Matriz de Controles para la Revisión de Seguridad para los Aspirantes a PCGCFDISP - Revisión de Seguridad

Área de Control	Sub-área de Control	ID Control	Control	Interpretación del Control	Periodicidad / Parámetro Requerido
Postura de la Empresa sobre la Seguridad de la Información					
	Política de Seguridad de la Información	1	Política de Seguridad de la Información	El Aspirante debe contar con un documento de Política de Seguridad de la Información autorizado. Debe estar publicado y disponible para el personal interno y terceros que colaboren con la empresa, dicho documento deberá de ser revisado periodicamente.	6 Meses
	Organización Interna	2	Compromiso de la Dirección	La Alta dirección debe apoyar activamente la seguridad de la información y demostrar su compromiso al respecto.	
		3	Acuerdos de Confidencialidad	El Aspirante debe tener acuerdos de confidencialidad y/o acuerdos de no divulgación firmados por el personal y el aspirante. Dichos Acuerdos deberán de aplicarse a personal interno y externo involucrado en el proceso de CFDI. Los Acuerdos de confidencialidad y/o acuerdos de no divulgación, debén de señalar que la responsabilidad de confidencialidad de la información, se mantiene de manera permanente, aun cuando el personal concluye su relación laboral con el aspirante.	
		4	Contacto con Grupos de Interés Especial	El Aspirante debe de establecer contacto con grupos especializados en seguridad de la Información y/o asociaciones especialistas en la materia.	
	Clasificación de la Información	5	Política y etiquetado de clasificación de la Información	El Aspirante debe de contar con un documento de Política de Clasificación de la Información autorizado. Debe estar publicado y disponible para el personal interno y terceros que colaboren con la empresa, dicho documento deberá de ser revisado periódicamente. El Aspirante debe de contar con un documento Procedimiento de Etiquetado de Información, que incluya la información física y electrónica involucrada en el proceso de CFDI, con el nivel mas alto de confidencialidad.	6 meses
Seguridad en el Personal					
	Personal Interno	6	Selección del Personal	El Aspirante debe de llevar a cabo la verificación de antecedentes de todos los candidatos a puestos internos dentro de la organización.	
		7	Responsabilidades del Personal Interno	El Aspirante debe de formalizar las responsabilidades del personal externo con respecto a la seguridad de la información.	
		8	Capacitación del Personal en materia de Seguridad de la Información	El Aspirante debe definir un Plan de capacitación al personal interno en Seguridad de la Información, al inicio de la relación laboral de manera periódica.	
	Personal Externo	9	Identificación de Riesgos inducidos por terceros	El Aspirante debe de identificar los riesgos inducidos por terceros al proceso de CFDI en cuanto a la seguridad de la información y a los medios de procesamiento con los que dispone.	
	Responsabilidades de los Usuarios	10	Uso de contraseñas	El Aspirante debe de contar con un documento Política de uso de contraseñas, donde se señale la responsabilidad de los usuarios en el uso de las mismas. El documento de Política de uso de contraseñas, debe de señalar las medidas de protección de las mismas, así como la caducidad, entre otras.	
		11	Equipo desatendido	El Aspirante debe de contar con un documento de Política de equipo desatendido que señale los requerimientos de seguridad, para el equipo cuando el usuario no está físicamente presente.	
	Terminación del Empleo	12	Eliminación de Derechos de Acceso	El Aspirante debe de contar con un documento Política de eliminación de derechos de Acceso, el cual debe de estar publicado, actualizado y disponible para el personal Interno del aspirante. El Aspirante debe de contar con un documento Procedimiento de eliminación de accesos lógicos y físicos.	
		13	Devolución de Activos	El Aspirante debe de contar con procedimientos que señalen la devolución de los activos del personal interno cuando concluye su relación laboral.	
Gestión de los Activos					
	Gestión de los Activos	14	Inventario de Activos	El Aspirante debe de identificar e inventariar todos los activos involucrados en el proceso de CFDI, dicho inventario debe de ser actualizado periódicamente y especificar la propiedad de los mismos.	
Seguridad Física en Oficinas					
	Seguridad Física	15	Perímetro de Seguridad Fisica	El Aspirante debe definir y utilizar perímetros de seguridad Física como son: Controles de Acceso, puertas de ingreso controlado, policías o recepcionistas, para proteger áreas operativas y de oficina que contienen información del proceso de CFDI.	

