CHECKLIST PARA CERTIFICAR LA SEGURIDAD DEL GFACE

Para certificar la seguridad informática de un Generador de Facturas Electrónicas (GFACE) que desea continuar brindando su servicio, la entidad Certificadora debe verificar que son cumplidos estos requisitos.

GFACE
Nombre:_____
NIT: _____
CERTIFICADOR
Nombre: _____
NIT: _____
RESULTADO DE LA VERIFICACIÓN
¿Cumple con TODOS los requisitos del presente checklist? *(ingrese SÍ o NO)*:...
Fecha de finalización de la verificación: _____/_____/_____

	REQUISITOS	**Cumple**	
	SEGMENTACIÓN LÓGICA DE INFRAESTRUCTURA	**Sí**	**No**
1.	¿Existe segmentación lógica de la red a la que pertenecen los equipos?		
2.	¿Existe segmentación física o por medio de redes VLAN para mejorar el control de acceso por red?		
3.	¿Hay un firewall protegiendo los equipos con reglas específicas y denegación de tráfico por defecto?		
4.	¿Existe una DMZ o una forma de separar los servidores públicos de los privados?		
5.	¿Existe una separación lógica de los servidores de prueba y los de producción?		
	PROTECCIÓN PERIMETRAL	**Sí**	**No**
6.	¿Cuenta con un firewall?		
7.	Los enlaces hacia clientes ¿están protegidos por un firewall?		
8.	¿Cuenta con un Firewall e IPS para proteger su salida a internet?		

9.	¿No existen reglas de "allow all" en la protección perimetral?		
10.	¿Cada zona está conectada a un puerto distinto o equipo distinto?		
11.	El equipo que protege el perímetro ¿cuenta con protección contra código malicioso?		
12.	El equipo que protege el perímetro ¿cuenta con protección contra ataques de penetración?		
13.	El equipo que protege el perímetro ¿cuenta con protección contra ataques de DoS o DdoS? (Evaluar si se requiere o se pide a futuro)		
14.	¿Cuenta la protección (firewall) o las protecciones con redundancia que garantice el tiempo de disponibilidad requerido?		
15.	¿Cuenta con un inventario de servicios/puertos expuestos a terceros?		
16.	Para los servicios/puertos expuestos a terceros ¿existen reglas específicas que apliquen restricciones a puertos no autorizados? Se requiere confirmación o evidencia.		
	ACCESO FÍSICO Y LÓGICO AL CENTRO DE CÓMPUTO	**Sí**	**No**
17.	¿Existen políticas establecidas de control de acceso físico y lógico al centro de cómputo?		
18.	Dentro de las políticas ¿se encuentra definida la responsabilidad de la seguridad física del centro de computo?		
19.	¿Existe un procedimiento de autorización de acceso al centro de cómputo?		
20.	¿Existe un procedimiento de bitácora de acceso al centro de cómputo?		
21.	¿Existen bitácoras de personas autorizadas y personas que ingresan al centro de cómputo?		
22.	¿Existen cámaras que registran el ingreso al centro de cómputo?		
23.	¿Existen sensores y controles electrónicos que registren el ingreso al centro de cómputo?		
24.	¿Existe la supervisión de los controles de acceso físico al centro de cómputo por una persona ajena a la administración del centro de cómputo?		
	CONTROLES DE ACCESO A BD Y SERVIDORES	**Sí**	**No**
25.	¿Existe y se cumple una política de acceso a los servidores y BD conforme ?		
26.	¿Existen y se cumplen los controles dentro de la política de acceso a servidores y BD?		
27.	¿Existe una política de autorización de acceso a servidores y BD?		
28.	¿Existen y se cumplen los controles dentro de la política de autorización de acceso a servidores y BD?		
29.	¿Existen y se cumplen los controles de administración de usuarios?		
30.	¿Existe una definición de roles y perfiles de acceso de acuerdo a las políticas de acceso y considerando la segregación de funciones del personal?		

