Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

ID	DOMINIO	CONTROL	PROPÓSITO DEL CONTROL	ATRIBUTOS DE CONTROL
1	Política de Seguridad	**Política General de Seguridad de la Información**	Asegurar que todo el personal de la organización y terceros, actúen y tomen decisiones en apego a los criterios y definiciones de la organización respecto a seguridad de información, además de asegurar el compromiso íntegro y participación activa de la alta dirección con la seguridad de la información.	**DISEÑO:** 1. Debe existir una *Política General de Seguridad de la Información* formalmente documentada. 2. Debe estar firmada de manera autógrafa o mediante e-firma, por la dirección general, representante o apoderado legal. 3. Debe incluir un apartado que describa el compromiso y participación activa de la dirección general con respecto a la seguridad de la información. 4. Debe incluir la definición de la seguridad de la información, es decir, como la organización concibe el concepto de la seguridad de la información. 5. Debe incluir referencias a la normatividad, legislación vigente y marcos de trabajo aplicables a la organización respecto a la seguridad de la información. 6. Debe incluir los objetivos de seguridad de la información de la organización. a. Deben estar alineados con la estrategia de la organización. b. Deben considerar la protección de datos personales e información de los contribuyentes. c. Deben considerar el cumplimiento normativo y regulatorio. 7. Debe incluir los roles y responsabilidades de la seguridad de la información y elementos tales como: a. Matriz de asignación de responsabilidades RACI u b. Organigrama con descripción de funciones o c. Perfiles de puestos con detalle de actividades. d. Medidas disciplinarias, sanciones y/o penalizaciones, en caso de incumplimientos a la política. 8. Debe incluir lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información tanto para personal interno como para personal ajeno a la organización. 9. Debe tener una sección para control de cambios y versiones de la política con fecha, participantes y control de cambios. 10. Debe definir una periodicidad de revisión de la política, al menos cada 12 meses. **IMPLEMENTACIÓN:** 1. La política debe estar comunicada y disponible a toda la organización y a terceros, proveedores, por medios físicos o electrónicos. 2. Debe existir evidencia de la revisión realizada a la política por lo menos cada 12 meses. 3. Debe existir evidencia de compromiso y participación activa de la dirección con la seguridad de la información.
2	Política de Seguridad	**Políticas específicas de Seguridad de la información**	Asegurar que todo el personal de la organización y terceros actúen y tomen decisiones en apego a los criterios y definiciones de la organización respecto a seguridad de información.	**DISEÑO:** Cada una de las políticas requeridas deberán cumplir por lo menos con los siguientes elementos: 1. Debe estar firmada de manera autógrafa o e-firma, por la dirección general, representante o apoderado legal. 2. Contar con un glosario de definiciones y/o conceptos que abarcan las políticas. 3. Contar con referencias a la normatividad, legislación vigente y marcos de trabajo aplicables a la organización, respecto al tema de la política. 4. Incluir roles y responsabilidades de la seguridad de la información mediante una matriz RACI, organigrama con descripción de funciones o perfiles de puestos con detalle de actividades. 5. Especificar medidas disciplinarias, sanciones y/o penalizaciones, en caso de incumplimientos a la política. 6. Incluir una sección de control de cambios y versiones de cada política con fecha, participantes y control de cambios. 7. Especificar una periodicidad de revisión, al menos cada 12 meses. 8. La política denominada *Política de Clasificación de la Información*, deberá cumplir por lo menos con los siguientes

