Anexo No. 3 del Documento Técnico para la Implementación del Acuerdo Número 024-2007 del Directorio de la SAT

Criterios de certificación de seguridad informática

Versión 1.1

CONTENIDO

1. Generalidades

1.1 Objetivo

Complementar el Documento Técnico para la Implementación del Acuerdo Número 024-2007 del Directorio de la Superintendencia de Administración Tributaria en lo relativo a criterios para la certificación de la seguridad informática.

1.2 Alcance

El presente documento describe los criterios de evaluación mínimos de seguridad informática que deberán aplicar las empresas autorizadas para la Certificación del Sistema FACE durante el primer año de operación de este régimen optativo.

Este documento no describe el proceso de certificación, metodología empleada o normas de auditoria y seguridad informática aplicable dado que las mismas son responsabilidad de las empresas autorizadas como certificadores, las cuales han demostrado dentro del proceso de autorización que su labor está respaldada en la experiencia, metodologías y respaldo de personal profesional en la materia.

2. Criterios de Seguridad Informática

2.1 Aspectos contractuales

La SAT ha realizado un proceso de autorización para empresas que pueden prestar el servicio de certificación del sistema FACE, estableciendo un contrato entre SAT y cada una de las empresas en el cual se han establecido los criterios y compromisos de los certificadores del sistema FACE autorizados en relación a los criterios descritos en el presente documento.

Las empresas que deseen ser GFACE tiene libertad de elección entre cualquiera de las empresas, siempre que no guarden una relación que genere conflicto de intereses entre ambas empresas. La contratación del servicio de certificación del sistema FACE es responsabilidad exclusiva de la empresa y la relación contractual entre la empresa contratante y la empresa certificadora del sistema FACE es ajena a la SAT.

La SAT, de acuerdo al contrato establecido puede solicitar la documentación de los informes finales de la empresa, no así de la documentación sensible o confidencial propiedad de la GFACE.

2.2 Criterios mínimos a evaluar

2.2.1 Segmentación lógica de Infraestructura

Los equipos que formen parte de la infraestructura del GFACE deben estar segmentados lógicamente, por medio de redes virtuales y firewall, separando los equipos del sistema FACE de otros equipos utilizados en la infraestructura.

Esto comprende también la separación de equipos en producción del resto de las aéreas y de los otros servidores que pudiera tener un GFACE, por ejemplo, ambiente de desarrollo a nivel de servidores y segmentos de red.

En esta segmentación debe considerarse que los equipos de base de datos y aquellos destinados al almacenamiento de la información no podrán estar en el mismo segmento de los servidores de aplicación que sean conectados hacia Internet o los EFACE.

2.2.2 Protección Perimetral

El GFACE debe garantizar que cuenta con equipos de protección perimetral que protejan de los distintos tipos de acceso hacia el sistema, por ejemplo:

- Enlace a SAT
- Enlaces a clientes (EFACE), si los hubiere.
- Internet
- Zona desmilitarizada

Esta configuración no implica que deba tenerse un equipo para cada enlace, pero si interfaces distintas para cada zona.

Esta protección, adicional a la protección que se deriva de reglas de acceso en el cortafuegos, debe proveer protección contra:

- Código Malicioso
- Ataques de penetración
- Ataques de denegación de servicio

Es un requerimiento que esta protección cuente con redundancia, por ser un elemento crítico de la infraestructura.

2.2.3 Procedimientos y control de acceso físico y lógico al centro de cómputo

Deben estar formalmente establecidos e implementados procedimientos de control de acceso físico y lógico al centro de cómputo, los cuales como mínimo deben considerar:

- Que se encuentre definida la responsabilidad de la seguridad física del centro de cómputo.
- Que exista un procedimiento de autorización y una bitácora de ingreso al centro de cómputo donde esté instalado el sistema.
- Que existan bitácoras de las personas autorizadas y las personas que ingresan al centro de cómputo.
- Que existan controles implementados con cámaras, sensores y controles de ingreso electrónicos.
- Debe establecerse la supervisión a los controles de acceso físico por parte de una persona ajena a la administración del centro de cómputo.

2.2.4 Controles de accesos a BD y servidores

El GFACE debe establecer formalmente los controles de acceso mínimos y procedimientos de autorización de acceso a los servidores de base de datos y servidores, los cuales serán evaluados de acuerdo a mejores prácticas comunes en materia de seguridad informática.

Estos controles deben definir como mínimo:

- Administración de usuarios, a todo nivel y para todo componente de la plataforma. (P.Ej.: base de datos, sistemas operativos, equipos de red)

- Definición de roles y perfiles de acceso acorde a las políticas de acceso y tomando en consideración la segregación de funciones del personal.

2.2.5 Aspectos físicos mínimos de la ubicación física de los GFACE en donde el sistema FACE este corriendo

El Centro de cómputo deberá ser exclusivo para procesar operaciones del sistema de facturación electrónica.

Deberá estar construido con materiales resistente a las llamas.

