1. OBJETIVO

Esta política de Segurança Cibernética é um conjunto formal de regras aplicáveis a todos os funcionários do Banco Caterpillar S.A. e a terceiros que têm acesso a recursos de tecnologia e de informação da empresa.

A política de Segurança Cibernética tem como objetivo:

- O compromisso com o tratamento adequado das informações do Banco Caterpillar S.A., clientes, funcionários e fornecedores está fundamentado nos seguintes princípios:
    - **Confidencialidade**: garantir que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;
    - **Integridade:** Garantir da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação. Garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência com os envolvidos. Faz parte da integridade a capacidade de agir preventivamente para prevenir, encontrar e reduzir qualquer tipo de vulnerabilidade relacionada com o ambiente cibernético.
    - **Disponibilidade**: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- Estabelecer para os usuários da empresa: funcionários, contratados, fornecedores e outros usuários autorizados suas obrigações para proteger os ativos de tecnologia e informação do Banco Caterpillar S.A.
- A política de segurança cibernética também descreve:
    - As responsabilidades e os privilégios do usuário;
    - O que é considerado uso aceitável;
    - Quais são as regras relativas ao acesso à Internet;
    - A descrição das limitações do usuário;
    - Penalidades por violação da política;
    - Procedimentos para responder a incidentes que ameaçam a segurança dos sistemas de computadores e da rede da empresa.

2. ÁREAS ENVOLVIDAS

Todas as áreas e funcionários da Instituição Banco Caterpillar S.A., terceiros, prestadores de serviço e fornecedores.

3. DEFINIÇÕES

Externamente acessível ao público. O sistema pode ser acessado via Internet por pessoas de fora da empresa, sem um ID de logon ou senha. É possível “pingar” o sistema pela

Internet. O sistema pode ou não estar por trás de um firewall. Um servidor da Web público é um exemplo desse tipo de sistema.

Não público, acessível externamente. Os usuários do sistema devem ter um ID de logon e senha válidos. O sistema deve ter pelo menos um nível de proteção de firewall entre sua rede e a Internet. O sistema pode ser acessado pela Internet ou pela Intranet privada. Um servidor FTP privado usado para trocar arquivos com parceiros de negócios é um exemplo desse tipo de sistema.

Internamente acessível apenas. Os usuários do sistema devem ter um ID de logon e senha válidos. O sistema deve ter pelo menos dois níveis de proteção de firewall entre sua rede e a Internet. O sistema não é visível para os usuários da Internet. Pode ter um endereço de Internet privado (não traduzido) e não responde a um "ping" da Internet. Um servidor da Web de intranet privada é um exemplo desse tipo de sistema.

Administrador de Segurança. O Gerente de Tecnologia local é designado como administrador responsável pela segurança cibernética da empresa.

4. ATIVOS A SEREM PROTEGIDOS

É dever de todos os usuários dos sistemas da empresa proteger os ativos de tecnologia e informação. Esta informação deve ser protegida contra o acesso não autorizado, roubo e destruição. Os ativos de tecnologia do Banco Caterpillar S.A. são compostos pelos seguintes componentes:

- Hardware de Computadores, CPU, discos, e-mail, servidores de aplicação, softwares para computadores, software de aplicativos, software de sistemas, etc.
- Software de sistemas incluindo: sistemas operacionais, sistemas de gerenciamento de banco de dados, e softwares de backup e restauração, protocolos de comunicação e assim por diante.
- Software aplicativo: usados pelos vários departamentos da empresa. Isso inclui aplicativos de softwares personalizados e comerciais e pacotes de software prontos para uso.
- Hardware de softwares de rede de comunicação incluindo: roteadores, tabelas de roteamento, hubs, modems, switches, firewalls, linhas privadas e ferramentas de gerenciamento de rede.

