ID Control	Control	Objetivo del Control	Interpretación del Control	Tipo de Control	Periodicidad / Parámetro Requerido
I.- Postura de Seguridad de la Información					
1	Política de Seguridad de la Información.	Establecer el Compromiso de la Alta Dirección con respecto a la Seguridad de la Información.	Se debe definir una Política de Seguridad de la Información, aprobada por la alta dirección, publicada y comunicada a empleados proveedores y terceros, que intervienen en proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos.
2	Compromiso de la Dirección.	Asegurar el cumplimiento, con lo dispuesto en las políticas y procedimiento organizacionales en materia de seguridad de la Información.	Se debe requerir a empleados, proveedores y terceros la aplicabilidad de lo dispuesto, en las políticas y los procedimientos establecidos en materia de seguridad de la Información.	**Administrativo**	
3	Política de clasificación de la Información.	Establecer los lineamientos organizacionales, en materia de seguridad de la información, aplicable a los activos de información, con el propósito de prevenir el mal uso de los mismos.	Se debe contar con una política de Clasificación de la Información, aprobada por la Alta Dirección, publicada y comunicada a los empleados en relación a su valor, requisitos legales, sensibilidad y criticidad para la organización.	**Administrativo**	1 vez al año / En cambios Tecnológicos.
3.1	Etiquetado de Información.	Comprobar la correcta implementación de lo dispuesto en la política de Clasificación de la Información referente al etiquetado de información.	Se debe de implementar procedimientos formales para el etiquetado y tratamiento de la información, conforme a la Política de clasificación de la información definida.	**Administrativo y Técnico**	
II.- Gestión de Activos					
4	Inventario de Activos.	Establecer los Activos de Información con los que la organización opera, con la intención de identificar en su totalidad los componentes tecnológicos requeridos.	Se debe elaborar, aprobar por la alta dirección y actualizar un inventario de todos los activos de información, asociados con el proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., el cual debe asentar la responsabilidad o propiedad de un área o empleado interno.	**Administrativo**	1 vez al año / En cambios Tecnológicos.
4.1	Devolución de Activos.	Avalar, la correcta implementación de los procedimientos estipulados con respecto a la devolución de activos de Información.	Se debe de implementar procedimientos formales de devolución de los activos de información, asociados con el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	Al finalizar la relación laboral y en cambio de rol o función dentro de la organización.
III.- Gestión de Riesgos					
5	Análisis de Riesgos.	Instaurar una metodología de Análisis de Riesgos organizacional, que permita identificar y dar seguimiento a todos aquellos riesgos de TI, que puedan presentarse en la organización, acorde prácticas y estándares Internacionales.	Se debe elaborar, aprobar por la alta dirección y actualizar un análisis de riesgos sobre los activos de Información asociados con el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos

6	Pruebas de Seguridad.	Establecer mecanismos de validación tecnológica, en materia de seguridad de la información, aplicable a los activos de información críticos, que provea a la organización conocimiento sobre las posibles amenazas y vulnerabilidad que lograrán presentarse.	Se debe de efectuar pruebas de seguridad a todos los activos de Información críticos asociados con el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	1 vez al año / En cambios Tecnológicos.
6.1	Seguimiento a Pruebas de Seguridad.	Avalar, el correcto seguimiento a las pruebas de seguridad realizadas a activos de Información críticos, que provea a la organización un nivel de confiabilidad, sobre el seguimiento de los hallazgos detectados que pudieran comprometer la información.	Se debe de definir un plan de seguimiento y atención a los hallazgos detectados a los activos de Información críticos, asociados con el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	1 vez al año / En cambios Tecnológicos.