El diseño del centro de cómputo deberá hacerse tomando en cuenta las regulaciones y protecciones en el evento de terremoto o inundaciones.

No deberá tener paredes o ventanas que que permitan el acceso directo desde la calle y deben contar con las medidas necesarias para asegurar su perímetro físico y protección de las áreas.

Deberá tener sistema de control de acceso, permitiendo únicamente el acceso a personal autorizado, de acuerdo a los controles de acceso físico definidos en su política de seguridad

Vigilancia por medio de cámara con grabación de acuerdo a una política establecida, considerando un resguardo de por lo menos 6 meses.

Alarma contra robos y accesos no autorizados.

Deberá contar con puertas blindadas a prueba de fuego

Redundancia en los sistemas de control ambiental.

Suministro eléctrico adecuado para el tipo y tamaño de las cargas del centro de cómputo, con las protecciones necesarias, incluyendo alimentación de respaldo.

Sistema de iluminación de emergencia.

El área donde el centro de cómputo se encuentre deberá contar con pararrayos o protección similar

Alarma contra incendios y sistema automático de supresión de fuegos.

La infraestructura de red debe estar protegida contra actos de sabotaje o vandálicos.

Los equipos de protección y de apoyo deben contar con un plan de mantenimiento preventivo.

La construcción debe ser adecuada para un centro de cómputo y considerar cableado estructurado y seguro.

Localización apropiada de servidores y equipo electrónico (gabinetes con cerradura)

2.2.6 Procedimientos de Respaldo

Sistema de respaldos que garanticen como mínimo la información completa de la o las bases de datos en donde se almacena la información de las transacciones realizadas por los EFACES.

Esto incluye pero no se limita a contar con un sistema de respaldo (backups) de la información utilizada y/o generada por su sistema de cómputo y diariamente producir las copias de seguridad de los CAE generados y sus sistemas de cómputo deberán almacenar todas las transacciones y copia de los registros electrónicos de las facturas de cada EFACE generadas. Además los GFACE deben mantener una copia redundante (backup) electrónica diaria de todas las transacciones de la base de datos en un lugar alterno.

El sistema debe contar con procedimientos documentados, controles y bitácoras de respaldos y deben realizarse pruebas de restauración de la información respaldada.

Deben documentarse los procesos para atender emergencias ante la caída de servidores, enlaces y/o comunicación.

Debe existir un procedimiento de traslado periódico de respaldos hacia un sitio alterno, el cual cuente con medidas de seguridad adecuadas, incluyendo en esto la garantía de la integridad, confidencialidad y disponibilidad de los respaldos.

Retención de los respaldos de la información de acuerdo a la legislación tributaria en cuanto al tiempo de conservación de los archivos y el periodo de prescripción.

Planes y programas de prevención contra contingencias y para la custodia de la información

2.2.7 Encriptación y firma de transmisión

Es indispensable que todos los componentes internos del sistema y aquellas interfaces que se comuniquen hacia SAT o los EFACE emplean una transmisión segura, empleando para esto mecanismos como VPN, aseguradas por medio de SSL.

Para los temas de códigos de seguridad (CAE, CAEC, CRFM) y sellos digitales deberá considerase lo establecido en el Documento Técnico de Implementación y los anexos correspondientes. En el proceso de certificación deberá validarse la aplicación de los aspectos técnicos que rigen la generación de los códigos y los sellos digitales, tales como validación de las firmas de códigos de seguridad y los sellos digitales.

El GFACE deberá definir y observar procedimientos y mejores prácticas de seguridad en el manejo de las llaves de encriptación, considerando temas como cambio periódico de llaves encriptación, tanto para firma de códigos de seguridad como en temas de encripción (p. Ej. VPN).

La conexión al sistema debe ser por medio del sistema de comunicaciones seguras por Internet conocido como SSL (Secure socket layer) sobre el protocolo http (HTTPS). El término de SSL para esta publicación implica tanto el estándar SSL 3.0 así como el TLS 1.0 (Seguridad de la Capa de Transporte) o superior utilizando claves de 128-bits (o más) para claves de cifrado simétricas.

Con el objeto de brindar confiabilidad en el sistema, el servidor de la página de Internet desde donde se preste el servicio de conexión debe poseer un certificado de encriptación emitido por Autoridades de Certificación que estén contenidas como Autoridades Raíz de Confianza en los navegadores Internet Explorer y Mozilla Firefox.

2.2.8 Vulnerabilidades Internas – Revisión

Los certificadores realizarán una evaluación de vulnerabilidades internas, dentro de la cual se considerará pero no se limita a:

Política de actualización de parches de todos los componentes del sistema, considerando mejores prácticas de seguridad informática.

Procedimientos definidos para el aseguramiento de los componentes, los que deben contar con un control y monitoreo periódico, siendo estos evaluados por los certificadores.

Los certificadores deben ejecutar revisiones de vulnerabilidades utilizando las herramientas que consideren convenientes de acuerdo su metodología de trabajo.