	UBICACIÓN FÍSICA DEL SISTEMA FACE	**Sí**	**No**
31.	El centro de cómputo donde se encuentre la infraestructura que soporta la operación del sistema FACE, ¿cuenta con las mejores prácticas aplicables?		
32.	En el caso de colocación de la infraestructura del GFACE, ¿se cuenta con un contrato que garantice las condiciones de seguridad del centro de cómputo?		
33.	En el caso de colocación, ¿el gabinete es exclusivo y cuenta con medidas de seguridad propias del GFACE?		
34.	¿Está construido con materiales resistentes a las llamas?		
35.	¿Cumple con regulaciones y protecciones para eventos sísmicos e inundaciones?		
36.	¿Alguna de sus paredes tiene acceso directo a la calle?		
37.	¿Cuenta con ventanas que den acceso directo a la calle?		
38.	¿Los sistemas de control de acceso cumplen con los controles establecidos en la política de acceso?		
39.	¿Las cámaras de seguridad cuentan con un resguardo de los últimos 6 meses?		
40.	¿El centro de computo cuenta con alarma antirrobo y de acceso no autorizado?		
41.	¿Las puertas del centro de cómputo son blindadas y contra incendios?		
42.	¿Cuenta con redundancia en los sistemas de control ambiental?		
43.	¿Cuenta con tierra física?		
44.	¿Cuenta con un suministro eléctrico adecuado?		
45.	¿Cuenta con una unidad de alimentación de respaldo de acuerdo a la carga de equipos que posee?		
46.	¿Cuenta con un sistema de iluminación de emergencia?		
47.	¿Cuenta con una alarma contra incendios y supresión automática de fuegos?		
48.	¿Los equipos de protección y apoyo cuentan con un contrato de mantenimiento preventivo?		
49.	¿Cuenta con alguna certificación del cableado estructurado del centro de computo?		
50.	¿Los servidores y equipo electrónico se encuentran en gabinetes con cerradura?		
	PROCEDIMIENTOS DE RESPALDO	**Sí**	**No**
51.	¿Existe un sistema de respaldos para las bases de datos en donde se almacenan las transacciones realizadas por los EFACES?		
52.	¿Se producen copias diarias de los CAE generados?		

53.	¿Se tiene copia de seguridad diaria de las transacciones y copia de los registros electrónicos de las facturas generadas?		
54.	¿Existe una copia redundante electrónica diaria de todas las transacciones de la base de datos en un lugar alterno?		
55.	¿Existen procedimientos documentados?		
56.	¿Existen controles de la realización de los respaldos?		
57.	¿Existen bitácoras de los respaldos?		
58.	¿Se realizan pruebas de restauración de la información respaldada?		
59.	¿Existen procesos documentados de cómo atender las emergencias ante la caída de servidores, enlaces y/o comunicación?		
60.	¿Existe un procedimiento de traslado periódico de respaldos hacia un sitio alterno?		
61.	¿En el procedimiento de traslado se garantiza la integridad, confidencialidad y disponibilidad de los respaldos?		
62.	¿La retención de los respaldos está de acuerdo a la legislación tributaria en cuanto al tiempo de conservación de los archivos?		
63.	¿Existen planes y programas de prevención contra contingencias y de custodia de la información?		
64.	¿La ejecución de la prueba de restauración del último respaldo del ambiente de operación en una plataforma diferente a la de producción fue exitosa?		
	ENCRIPTACIÓN Y FIRMA DE TRANSMISIÓN	**Sí**	**No**
65.	La comunicación entre los EFACE y la SAT ¿está encriptada de alguna manera?		
66.	¿Está validado el proceso de generación de códigos de seguridad (CAE, CAEC, CRFM)?		
67.	¿Existen procedimientos y mejores prácticas en el manejo de llaves de encriptación?		
68.	La conexión al sistema ¿cuenta con un certificado SSL de 128 bits o más de encriptación?		
69.	Toda operación del sistema por Internet ¿se realiza por protocolos seguros (SSL 3.0 o TLS 1.0 o superior)?		
70.	El servidor web publicado en Internet ¿cuenta con un certificado emitido por una Autoridad Raíz de confianza reconocida?		
71.	No existe ninguna transacción del sistema publicada bajo protocolos inseguros (Por ejemplo: HTTP o FTP)		
	SEGREGACIÓN DE LOS EQUIPOS	**Sí**	**No**
72.	Los equipos ¿se utilizan únicamente para el GFACE y el sistema FACE?		
73.	¿Existen servidores redundantes?		