IV.- Seguridad en el Personal Interno					
7	Política de selección del Personal.	Establecer los lineamientos organizacionales, en materia de selección de personal en el ámbito de seguridad de la Información.	Se debe definir una política de selección de personal que señale a nivel alto, el cumplimiento con los requisitos de seguridad de la Información establecidos por la organización, aplicable en el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	
7.1	Selección de Personal.	Asegurar la correcta implementación de los procedimientos estipulados de selección de personal que provea a la organización un nivel de confiabilidad sobre el personal que labora en la organización.	Se debe de implementar procedimientos formales de selección de personal que incluya la verificación de antecedentes de los candidatos a puestos interno de la empresa.	**Administrativo**	Al Inicio de la Relación Laboral y en Cambio de Rol o Función dentro de la Organización
8	Responsabilidades del Personal Interno.	Instituir la responsabilidad en seguridad de la información a nivel organizacional, con la intención de formalizar el cuidado de la misma.	Se debe de formalizar la responsabilidad de seguridad de la Información a todo el personal Interno, que interviene en el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	Al Inicio de la Relación Laboral y en Cambio de Rol o Función dentro de la Organización
9	Capacitación del Personal en materia de Seguridad de la Información.	Definir programas de mejora continua, en capacitación con respecto a seguridad de la información, con la intención de obtener conocimiento actualizado en la materia.	Se debe de implementar programas de capacitación aprobados por la Alta Dirección, para el personal interno que interviene en el proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT. en materia de seguridad de la información.	**Administrativo**	1 vez al año / En cambios Tecnológicos
V.- Relación con Proveedores y Terceros					
10	Contratación de Servicios Tecnológicos.	Establecer elementos de control, en materia de seguridad de la información, con respecto al cumplimiento de las obligaciones contractuales adquiridas, con proveedores y terceros.	Se debe de contar una política de contratación con proveedores y terceros, que intervienen en el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT. Dicha política debe de establecer la responsabilidad con respecto a la seguridad de la información y el cumplimiento tecnológico de los servicios adquiridos.	**Administrativo**	

10.1	Revisión Contratación de Servicios Tecnológicos.	Definir elementos de verificación, sobre el cumplimiento sobre las obligaciones adquiridas con proveedores y terceros.	Se debe de definir un plan de revisiones de cumplimiento contractual tecnológico, con Proveedores y Terceros que intervienen en el proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT. según lo estipulado en la política de Contratación con proveedores y terceros.	**Administrativo**	1 vez al año / En cambios Tecnológicos
VI.- Gestión Física y del Entorno					
11	Perímetro de Seguridad Física en Oficinas Operativas.	Definir elementos de control, tecnológico y operativo que prevean y alerten a la organización, accesos no autorizados a las Instalaciones operativas.	Se debe de definir e implementar un perímetro de seguridad físico controlado, que restringa el acceso a personal no autorizado, a áreas relativas al proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT, en oficinas operativas.	**Administrativo y Técnico**	
11.1	Medidas de Acceso Restringido en Oficinas Operativas.	Verificar la efectividad de los elementos de control, tecnológico y operativo, que provean a la organización control del personal que ingresa a la Oficinas Operativas.	Se debe de registrar en bitácoras el acceso a áreas restringidas a personal debidamente identificado y autorizado.	**Administrativo y Técnico**	
12	Perímetro de Seguridad Física en Centro de Datos	Definir elementos de control, tecnológico y operativo que prevean y alerten a la organización, accesos no autorizados al Centro de Datos.	Se debe de definir e implementar un perímetro de seguridad físico controlado, que restringa el acceso a personal no autorizado, a áreas relativas al proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT, en el centro de datos.	**Administrativo y Técnico**	
13	Medidas en Servicios de Soporte en el Centro de Datos	Establecer servicios de soporte tecnológico, ambientales y del entorno, al proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT, en el Centro de Datos, que garanticen la disponibilidad de los servicios.	Se debe definir e implementar servicios de soporte en el Centro de Datos, con el objetivo de garantizar la disponibilidad en el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	
VII.- Control de Acceso					
14	Política de Control de Accesos	Establecer los lineamientos organizacionales, con respecto al control de acceso a los activos de información.	Se debe definir una Política de Control de Accesos aprobada por la alta dirección, publicada y comunicada a empleados proveedores y terceros, acorde al proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos
15	Eliminación de Derechos de Acceso	Comprobar la correcta implementación de lo dispuesto en la política de Control de Accesos, que provea a la organización elementos comprobatorios de su implementación.	Se debe de implementar procedimientos formales de Eliminación de Derechos de Acceso, aplicables al proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., en los casos de culminación de la relación contractual con empleado, proveedores y terceros.	**Administrativo y Técnico**	