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

				elementos: a. Definición de los rubros en los que será clasificada la información, con base en la criticidad y sensibilidad de la información para la organización. b. Directrices y/o Lineamientos de clasificación de información. Nota: Como mínimo se deberá considerar lo establecido en la LFPDPPP y el artículo 69 del CFF. 9. La política denominada *Política de escritorio limpio y equipo desatendido*, deberá cumplir por lo menos con los siguientes elementos: a. Lineamientos para asegurar que las áreas de trabajo se encuentren libres de documentos con información sensible, información de autenticación, medios de almacenamiento extraíbles. b. Lineamientos para mantener la pantalla despejada evitando colocar información sensible en la pantalla de inicio de la sesión del usuario (escritorio); lo anterior aplicable a personal interno y proveedores. c. Lineamientos para el equipo desatendido en cuanto al bloqueo del equipo de cómputo después de determinado tiempo. d. Indicar los mecanismos de verificación del cumplimiento de la política. e. Indicar las sanciones aplicables en caso de incumplimiento de la política. f. Debe ser aplicable tanto a personal interno y proveedores que labore en las instalaciones de la organización. 10. La política denominada *Política de gestión de incidentes de seguridad de la información*, deberá cumplir por lo menos con los siguientes elementos: a. Lineamientos para el manejo y reporte de incidentes, así como problemas de seguridad de la información en la organización. b. Lineamientos para el manejo y reporte de incidentes, así como problemas de seguridad de la información dirigido a proveedores. 11. La política denominada *Política de uso aceptable de activos y de la información*, deberá cumplir por lo menos con los siguientes elementos: a. Lineamientos para utilizar los activos relacionados con los servicios que proporciona. b. Listado de sistemas de información, software y activos tangibles contemplados en la presente política. 12. La política denominada *Política de control de accesos lógicos*, deberá cumplir por lo menos con los siguientes elementos: a. Listado de sistemas operativos y de información, redes y software; o activos tangibles y no tangibles, incluyendo los correspondientes a servicios en la nube, contemplados en la presente política. b. Lineamientos que establezcan las condiciones, requerimientos y autorizaciones para otorgar, modificar y eliminar accesos. c. Roles, responsabilidades y autoridades para otorgar, modificar y eliminar accesos. 13. La política denominada *Política de respaldos*, deberá cumplir por lo menos con los siguientes elementos: a. Listado de sistemas, activos y herramientas que deben ser sujetos a respaldo. b. Definición de tipos y frecuencias de respaldo realizados en la organización, incluyendo respaldos de proveedores. c. Lineamientos para la selección y autorización de medios de respaldo o repositorios en la nube donde se colocarán dichos respaldos.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

				d. Lineamientos para la ejecución periódica de pruebas de respaldos. e. Lineamientos de autorización para acceso a respaldos y supervisión. f. Lineamientos para la destrucción de respaldos. g. Determinación de periodo de almacenamiento o retención de respaldos. 14. La política denominada *Política de cifrado de información y gestión de llaves*, deberá cumplir por lo menos con los siguientes elementos: a. Listado sistemas de información, software y activos tangibles que contienen información de los contribuyentes, contemplados en la presente política. b. Descripción de algoritmos de cifrado utilizados por la organización. c. Condiciones para el uso de controles de cifrado. d. Lineamientos para la administración de llaves utilizadas en los controles de cifrado, entre otros lo relativo a la entrega, uso, resguardo y disposición. 15. La política denominada *Política de uso de contraseñas*, deberá cumplir por lo menos con los siguientes elementos: a. Listado de sistemas de información y software contemplado en la política. b. Lineamientos para definir la longitud y complejidad de contraseñas. c. Aspectos de uso de contraseñas para personal interno y proveedores. d. Lineamientos más robustos para contraseñas de cuentas privilegiadas y de acceso a servicios en la nube. e. Disposiciones para almacenar las contraseñas en los sistemas de la organización, de tal forma que no sean almacenadas en texto plano. 16. La política denominada *Política de trabajo remoto para empleados*, deberá cumplir por lo menos con los siguientes elementos: a. Condiciones para la autorización. b. Lineamiento sobre el aprovisionamiento. c. Período de autorización. d. Lineamientos para la cancelación de la autorización. e. Lineamientos sobre la revisión periódica de cuentas de accesos remoto. 17. La política denominada *Política de desarrollo seguro*, deberá cumplir por lo menos con los siguientes elementos: a. Lineamientos de seguridad para desarrollos internos y desarrollos requeridos a proveedores. b. Estándares de codificación segura utilizados. c. Lineamientos de aceptación y revisión de aspectos de seguridad en los desarrollos. d. Lineamientos para definir la propiedad intelectual de los desarrollos contratados con terceros. e. Lineamientos para establecer un entorno seguro para desarrollos internos. 18. La política denominada *Política de relación con proveedores*, deberá cumplir por lo menos con los siguientes elementos: a. Lineamientos para definir alcance y objetivo de los acuerdos con proveedores. b. Lineamientos para definir las condiciones de entrega de servicio de los proveedores. c. Lineamientos para autorizar el acceso a la información de contribuyentes a los proveedores. d. Controles de seguridad para los servicios.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