Área de Control	Sub-área de Control	ID Control	Control	Interpretación del Control	Periodicidad / Parámetro Requerido
Procesos de Gestión de la Seguridad					
	Gestión de Riesgos	16	Análisis de Riesgos	El aspirante debe de contar con Documento Análisis de Riesgos sobre el proceso de CFDI, el cual señale como mínimo los siguientes: - Identificación de los Activos involucrados - Identificación de Amenazas - Identificación de Vulnerabilidades - Estimación de los Riesgos - Clasificación de Riesgos - Priorización de los Riesgos a mitigar - Reporte de riesgos encontrados - Plan de mitigación de Riesgos (Prioritarios)	
	Manejo de Incidentes y Problemas	17	Incidentes y Problemas	El aspirante debe de contar con Documento política para la Gestión de Incidentes y problemas de Seguridad en el proceso de CFDI. el cual debe de estar publicado, actualizado y disponible para el personal Interno, el cual señale como minimo: - Identificación de Incidentes y Problemas - Registro de Incidentes y Problemas - Notificación y Escalación de Incidentes y Problemas - Seguimiento de Incidentes y Problemas - Notificación al SAT	12 meses
	Monitoreo de Seguridad	18	Definición de Eventos de Seguridad	El aspirante debe de definir los eventos de seguridad sujetos a monitorear en el proceso de CFDI. Dicha definición deberá de considerar al menos los siguientes: - Uso de cuentas privilegiadas. - Acceso a información con clasificación alta de confidencialidad.	
		19	Bitácoras de Eventos	El aspirante debe de implementar la creación y resguardo de bitácoras donde se almacenen los eventos de seguridad relevantes. Las bitácoras deben ser resguardadas en un lugar seguro por lo menos durante 6 meses. Las bitácoras de eventos deben tener acceso controlado sólo a personal autorizado y se debe guardar un registro de la consulta de las mismas.	6 meses
	BCP	20	Plan de Continuidad del Negocio (BCP)	El aspirante debe de contar con un Plan de Continuidad de Negocio (BCP), acorde al proceso de CFDI, el cual debe ser actualizado y probado periódicamente e incluir como mínimo: - Identificación de los activos que le dan soporte al proceso. - Requerimientos de procesamiento, personal. - Información y todo lo necesario para garantizar la continuidad del servicio de CFDI. - Plan de Pruebas	12 Meses
Seguridad de la Plataforma Tecnológica					
	DRP	21	Plan de Recuperación de Desastres (DRP)	El aspirante debe de contar con un Plan de Recuperación de Desastres (DRP), acorde al proceso de CFDI, el cual debe ser actualizado y probado periódicamente e incluir como mínimo: - Identificación de los activos que le dan soporte al proceso. - Plan de Pruebas	12 Meses
	Control de Accesos Lógicos Locales y Remotos	22	Política de Control de Accesos	El aspirante debe de contar con Documento de Política de Control de Acceso que aplique a todos los activos acorde al proceso de CFDI, el cual debe ser actualizado y probado periódicamente. El aspirante debe de contar con un procedimiento de Altas, Bajas y Cambios de Accesos de Usuarios.	6 meses

Área de Control	Sub-área de Control	ID Control	Control	Interpretación del Control	Periodicidad / Parámetro Requerido
	Centro de Datos	23	Requisitos de seguridad en el centro de datos	El Aspirante debe alojar los activos de infraestructura tecnológica clave que soportan el proceso de CFDI en un centro de datos primario que cuente con las siguientes mecanismos y servicios de soporte: - Instalaciones libres de altos riesgos (por lo menos a 100 m de lugares como gasolineras, gaseras, minas, etcétera) y con una instalación no evidente. - Control de acceso físico sólo a personal autorizado a través de un procedimiento y registro de accesos a las instalaciones y áreas restringidas. - Personal de vigilancia y monitoreo las 24 horas y un sistea de monitoreo de las instalaciones (CCTV) con un historial de al menos 30 días. - Detección y supresón de incendios. - Señalización de áreas restringidas, rutas de evacuación y ubicación de equipo de emergencia para el personal. - Aire acondicionado (sensor de temperatura, enfriamiento). - Sistemas de energia Initerrumpida (UPS) suficiente para los equipos del centro de datos. - Plantas generadoras de energía eléctrica de emergencia suficente para los equipos del centro de datos. - Planes de mantenimiento de al menos 6 meses y contratos vigentes de los mecanismos y servicios de soporte.	
	Comunicaciones	24	Prevención y Detección de Intrusos	El aspirante debe definir una separación lógica de los activos de infraestructura tecnológica que soportan o son utilizados en la administración del proceso de CFDI en una red segmentada del resto de los activos tecnológicos de las áreas de la organización; en los segmentos clave de la red se debe contar con dispositivos de prevención o detección de intrusos. El acceso entre redes debe estar restringido a través de listas de control de acceso.	
		25	Actualizaciones	El Aspirante debe instalar los últimos parches de seguridad y actualizaciones emitidas por el fabricante, organización o empresa responsable del hardware o software para los activos de infraestructura tecnológica que soportan o son utilizados en la administración del proceso de CFDI; la implementación o instalación de estas actualizaciones deben haber cumplido con un procedimiento de pruebas previas.	
	Respaldos	26	Respaldos	El Aspirante debe generar respaldos de los activos tecnológicos de soporte y la información utilizada en el proceso de CFDI, con una periodicidad semanal total para las bases de datos y el resto de la información en un esquema no mayor a dos meses definido por la empresa; el esquema debe considerar en su alcance el respaldo de configuraciones de dispositivos de red, middleware, DBMS, aplicativos y media; además de información de la operación del proceso de CFDI.	