74.	¿Existe almacenamiento en alta disponibilidad?		
	DOCUMENTACIÓN DE LAS CONFIGURACIONES	**Sí**	**No**
75.	¿Existe documentación del sistema de infraestructura?		
76.	¿Existe un mapa de red?		
77.	¿Existe un diagrama de funciones de los servidores y equipos?		
78.	¿Existe un procedimiento de Gestión de Cambios? Incluyendo su traslado a producción.		
79.	¿Existe un procedimiento de monitoreo de bitácoras de hardware y software?		
80.	¿Existe una copia de esta documentación en un sitio alterno?		
	PROCEDIMIENTOS DE CONTINGENCIA	**Sí**	**No**
81.	¿Cuentan los equipos y elementos de red con alta disponibilidad que garantice el tiempo de funcionamiento requerido? Esto incluye servidores, equipos de red y enlaces.		
82.	¿El almacenamiento se da en un subsistema de disco que tenga al menos RAID5?		
83.	¿Existen procedimientos de recuperación en caso de desastre?		
	BITÁCORAS	**Sí**	**No**
84.	¿Existe una política de manejo de bitácoras que contemple un almacenamiento, control, monitoreo y auditoría de las mismas?		
85.	¿Existen bitácoras de auditoría de aplicaciones?		
86.	¿Existen bitácoras de auditoría de bases de datos?		
87.	¿Existen bitácoras de auditoría de sistemas operativos?		
88.	¿Existe una política de respaldo y retención de bitácoras?		
	POLÍTICAS DE SEGURIDAD	**Sí**	**No**
89.	¿Existen políticas de seguridad y están estas publicadas?		
90.	¿Cuenta con una política de uso de contraseñas?		
91.	¿Cuenta con una política de conexión a terceros?		
92.	¿Cuenta con documentos de controles lógicos de acceso a instalaciones?		
93.	¿Cuenta con documentos de controles lógicos de acceso al centro de computo?		
94.	¿Cuenta con documentos de controles lógicos de acceso a las aplicaciones?		
95.	¿Cuenta con documentos de controles lógicos de acceso a los sistemas operativos?		
96.	¿Cuenta con documentos de controles de acceso físico?		

97.	¿Cuenta con criterios de segmentación de funciones?		
98.	¿Cuenta con políticas de confidencialidad y privacidad?		
99.	¿Cuentan con política y procedimiento de control de configuración?		
100.	¿Cuentan con política y procedimiento de control de cambios de software?		
	CONTROLES SOBRE EL PERSONAL	**Sí**	**No**
101.	¿Existe un proceso de selección y reclutamiento documentado?		
102.	¿Se revisan antecedentes e historial laboral de la persona?		
103.	¿Existen contratos laborales firmados y acuerdos de confidencialidad?		
104.	¿Existen manuales y descriptores de puestos?		
105.	¿Existen procedimientos documentados para la terminación de la relación laboral'		
106.	¿El personal de desarrollo es distinto al de producción?		
	ANTIVIRUS	**Sí**	**No**
107.	¿Cuenta con Antivirus en su centro de datos y en su red de operaciones?		
	GESTIÓN DE VULNERABILIDADES	**Sí**	**No**
108.	¿Cuenta con política de actualización de parches para todos los componentes del sistema?		
109.	¿Cuenta con una política y procedimientos de aseguramiento de componentes con supervisión comprobable?		
110.	¿Tiene evidencia de revisiones y mitigación de vulnerabilidades internas y DMZ de los últimos tres meses?		
111.	¿Es aceptable el nivel de vulnerabilidades detectado o sus medidas de mitigación? Medidas de mitigación en marcha para todas las vulnerabilidades altas (CVSS scrore >=7)		
112.	¿Tiene evidencia de revisiones y mitigación de vulnerabilidades externas (Internet) de los últimos tres meses?		
	CASOS DE PRUEBA	**Sí**	**No**
113.	Verificar con evidencia documental de los sistemas de producción que el sistema cumple con los tiempos de respuesta requeridos en la prueba de estrés.		
114.	Vulnerabilidades internas: Parches actualizados en todos los componentes del sistema FACE; endurecimiento de servidores y equipos (verificado por ente certificador)		
115.	Vulnerabilidades externas: Parches actualizados en todos los componentes del sistema FACE; endurecimiento de servidores y equipos (verificado por ente certificador)		