				e. Inclusión de cláusula de auditoría para contratación de servicios con proveedores. f. Lineamientos para realizar cambios en las condiciones de entrega de servicios. 19. La política denominada *Política para seguridad de los recursos humanos*, deberá cumplir por lo menos con los siguientes elementos: a. Lineamientos relacionados con el apego a las políticas de seguridad de la información, código de conducta, términos y condiciones de contratación. b. Obligaciones y responsabilidades generales de seguridad de la información, del personal interno y proveedores. c. Lineamientos de capacitación y concientización de personal en materia de seguridad de la información. 20. La política denominada *Política de seguridad física y ambiental*, deberá cumplir con los siguientes elementos: a. Identificación de las áreas físicas y ubicaciones geográficas donde residen activos críticos así como centro de procesamiento de datos principal y alterno. b. Lineamientos para establecer el perímetro de seguridad física de las distintas instalaciones. c. Lineamientos generales del acceso físico a instalaciones de la organización. d. Lineamientos que establezcan las condiciones, requerimientos y autorizaciones para otorgar, modificar y eliminar accesos. e. Lineamientos para la protección contra las amenazas externas o causadas por el medio ambiente. 21. La política denominada *Política de seguridad en las comunicaciones*, deberá cumplir con los siguientes elementos: a. Identificación de activos de red, contemplados en la presente política. b. Lineamientos y responsabilidades sobre la administración de los activos y servicios de red. c. Lineamientos de seguridad para los activos y servicios de red. 22. La política denominada *Política de seguridad de servicios de nube*, deberá cumplir por lo menos con los siguientes elementos: a. Identificación de activos y servicios en la nube. b. Lineamientos que establezcan las condiciones, requerimientos y restricciones de uso de los activos y servicios en la nube. c. Lineamientos de seguridad para los activos y servicios en la nube. **IMPLEMENTACIÓN:** 1. Las políticas deben estar comunicadas y disponibles a toda la organización y proveedores aplicables, por medios físicos y/o electrónicos. 2. Las políticas deben contar con evidencia de la revisión realizada por lo menos cada 12 meses.
3	Planeación	**Proceso de análisis de riesgos**	Asegurar que la organización tiene identificados todos los riesgos de seguridad de información y de continuidad operativa; que todos los riesgos cuentan con un nivel de riesgo	**DISEÑO:** 1. La *Metodología de Análisis de Riesgos* debe estar documentada. 2. Debe incluir firma autógrafa o e-firma de la dirección general, representante o apoderado legal. 3. Debe incluir la definición de riegos de la organización, es decir una descripción de cómo la organización concibe dicho concepto. 4. Debe incluir el marco de referencia utilizado para la gestión de riesgos. 5. Debe incluir roles y responsabilidades relacionados con la seguridad de la información mediante una matriz RACI, organigrama con descripción de funciones o perfiles de puestos con detalle de actividades.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

			adecuadamente fundamentado y que todos los riesgos se mantienen dentro de los niveles de tolerancia definidos por la organización.	6. Debe especificar el proceso para la gestión de riesgos, considerando los siguientes elementos: a. Nivel de riesgo aceptable. b. Proceso de valoración de riesgos, es decir identificación, análisis y evaluación de riesgos. c. Criterios para la determinación de impacto al negocio, la probabilidad de ocurrencia y nivel de riesgo. d. Proceso de tratamiento de riesgo, incluyendo actividades de definición y seguimiento de planes de mitigación de riesgos. 7. Debe incluir lineamientos para la ejecución periódica, al menos cada 12 meses, de la valoración de riesgos e identificar los cambios en el entorno que puedan incrementar el nivel de riesgo. **IMPLEMENTACIÓN:** 1. El alcance de la valoración de riesgos debe incluir a todos los activos de información, tanto locales como en la nube, que soportan las áreas de negocio afines a la autorización del SAT. 2. Debe existir un inventario de riesgos identificados por la organización donde se consideren los riesgos de seguridad de la información, tecnológicos, inducidos por terceros, normativos y legislativos, derivados de eventos climatológicos y sociales. 3. Los riesgos deben estar calificados con base en los criterios de probabilidad e impacto definidos en la metodología y dichos criterios deben estar definidos en la propia metodología. 4. Debe existir una priorización de acciones para tratamiento de riesgos con base en el nivel de riesgo aceptable, el cual también debe estar definido en la propia metodología. 5. Debe existir un plan de tratamiento de riesgos con las actividades, fechas y resultados esperados, así como evidencia de su seguimiento.
4	Gestión de incidentes en la seguridad de la información	**Procedimiento para la Gestión de Incidentes de Seguridad de la Información**	Asegurar que los incidentes de seguridad son gestionados de forma planeada, consistente y eficaz, con el objetivo de contener o reducir las consecuencias para la organización a un nivel aceptable.	**DISEÑO:**1. Se debe contar con un *Procedimiento de Gestión de Incidentes de Seguridad de la Información*.2. Debe incluir firmas de autorización.3. Debe incluir a los responsables del monitoreo de incidentes de seguridad en áreas y activos críticos.4. Debe incluir el proceso para la identificación, evaluación, clasificación, registro, atención, escalamiento, seguimiento y cierre de incidentes de seguridad de la información.5. Debe incluir una matriz de escalamiento.6. Debe incluir los tiempos de respuesta a incidentes de acuerdo con su urgencia y criticidad.7. Debe incluir el proceso de notificación de incidentes, incluyendo: a. Protocolo de notificación interna de incidentes. b. Protocolo de notificación en el que se describa cómo el proveedor de servicios en la nube y/o del centro de datos on premise, notificarán a la organización en caso de incidentes. c. Protocolo de contacto con autoridades competentes. d. Apartado en el que la organización declare que permitirá que las autoridades competentes realicen investigaciones de acuerdo a sus facultades.8. Debe incluir los protocolos de notificación de lo que se debe de comunicar, a quién se debe comunicar, cuando se debe llevar a cabo esa comunicación, a quién va dirigido y los medios de comunicación.**IMPLEMENTACIÓN:**1. Registros de incidentes en formato físico o electrónico, incluyendo el impacto del incidente.2. Documentación del diagnóstico y la solución detallada del incidente, con el objetivo de generar una base de conocimiento.3. Notificación realizada de manera interna y comunicación con terceros y proveedores.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