16	Política de Contraseñas	Establecer los lineamientos organizacionales, con respecto al manejo de contraseñas.	Se debe definir una Política de contraseñas, aprobada por la alta dirección, publicada y comunicada a empleados proveedores y terceros, acorde al proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos
16.1	Uso de Contraseñas	Comprobar la correcta implementación de lo dispuesto en la política de contraseñas, que provea a la organización elementos comprobatorios de su implementación.	Se debe de definir mecanismos de gestión de contraseñas de Acceso, aplicables al proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., dichos mecanismos deben de dejar la trazabilidad a través de bitácoras.	**Administrativo y Técnico**	
VIII.- Gestión de Aplicaciones					
17	Practicas Seguras de Desarrollo	Instaurar prácticas de desarrollo seguro, apegada a estándares internacionales en la materia, las cuales provean a la organización el apego a dichas prácticas.	Se debe definir e implementar prácticas de desarrollo seguro apegadas a marcos internacionales en materia de seguridad de la Información.	**Administrativo y Técnico**	
18	Seguridad en Bases de Datos	Definir elementos de control de protección en las Bases de Datos, los cuales deberán de considerar la integridad, disponibilidad y confidencialidad de la información almacenada en ellas	Se debe de diseñar e implementar medidas de Seguridad de la Información, en las Bases de Datos.	**Administrativo y Técnico**	
19	Criptografía en Aplicaciones	Definir elementos criptográficos que provean un mecanismo de comunicación seguro, en aplicaciones, cuando se usan a través de redes públicas.	Se debe de implementar mecanismos criptográficos para las aplicaciones que intervienen el proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., que salvaguarden el intercambio de información, entre los distintos componentes tecnológicos implementados.	**Administrativo y Técnico**	
20	Separación de Ambientes	Implantar ambientes independientes, en aplicaciones que provea a la organización una estructura de desarrollo fortalecida.	Se debe de implementar una separación física o lógica de los ambientes de desarrollo, pruebas y producción en el proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	
21	Aislamiento de información	Precisar mecanismos de independencia de información de los distintos procesos operativos de la organización.	Se debe de Implementar medidas de aislamiento de la información físico o lógico del proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., de todos aquellos procesos adicionales de negocio con los que se cuenta.	**Administrativo y Técnico**	
22	Control de Versiones	Especificar medidas de control, con respecto a la liberación de las aplicaciones críticas en entornos de producción, que provea a la organización un control sobre los distintos tipos de liberaciones.	Se debe de implementar procedimientos formales de Control de Versiones sobre los aplicativos que dan soporte al proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	
23	Expiración de sesión por inactividad en aplicaciones	Definir parámetros de control, que prevean la ausencia de personal, evitando el acceso a aplicaciones de personal no autorizado.	Se debe de implementar en aplicaciones del proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., parámetros de expiración por inactividad.	**Administrativo y Técnico**	El parámetro de expiración por inactividad no deberá de ser mayor a 5 Minutos.

24	Bloqueo de Sesión	Definir parámetros de control, que prevean el bloqueo de sesión, evitando el acceso a aplicaciones de personal no autorizado a través de intentos fallidos.	Se debe de implementar en aplicaciones del proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., mecanismos de bloqueo de sesión.	**Administrativo y Técnico**	El parámetro de bloqueo no deberá de ser mayor a 5 Intentos por unidad de tiempo.
25	Documentación Tecnológica y Operativa	Constituir un control documental, actualizado sobre toda la documentación tecnológica y operativa en aplicaciones que provea a la organización una fuente fidedigna formal de consulta.	Se debe de crear documentación Técnica y Operativa sobre la operación proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., acorde a lo dispuesto por la Resolución Miscelánea Fiscal y Regulaciones Aplicables.	**Administrativo y Técnico**	
26	Bitácoras de Eventos de Seguridad en Aplicaciones	Implementar un mecanismo de control de los eventos de seguridad de la información en aplicaciones, que proporcione a la organización información sobre las posibles amenazas.	Se debe de implementar Bitácoras de eventos que registren todos los eventos de seguridad de la información, en aplicativos del proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	Resguardo de Bitácoras 1 Año
27	Protección contra Código Malicioso	Puntualizar controles de protección en contra amenazas informáticas, que puedan comprometer los activos de información.	Se debe de implementar mecanismos de identificación y protección de código malicioso, el cual debe de estar habilitado y actualizado.	**Administrativo y Técnico**	
IX.- Gestión Operativa y de Negocio					
28	Plan de Continuidad del Negocio (BCP).	Definir un Plan de continuidad de Negocio que pueda dar soporte, en caso de una interrupción a los Servicios críticos de la organización.	Se debe diseñar, documentar, implementar y actualizar un Plan de Continuidad de Negocio por sus siglas en inglés (BCP), el cual de soporte en caso de una recuperación a los activos critico dentro del proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos
