que a revisão deve considerar as mudanças no ambiente de negócio, novas ameaças a segurança e as melhores práticas do mercado.

A gestão da segurança da informação na ISO 27000 envolve a implementação de um SGSI, um processo cíclico que visa garantir a segurança da informação de forma contínua e proativa. As etapas principais do SGSI incluem:

* Estabelecimento de uma Política de Segurança da Informação: Define os princípios e diretrizes que norteiam a segurança da informação na organização.
* Identificação de ativos: Identificar quais são os ativos da empresa, isso pode incluir dados, softwares, hardwares, documentos da empresa, etc.
* Identificação e Avaliação de Riscos: Determina os riscos potenciais à segurança da informação e avalia seu impacto e probabilidade.
* Tratamento de Riscos: Implementa medidas de controle para mitigar os riscos identificados, como firewalls, criptografia, controle de acesso e treinamento de funcionários.
* Monitoramento e Revisão: Monitora continuamente a efetividade dos controles de segurança e revisa o SGSI periodicamente para garantir sua adequação às necessidades da organização.

Para garantir que essas medidas sejam cumpridas devem ser feitas auditorias internas sobre a segurança da informação na empresa:

* A auditoria interna da segurança da informação deve ser planejada com antecedência, o planejamento deve definir os objetivos da auditoria, o escopo da auditoria, a metodologia de auditoria e a equipe de auditoria.
* A equipe de auditoria deve realizar a avaliação dos controles de segurança da informação implementados pela Idle Corp., a avaliação deve verificar se os controles estão de acordo com a Política de Segurança da Informação e se estão sendo implementados de forma eficaz.
* Após a execução da auditoria, a equipe deve elaborar um relatório, o relatório deve documentar os resultados da auditoria, incluindo as constatações, as não-conformidades identificadas e as recomendações para melhoria.
* A Diretoria da Idle Corp. deve analisar o relatório de auditoria e definir um plano de ação corretiva, o plano de ação corretiva deve definir as ações que serão tomadas para corrigir as não-conformidades identificadas na auditoria.

Então a empresa terá que fazer algumas novas políticas para garantir a segurança das informações da Idle Corp.

* A Idle Corp. deve implementar controles de acesso para restringir o acesso aos ativos de informação apenas às pessoas autorizadas, os controles de acesso podem incluir senhas fortes, autenticação multifator, permissões de acesso granular e controle de dispositivos.
* Ela deve implementar medidas para proteger os dados da empresa contra perda, roubo, uso indevido, acesso não autorizado, modificação e destruição, as medidas de proteção de dados podem incluir criptografia, backups regulares e procedimentos de descarte seguro de dados.
* A empresa também tem de implementar medidas de segurança de rede para proteger seus sistemas e dados contra ataques cibernéticos, as medidas de segurança de rede podem incluir firewalls, sistemas de detecção de intrusão e software antivírus.
* A Idle Corp deve implementar medidas de segurança de software para proteger seus sistemas contra vulnerabilidades e malware, as medidas de segurança de software podem incluir a utilização de software licenciado e atualizado, o uso de técnicas de desenvolvimento seguro e a realização de testes de vulnerabilidade.
* A corporação também deve realizar treinamentos de conscientização e segurança da informação para todos os colaboradores da empresa, os treinamentos devem abordar tópicos como a importância da segurança da informação, as ameaças à segurança da informação, os controles de segurança implementados e as responsabilidades dos colaboradores.

A Idle Corp. também terá que observar os incidentes de segurança que ocorreram na segurança da empresa:

* A Idle Corp. deve estabelecer um processo para notificar os incidentes de segurança da informação, o processo deve definir quem deve ser notificado, quando deve ser feita a notificação e como deve ser feita a notificação.
* Ela também deve estabelecer um processo para investigar e responder a incidentes de segurança da informação, o processo deve definir as etapas para a contenção do incidente, a erradicação do incidente e a recuperação dos dados.
* Após a resolução de um incidente de segurança da informação, a XYZ Games deve documentar as lições aprendidas, as lições aprendidas devem ser utilizadas para melhorar o programa de segurança da informação da empresa.

Boas práticas:

Backups:

* Realize backups regulares**:** Crie backups frequentes de todos os dados críticos da empresa, incluindo código-fonte dos jogos, designs, dados de jogadores e outros arquivos importantes. Armazene os backups em locais seguros e offsite para garantir a recuperação em caso de falhas de hardware, ataques cibernéticos ou outras situações de perda de dados.
* Teste seus backups: Verifique periodicamente se os backups podem ser restaurados com sucesso para garantir que você possa recuperar seus dados em caso de necessidade.
* Conscientize seus funcionários: Treine seus funcionários sobre a importância dos backups e como realizar backups de seus dados de trabalho.

Sites Não Confiáveis:

* Implemente filtros de internet: Utilize firewalls e softwares de filtragem de conteúdo para bloquear o acesso a sites não confiáveis, maliciosos ou que podem conter phishing ou malware.
* Eduque seus funcionários: Oriente seus funcionários sobre os perigos de acessar sites não confiáveis e como identificar sites potencialmente perigosos.
* Crie políticas de uso de internet: Estabeleça políticas claras sobre o uso da internet na empresa, incluindo o tipo de conteúdo que pode ser acessado e as medidas a serem tomadas em caso de acesso a sites não autorizados.

Trabalho Remoto:

* Implemente uma VPN: Utilize uma rede privada virtual (VPN) para garantir que os funcionários em trabalho remoto se conectem à rede da empresa de forma segura e criptografada.
* Utilize ferramentas de autenticação multifator: Exija que os funcionários em trabalho remoto usem autenticação multifator para acessar os sistemas e dados da empresa, adicionando uma camada extra de segurança além das senhas.
* Limite o acesso a dados confidenciais: Restrinja o acesso a dados confidenciais da empresa apenas aos funcionários que realmente precisam deles para realizar seu trabalho.
* Treine seus funcionários em trabalho remoto: Forneça treinamento aos funcionários em trabalho remoto sobre as práticas de segurança da informação que devem ser seguidas quando trabalharem fora do escritório.

Segurança de Software:

* Utilize software licenciado e atualizado: Instale apenas softwares licenciados e atualizados em todos os computadores da empresa para garantir que você tenha as últimas correções de segurança e proteção contra vulnerabilidades conhecidas.
* Implemente um sistema de gerenciamento de patches**:** Utilize um sistema de gerenciamento de patches para automatizar a instalação de atualizações de segurança em todos os computadores da empresa.
* Realize testes de vulnerabilidade: Faça testes de vulnerabilidade regulares em seus sistemas para identificar e corrigir falhas de segurança antes que elas sejam exploradas por hackers.