Sumário

1. Objetivo

Esta Política de Segurança da Informação contém os requisitos de segurança que visam garantir a segurança da informação em vigor, a fim de proteger as informações da SCC Check.

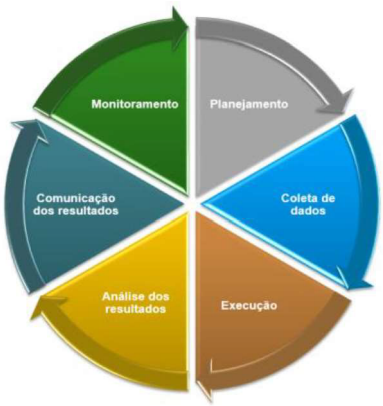
2. Escopo / Aplicabilidade

Aplicável a todos as frentes de negócio da SCC Check

3. Diretrizes Gerais

Esta Política define as diretrizes para a Segurança da Informação, visando definir os requisitos mínimos para garantir a integridade, confidencialidade e disponibilidade das informações compartilhados pela SCC Check com os seus clientes finais, fornecedores e colaboradores, identificados como USUÁRIOS

O Programa de Avaliação de Segurança é dividido em fases conforme abaixo:



Planejamento - Elaboração da agenda anual das avaliações;

Coleta de dados - Envio de questionário de avaliação criado de acordo com a necessidade;

Execução - Análise do ambiente com entrevistas que serão realizadas com os profissionais de tecnologia para a obtenção do entendimento da infraestrutura e da coleta e análise das evidências;

Análise dos resultados - Elaboração de plano de ação com prazo de implementação;

Comunicação dos resultados - Envio dos resultados para as partes envolvidas;

Monitoramento - Follow-up de implantação das ações necessárias.

Todas as avaliações são baseadas na Política de Segurança em linha com as melhores práticas do mercado.

4. Papéis & Responsabilidades

O usuário deverá implementar e manter os requisitos de Segurança da Informação apropriados ao seu tamanho e complexidade, a natureza e o alcance de suas atividades, e a sensibilidade da informação fornecida a ele pela SCC Check. Tais garantias deverão incluir os elementos estabelecidos nos Controles de Segurança especificados neste documento, e devem ser implementados para garantir a segurança e confidencialidade das informações fornecidas pela SCC Check. Esses controles visam proteger a integridade das informações contra quaisquer ameaças e/ou riscos, protegendo-as contra o acesso não autorizado e/ou o uso de tais informações de forma indevida.

A SCC Check terá o direito de auditar o usuário para assegurar a implementação dos controles de segurança previsto nesta política. A SCC Check será responsável por assegurar a plena cooperação de seus Provedores Técnicos, em conexão com as auditorias.

O usuário deverá responder imediatamente ou no prazo previamente estabelecido, de acordo com a tabela abaixo, todas as fases relacionadas na auditoria de Segurança da Informação.

O não atendimento dentro do período acordado poderá submeter a o usuário às sanções previstas em contrato.

Fase	Prazo para resposta
Coleta de Dados / Questionário	10 dias
Comunicação dos resultados / Aceite do plano de ação	10 dias
Monitoramento / Evidencias	De acordo com o plano de ação

5. Anexos

Guia Prático de Segurança da Informação

6. Referências

Todas as avaliações são baseadas na Política de Segurança em linha com as melhores práticas do mercado.

7. Glossário

Controles de Segurança

Antivírus
Aquisição de solução de antivírus comercial, para prover proteção para equipamentos (desktops, servidores, tablets e notebooks), licença de uso de software, implantação e garantia de atualização contínua.

Firewall
Os firewalls são dispositivos que controlam o tráfego externo via computador implementados na rede da empresa. Sua função consiste basicamente em bloquear o tráfego em áreas mais críticas dentro da rede interna e liberar acessos bem-vindos. Todos os sistemas devem ser protegidos contra o acesso não autorizado através da Internet, seja ele via e-commerce, acesso dos funcionários com base na Internet e via browsers, ou acesso via e-mail de funcionários. O firewall é o principal mecanismo de proteção de qualquer rede de computador.

Backups
Os backups devem fazer parte da rotina de operação dos seus sistemas baseando-se numa política determinada. A existência de uma política de backup em sua empresa tem como objetivo armazenar informações valiosas, levando em consideração a segurança e integridade dos dados, para que em caso de necessidade seja possível recuperá-los.