28.1	Pruebas al Plan de Continuidad del Negocio (BCP).	Verificar la correcta implementación del Plan de Continuidad de negocio, con la intención de que la organización lleve un control de las mejoras necesarias detectadas en las pruebas.	Se debe de diseñar un Plan de pruebas del Plan de Continuidad de Negocio (BCP), el cual identifique oportunidades de mejora en la ejecución y puesta en operación del Plan en caso de una recuperación al proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos
29	Plan de Recuperación de Desastres (DRP).	Definir un Plan de Recuperación de Desastres, que pueda dar soporte en caso de un desastre a la organización.	Se debe diseñar, documentar, implementar y actualizar un Plan de Recuperación de Desastres por sus siglas en inglés (DRP), el cual de soporte en caso de un desastre a los activos critico dentro del proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos
29.1	Pruebas de Recuperación de Desastres (DRP).	Verificar la correcta implementación del Plan de Recuperación de Desastres, con la intención de que la organización lleve un control de las mejoras necesarias detectadas en las pruebas.	Se debe de diseñar un Plan de pruebas del Plan de Recuperación de Desastres (DRP), el cual identifique oportunidades de mejora en la ejecución y puesta en operación del Plan en caso de un desastre al proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos

X.- Seguridad de la Plataforma Tecnológica					
30	Bitácoras de Eventos de Seguridad.	Implementar un mecanismo de control de los eventos de seguridad de la información en los activos de información, que proporcione a la organización información sobre las posibles amenazas.	Se debe de habilitar registros de eventos de seguridad de la información (Bitácoras) a todos los activos de Información "críticos" asociados con el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	Resguardo de Bitácoras 1 Año
31	Línea base de seguridad.	Especificar los criterios en materia de seguridad de la información aplicables a los activos de Información.	Se debe diseñar e implementar una línea base de seguridad de la información, que cubra a todos y cada uno de los activos que intervienen en el proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., la cual debe de ser documentada, aprobada, revisada y actualizada.	**Administrativo y Técnico**	
32	Respaldos.	Establecer mecanismos de respaldo de información, periódicos que permitan a la organización.	Se deben implementar procedimientos formales de respaldo de la información, correspondientes al proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT., dicho respaldos deben de mantener la confidencialidad e integridad de la información.	**Administrativo y Técnico**	
33	Destrucción o Borrado.	Instaurar mecanismos de Borrado p Destrucción de información, que garantice la no recuperación de la mismas a través de procesos tecnológicos	Se deben implementar procedimientos formales de destrucción o borrado seguro de la Información almacenada en los activos de información del proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	En de uso de equipo, baja de los activos.
34	Criptografía en servicios expuestos.	Definir elementos criptográficos que provean un mecanismo de comunicación seguro, en los activos de Información, cuando se usan a través de redes públicas.	Se debe de Implementar mecanismos criptográficos, en los activos de información, que se encuentran expuestos en servicios públicos.	**Administrativo y Técnico**	
35	Control de Cambios.	Especificar medidas de control, con respecto a los cambios de los activos de información.	Se deben implementar procedimientos formales de Control de cambios a todos los Activos de información que soportan el proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.:	**Administrativo y Técnico**	
36	Actualizaciones.	Verificar que los Activos de Información, se encuentran actualizados con los últimos parches de seguridad.	Se deben implementar procedimientos formales, de aprovisionamiento de Parches de Seguridad de la Información que soportan el proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	
37	Prevención y Detección de Intrusos.	Implementar mecanismos de detección y prevención de accesos o conexiones no deseadas a activos de información, que proporcione información al respecto.	Se deben de implementar mecanismos de protección contra amenazas, en las fases de Detección y Prevención, aplicable al proceso de proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo y Técnico**	

38	Expiración de sesión por inactividad.	Definir parámetros de control, que prevean la ausencia de personal, evitando el acceso a activos de Información a personal no autorizado.	Se debe de implementar un mecanismo de expiración de sesión por inactividad, aplicable a todos los activos de información.	**Administrativo y Técnico**	El parámetro de expiración por inactividad no deberá de ser mayor a 5 Minutos.
39	Documentación.	Constituir un control documental, actualizado sobre toda la documentación tecnológica, acorde a los activos de Información, que provea a la organización una fuente fidedigna formal de consulta.	Se debe de generar todo la documentación técnica referente a los activos de información correspondiente al proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos
XI.- Cumplimiento Legal y Regulatorio					
40	Cumplimiento de Requisitos y Obligaciones.	Avalar el cumplimiento con lo dispuesto en la Normativa Vigente.	Se debe de asentar en un escrito, emitido por la Alta Dirección, el cabal cumplimiento a lo Dispuesto en la normativa vigente, Código Fiscal de la Federación, Resolución Miscelánea Fiscal, Ley del Impuesto sobre la renta, así como la correcta supervisión de lo dispuesto por Proveedores y Contratistas dentro del proceso de registro, control, almacenamiento y entrega de códigos de seguridad generados por el SAT.	**Administrativo**	1 vez al año / En cambios Tecnológicos