5. POSSÍVEIS AMEAÇAS À SEGURANÇA

5.1. Funcionários

Uma das maiores ameaças à segurança são os próprios funcionários e colaboradores. Eles podem causar danos aos seus sistemas e informações, seja de maneira intencional ou não. Com isso, camadas de segurança devem ser criadas com o objetivo de compensar essa exposição, seguem exemplos:

- Somente forneça acessos apropriados aos sistemas e arquivos. Restrinja o acesso sempre que possível.
- É permanentemente proibido o compartilhamento de contas para acesso aos sistemas. Os funcionários e colaboradores nunca devem compartilhar suas informações de “Login” com outras pessoas.
- Aplicar segurança aos ativos de tecnologia, para que apenas os funcionários com comprovada necessidade tenham acesso.
- Em casos de desligamento, todos os acessos devem ser removidos. Já em casos de mudança de cargos ou departamentos todos os acessos devem ser revisitados e limitados a nova necessidade.

5.2. Hackers amadores ou vândalos

Essas pessoas são o tipo mais comum de invasores na Internet. A probabilidade de ataque é extremamente alta e é provável que haja um grande número de ataques. Estes são geralmente crimes de oportunidade. Esses hackers amadores estão examinando a Internet e procurando por falhas de segurança bem conhecidas que não foram conectadas. Servidores da Web e correio eletrônico são seus alvos favoritos. Uma vez que eles encontrarem uma fraqueza, eles a explorarão para plantar vírus, cavalos de Tróia ou usar os recursos do seu sistema para seus próprios meios. Se eles não encontrarem uma fraqueza óbvia, provavelmente passarão para um alvo mais fácil.

5.3. Hackers criminosos e sabotadores

A probabilidade deste tipo de ataque é baixa, mas não é totalmente improvável, dada a quantidade de informações confidenciais contidas nos bancos de dados. A habilidade desses invasores é de média a alta, já que eles provavelmente serão treinados no uso das mais recentes ferramentas. Os ataques são bem planejados e se baseiam em quaisquer pontos fracos descobertos que permitam a entrada na rede.

6. MONITORAMENTO DO USO DE COMPUTADORES E SISTEMAS

A empresa tem o direito e a capacidade de monitorar informações eletrônicas criadas e/ou comunicadas por pessoas que usam sistemas ou a rede de computadores da empresa, incluindo mensagens de e-mail e uso da Internet. Não é política ou intenção da empresa monitorar continuamente todo o uso do computador por funcionários ou outros usuários dos sistemas de computadores e rede da empresa. No entanto, os usuários dos sistemas devem estar cientes de que a empresa pode monitorar o uso, incluindo, mas não limitado a padrões de uso da Internet (por exemplo, acesso a sites, tempo do acesso, horário de acesso) e arquivos eletrônicos dos funcionários e mensagens, na medida necessária para garantir que a Internet e outras comunicações eletrônicas estejam sendo usadas em conformidade com as leis brasileiras e com as políticas da empresa.

A internet é uma ferramenta de negócios da empresa. Ela deve ser usada para fins relacionadas ao negócio, como: comunicação via correio eletrônico com fornecedores, clientes e parceiros de negócios, obtenção de informações comerciais úteis e tópicos técnicos ou comerciais relevantes.

O uso dos recursos de tecnologia do Banco Caterpillar S.A. pode ser examinado, auditado ou verificado pela instituição, sempre respeitando a legislação vigente.

A empresa fornecerá acesso à internet para os funcionários e colaboradores conectados à rede interna corporativa e que tenham necessidade comercial para esse acesso.

7. CONTROLE DE ACESSO

Um componente fundamental da Política de Segurança Cibernética é o controle do acesso aos recursos de informações críticas que exigem proteção contra divulgação ou modificação não autorizada. O significado fundamental do controle de acesso é que as permissões são atribuídas a indivíduos ou sistemas que estão autorizados a acessar recursos específicos. Controles de acesso existem em várias camadas do sistema, incluindo a rede. O controle de acesso é implementado pelo ID de logon e senha. No nível do aplicativo e do banco de dados, outros métodos de controle de acesso podem ser implementados para restringir ainda mais o acesso. O aplicativo e os sistemas de banco de dados podem limitar o número de aplicativos e bancos de dados disponíveis para os usuários com base em seus requisitos de trabalho.

Administradores de sistema, administradores de rede e administradores de segurança terão acesso (tipo de acesso) a servidores, roteadores, hubs e firewalls, conforme necessário para cumprir as obrigações de seu trabalho.