		27	Destrucción o Borrado	Los medios de almacenamiento físico o lógico donde se almacena información de los contribuyentes, del SAT o del proceso de CFDI, deben estar sujetos a un procedimiento y registro de destrucción física o borrado lógico seguro que debe registrar como mínimo: - Fecha, hora, lugar, medio de almacenamiento, mecanismo de destrucción o borrado, resultado, personal que lo realiza.	
	Criptografía	28	Criptografía en servicios expuestos	Los servicios tecnológicos, aplicativos o transferencias de información a través de redes externas o accedidos desde Internet deben utilizar certificados, protocolos criptográficos u otros mecanismos que aseguren la confidencialidad de la información.	
		29	Protección de Llaves y Certificados	El Aspirante debe contar con un mecanismo de protección de llaves y Certificados usados para el cifrado que impidan la extracción de la información o que comprometa el resguardo de llaves y certiicados. El mecanismos debe implementar las siguientes medidas: - Control de Accesos Físicos y Lógicos (Sólo personal autorizado). - Registro de Hashes de Control. - Segregación de roles con acceso a los dispositivos de almacenamiento de llaves y certificados. - Instalación única de la llave provista por el SAT (respaldada por un acta firmada por los responsables de su instalación y custodia).	
	Protección Contra Código Malicioso	30	Protección contra Código Malicioso	El Aspirante debe contar con una solución de protección contra código malicioso instalada y actualizada para los activos de infraestructura tecnológica que soportan o son utilizados en la administración del proceso de CFDI.	
	Separación de Ambientes	31	Separación de Ambientes	El Aspirante debe separar física o lógicamente los ambientes tecnológicos de desarrollo y/o pruebas y producción en soporte al proceso de CFDI, unos de otros y todos deben tener su propia administración de accesos. Las cuentas existentes en cada ambiente deben estar debidamente identificadas y registradas a personal autorizado.	
		32	Aislamiento de información de CFDI	El Aspirante debe estar separar física o lógicamente los activos de infraestructura tecnológica que soportan el proceso de CFDI de la información de otros procesos o aplicativos proporcionados por la empresa.	
		33	Documentación	El Aspirante debe contar con documentación técnica completa, del aplicativo utiizado en el proceso de CFDI, que incluya como mínimo lo siguiente: - Descripción de módulos y funcionalidades. - Flujo de Datos. - Modelo y Diccionario de Datos. - Diagrama de implementación.	
		34	Control de Accesos	El Aspirante debe contar en el aplicativo utilizado en el proceso de CFDI con un módulo o mecanismo de control automatizado de accesos autorizados, de acuerdo a las políticas y procedimientos de control de accesos definidos.	
		35	Control de Cambios	El Aspirante debe contar con un proceso formal de control de cambios para los activos de infraestructura tecnológica que soportan o son utilizados en la administración del proceso de CFDI, el cual debe incluir como mínimo: - Estimación de impacto de cambios. - Ejecución de pruebas previo al cambio. - Autorización. - Liberación de cambios. - Reversos de cambios (rollback).	

Área de Control	Sub-área de Control	ID Control	Control	Interpretación del Control	Periodicidad / Parámetro Requerido
	Seguridad en Aplicativo	36	Bitácoras	El Aspirante debe contar con bitácoras de acceso y uso del aplicativo utilizado en soporte del proceso de CFDI que deben contener como mínimo: - Fecha y hora. - Usuario. - IP origen. - Registro de intentos de acceso fallidos. - Registro de accesos exitosos. - Registro de actividad de los usuarios. - Registro de cierre de sesión ya sea por inactividad o por parte del usuario. - Registro de consulta de las propias bitácoras. - Registro de errores y/o excepciones.	
		37	Expiración de sesión por inactividad	El aspirante debe implementar en el aplicativo utilizado en soporte del proceso de CFDI sesiones que expiren	10 minutos
		38	Línea base de seguridad	El Aspirante debe tener aplicada una línea base de seguridad en el aplicativo utilizado en el proceso de CFDI que debe incluir como mínimo: - Implementación de autenticación de los usuarios (internos o clientes). - Implementación de mecanismo de no repudio de transacciones. - Protección contra inyección de código. - Inicio de sesión seguro. - Validación de datos de entrada / salida para evitar errores en el procesamiento de la información. - Manejo de errores.	
	Transaccionalidad	39	NTP	El Aspirante debe implementar un mecanismo de sincronización de NTP con GPS para las transacciones de timbrado del proceso de CFDI.	
	Encripción de Datos	40	Encripción de Datos de los Contribuyentes	El Aspirante debe contar con una política y procedimientos formales que aseguren que la información de facturación y los datos personales de los Contribuyentes deban estar cifrados tanto en su almacenamiento, tránsito y medios que los contengan.	
Cumplimiento Legal y Regulatorio					
	Cumplimiento con Leyes y Regulaciones Aplicables	41	Conocimiento de Leyes y Regulaciones Aplicables	EL Aspirante debe presentar un documento autorizado donde incluya como mínimo lo siguiente: - Declare que conoce y respetará el apego a las leyes aplicables vigentes. - Indique que conoce su responsabilidad de verificar el cumplimiento con dichas leyes. - Exime al SAT de cualquier responsabilidad derivada del incumplimiento de las leyes aplicables.	