2.2.9 Vulnerabilidades Externas – Revisión

La revisión de vulnerabilidades externas se refiere a la revisión de la seguridad de todo servicio (puerto, servidor, aplicación) que este expuesto a un tercero, la cual debe hacerse desde afuera de la protección perimetral de cada zona expuesta. Si esto no es posible, por ejemplo, que la exposición sea por medio de una VPN, se evaluará localmente al segmento de red la seguridad del servicio expuesto.

El aseguramiento del perímetro deben considerar y el certificador revisará, que se empleen las reglas de mínimo acceso requerido y que por defecto se utilice la regla de denegación de todo tráfico.

Todo servicio permitido o expuesto hacia una zona debe estar justificado y contar con documentación y controles apropiados.

Los certificadores deben ejecutar revisiones de vulnerabilidades utilizando las herramientas que consideren convenientes de acuerdo su metodología de trabajo.

2.2.10 Segregación de Equipos

Como norma general, los equipos no deben compartir funciones, por lo que se debe evaluar que los equipos:

- Deben ser usados solo para el GFACE y los procesos propios del Sistema FACE.
- Equipos físicos no pueden ser compartidos con terceros o con aplicaciones ajenas al sistema FACE.
- Cada equipo debe servir para una función única con el objeto de poder asegurar al máximo cada componente.
- Toda vez que se definan mecanismos de redundancia y de continuidad del servicio, se puede utilizar la virtualización, pero como mínimo deberá contemplarse servidores redundantes y almacenamiento de alta disponibilidad.

2.2.11 Documentación de configuraciones

Todo el sistema e infraestructura debe estar debidamente documentado y contar además con procedimientos de gestión de cambios, traslado a producción, monitoreo y bitácoras, tanto para hardware como para software.

Esta documentación debe mantenerse actualizada y además tener un resguardo adecuado de toda la documentación de acuerdo al nivel de sensibilidad de la misma. Es requerido mantener una copia de la documentación en una ubicación alterna, de acuerdo a una política definida.

2.2.12 Procedimientos de Contingencia – Alta disponibilidad

Los equipos y elementos de redes deben tener alta disponibilidad, la cual deberá considerar como objetivo que el sitio primario garantice el uptime requerido en el Acuerdo de Directorio Número 24-2007.

Esto implica que todos los componentes críticos (incluyendo pero no limitando a servidores, redes, enlaces de telecomunicaciones) deben tener redundancia.

Se requiere que el almacenamiento de la información se realice en subsistemas de disco que implemente por lo menos el sistema de redundancia RAID 5.

También es importante que el GFACE posea procedimientos de recuperación en caso de desastre, los cuales deben atender el acuerdo de nivel de servicio que ofrezcan a sus clientes.

2.2.13 Administración de antivirus

El GFACE debe implementar sistemas y procedimientos de antivirus y protección de código malicioso en su centro de cómputo y en toda su red de operaciones.

Debe garantizar que ha tomado acciones para prevenir infecciones y sobre todo la propagación de virus y otro código malicioso dentro de su red y hacia los terceros con quien tiene relación.

2.2.14 Bitácoras

Se evaluará que se cuente con una política adecuada de manejo de bitácoras que contemple el control, monitoreo y auditoria de las mismas con el fin de garantizar su continuidad, integridad y utilidad.

Deben verificarse, pero no limitarse a los siguientes tipos de bitácoras:

- Bitácoras de auditoria de aplicaciones
- Bitácoras de auditoria de base de datos
- Bitácoras de auditoria de sistemas operativos

Es importante que el procedimiento y políticas incluyan definición respecto al respaldo y retención de bitácoras

2.2.15 Políticas de Seguridad escritas y publicadas

Se revisará la existencia y se evaluará el contenido de las políticas de seguridad escritas y publicadas, conforme a la metodología y mejores prácticas de seguridad informática.

Como mínimo estas deben incluir:

- Uso de contraseñas
- Conexión con terceros
- Documentos de controles lógicos de acceso a las instalaciones
- Documentos de controles lógicos de acceso al centro de cómputo
- Documentos de controles lógicos de acceso a las aplicaciones
- Documentos de controles lógicos de acceso a los sistemas operativos
- Documentos de controles de acceso físico
- Criterios de segmentación de funciones
- Confidencialidad y Privacidad

2.2.16 Controles sobre personal

Como parte de las prácticas de seguridad, también se evaluaran aspectos vinculados a los procesos de gestión del personal, para lo cual debe considerarse:

Que exista un proceso de selección y reclutamiento documentado y que considere aspectos relacionados con seguridad, que incluya pero no se limite a:

- Verificación de antecedentes e historial laboral del personal contratado.
- Contratos firmados, laborales y acuerdos de confidencialidad.
- Manuales y descriptores de puestos.
- Procedimientos documentados para la terminación de la relación laboral.

Es importante que en su estructura de organización consideren la separación de funciones, para lo cual con el fin de aplicar mejor los controles de seguridad deberán separarse las funciones del personal de los departamentos de desarrollo del departamento de producción y operaciones.