Política de backup: Define as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução;

Backup criptografado: Você deve armazenar dados sensíveis (informações do banco de dados, informações dos clientes; código fonte da aplicação e etc.) em formato criptografado,

Implementar criptografia nos Backups para não correr o risco do uso indevido de informações sigilosas.

Site HTTPS
O site do usuário deve implementar a utilização do protocolo de comunicação HTTPS, em regra, quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros. Através desse protocolo, os dados são transmitidos por meio de uma conexão criptografada, criando um canal seguro com alto nível de proteção para as suas informações sensíveis.

Ambiente Compartilhado
Empresas do mesmo segmento que prestam serviços de informações, desde que esses não sejam iguais ou que tenham alguma semelhança com aqueles oferecidos pela SCC Check e seus fornecedores, não podem ter o ambiente tecnológico compartilhados.

Armazenamento do "resultado" da consulta realizada
Absolutamente vedado o armazenamento do relatório gerado e fornecido ao usuário. Reter esses dados para quaisquer fins é considerado violação de contrato e pode ser caracterizado como fraude cabível de multa e destrato.

Log

Data, Hora e IP: Deverá manter armazenados os logs de operações como registro da data, da hora, da identificação, inclusive do “Internet Protocol”- IP do consulente quando executada a consulta, mantendo-os à disposição da SCC Check.

Troca de Senhas: Deverá manter armazenados os logs de quando é realizada a troca de senha do usuário. Não ter o registo no log torna impossível afirmar que os usuários realizam a troca de senha regularmente.

A tabela no banco de dados da aplicação que armazenam o logon e a senha dos usuários devem ser criptografadas;
Senhas e logons em texto limpo ficam vulneráveis para serem visualizadas, comprometendo assim a segurança das informações. O usuário deverá manter criptografado os dados confidenciais dos usuários, aumentando seu nível de segurança.
É de responsabilidade do usuário zelar integralmente pela segurança e confidencialidade das informações dos seus clientes.

Usuário e senha de conexão com a SCC Check devem ser protegidos com Controle de Acesso e Criptografia;
O usuário e senha de conexão via string com a SCC Check devem ser protegidos no ambiente tecnológico com um conjunto de procedimentos e medidas, a fim de resguardar ambas as partes contra tentativas de acesso não autorizados.
É de responsabilidade do usuário zelar integralmente pela segurança e confidencialidade do usuário e senha de conexão com a SCC Check.

Conscientização e aplicação de Política de Segurança da Informação para funcionários e clientes;
O usuário deverá conscientizar e/ou reforçar assuntos de Segurança da Informação que necessitam serem abordados por comunicação. As boas práticas de Segurança da Informação aplicadas em sua totalidade serão de grande valia para proteção de seus negócios, reduzindo riscos de ataques, comprometimento de informações confidenciais e fraudes.

Terceirização de Serviços;

Ao usar os Provedores de Tecnologia para acessar, transmitir, desenvolver sistemas ou processar dados, o usuário deve:

a. Adequar due diligence para manter a conformidade com as leis e regulamentos aplicáveis e obrigações contratuais;

b. Estabelecer contratos de Confidencialidade / NDA (Non Disclosure Agreement), obrigação de Confidencialidade dos Provedores de Tecnologia;

c. Considerar que os processos desses prestadores de serviços também serão escopo da avaliação de segurança realizado pela SCC Check;

d. Assegurar que o mesmo prestador de serviços não possua contrato semelhante com outro empresa do mesmo setor da SCC Check.

Para que os usuários possam utilizar meio de acesso Logon Master é necessária a troca de senha periódica;

É recomendado implementar uma troca de senha ao usuário Logon Master para evitar o vazamento da senha e a ocorrência de fraudes.

Continuidade de Negócios e Recuperação de Desastres;

Em caso de sinistro é de responsabilidade do usuário um nível de atendimento/suporte mínimo para seus clientes.

Segurança Física.

Responsabilidade do usuário implementar controles que minimamente protejam a integridade física do ambiente da empresa, tais como:

i. Definição dos controles necessários para uma dependência segura;

ii. Controle de acesso físico às áreas restritas (ex.: sala de servidores).

Histórico do documento:
Data criação: 02/2019
Atualizado em: 05/2021
Atualizado em: 02/2022