8. INFORMAÇÕES SENSÍVEIS

A Definição de Informações sensíveis para o Banco Caterpillar S/A:

- se impossibilita a execução do negócio do Banco Caterpillar e/ou;
- gera/afeta/controla informações contábeis e/ou;
- armazena informações sensíveis (ex.: nome, CPF / CNPJ, informações financeiras) de clientes, funcionários ou fornecedores.

9. CONTROLES ESPECÍFICOS VOLTADOS PARA A RASTREABILIDADE DA INFORMAÇÃO, QUE BUSQUE GARANTIR A SEGURANÇA DE INFORMAÇÕES SENSÍVEIS

A Caterpillar dispões de diretivas corporativas seguidas pelo Banco Caterpillar S.A. referentes ao controle e garantia de segurança para informações sensíveis.

10. PROCEDIMENTOS DE GESTÃO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA

Esta seção fornece algumas diretrizes e procedimentos para lidar com incidentes de segurança. O termo "incidente de segurança" é definido como qualquer evento adverso ou irregular que ameace a segurança, a integridade ou a disponibilidade dos recursos de tecnologia e informações em qualquer parte da rede da empresa. Alguns exemplos de incidentes de segurança são:

- Acesso ilegal de um sistema de computador da empresa. Por exemplo, um hacker faz logon em um servidor de produção e copia arquivos contendo informações confidenciais.
- Danos ao sistema de computador ou rede da empresa causados por acesso ilegal. Liberar um vírus seria um exemplo.
- Ataque de negação de serviço contra um servidor web da empresa. Por exemplo, um hacker inicia repetidos envios de pacotes contra um servidor web com o objetivo de causar falhas no servidor ou rede da empresa.
- Uso malicioso de recursos da empresa para iniciar um ataque contra outro computador fora da rede da empresa. Por exemplo, o departamento de tecnologia percebe uma conexão com uma rede desconhecida e um processo estranho.

Os funcionários, que acreditam que seus sistemas ou computador tenham sido submetidos a um incidente de segurança, ou que tenham sido acessados ou usados de maneira inadequada, devem relatar a situação imediatamente ao departamento de Tecnologia da Informação. O funcionário não deve desligar o computador ou excluir arquivos suspeitos. Deixar o computador na condição em que estava quando o incidente de segurança foi descoberto ajudará a identificar a origem do problema e a determinar as etapas que devem ser tomadas para solucionar o problema.

O detalhamento do procedimento para gestão dos incidentes de segurança cibernética fica publicado internamente com acesso a todos os funcionários da instituição.

11. DIRETIVAS CORPORATIVAS DA SEGURANÇA CIBERNÉTICA

O Banco Caterpillar S.A. adota uma série de diretivas corporativas com o objetivo de mitigar as vulnerabilidades do ambiente cibernético, essas diretivas ficam disponibilizadas na intranet da Caterpillar.

A elaboração dos cenários de incidentes, considerados nos testes de continuidade de negócios ficam descritos em política interna específica.

Essas diretivas são classificadas por assunto, enumeradas e listam os pontos de contatos relevantes, como por exemplo a autoridade aprovadora e o ponto de contato operacional.

12. OS MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA NA INSTITUIÇÃO, INCLUINDO:

O Banco Caterpillar S.A. tem como objetivo capacitar todos os seus funcionários em relação a importância da Segurança Cibernética através de treinamentos renovados anualmente e através de eventos anuais que tem como objetivo reforçar o assunto e trazer novos meios para transmitir esse conteúdo para os funcionários.

13. PENALIDADES REFERENTES A VIOLAÇÃO DA SEGURANÇA

A empresa leva a questão da segurança a sério. As pessoas que usam os recursos de tecnologia e informação da empresa devem estar cientes de que podem passar por processos administrativos se violarem essa política.

14. REGULAMENTAÇÃO ASSOCIADA / REFERÊNCIAS

- Resolução n° 4.658 de 26/4/2018 do Banco Central do Brasil;
- Lei Nº 13.709, de 14 de agosto de 2018;