5	Gestión de incidentes en la seguridad de la información	**Procedimiento de Notificación al SAT**	Asegurar que los responsables del SAT son informados fidedigna y oportunamente sobre eventos voluntarios o involuntarios que afecten la operación de la organización o cambios en la configuración de la infraestructura.	**DISEÑO:** 1. Se debe contar con un *Procedimiento de Notificación al SAT*. 2. Debe especificar los datos de contacto del personal autorizado de la organización y del SAT para establecer la comunicación. 3. Debe especificar los medios de comunicación autorizados para realizar la notificación. 4. Debe especificar la documentación física y electrónica que debe adjuntarse a la notificación al SAT. 5. Debe contemplar protocolos de comunicación y registro de incidentes, cambios o eventos que afecten los procesos de la organización: a. Interrupciones en los procesos del negocio. b. Interrupciones en el servicio de entrega (específico para la factura electrónica y documentos digitales al SAT). c. Ventanas de mantenimiento. d. Cambios en la infraestructura tecnológica de la organización. e. Cambios en el software de la organización relacionado con los procesos afines a la autorización. **IMPLEMENTACIÓN:** 1. Registros de incidentes, cambios o eventos notificados al SAT. 2. Documentación del diagnóstico y la solución detallada del incidente, cambio o evento, con el objetivo de generar una base de conocimiento. 3. Notificación realizada al SAT por los medios señalados.
6	Organización de la seguridad de la información	**Definición de roles y responsabilidades de seguridad de la información**	Que el personal encargo de la seguridad de la información tenga claridad de sus funciones y responsabilidades para realizarlas de forma completa y adecuada. Que todo el personal tenga claridad de sus responsabilidades en materia de seguridad de la información.	**DISEÑO:** 1. Se deben presentar los roles encargados de la seguridad de la información con las funciones y responsabilidades correspondientes. 2. Los contratos del personal de la organización deben incluir las responsabilidades relacionadas con seguridad de información. 3. Los contratos con proveedores o personal tercerizado deben incluir las responsabilidades relacionadas con seguridad de información. 4. Los expedientes del personal deben incluir una carta responsiva que considere como mínimo el tipo de documento, área, fecha, nombre, puesto, descripción, texto que identifique a qué información accede, responsabilidades y obligaciones sobre el manejo de la información, marco de referencia normativo interno y externo, firma del empleado con fecha de aceptación y conformidad. 5. Los contratos con terceros deben especificar cómo la organización evita el conflicto de intereses de los diferentes puestos respecto a sus actividades, roles y responsabilidades. **IMPLEMENTACIÓN:** 1. Evidencia de la asignación formal de los roles encargados de la seguridad de la información en la organización. 2. Muestra física y digital de contratos y anexos donde se muestren las obligaciones y responsabilidades específicas de los empleados en materia de seguridad de la información. 3. Muestra física y digital de cartas responsivas firmadas por el empleado. 4. Muestra física y digital de la documentación donde se especifique cómo la persona moral evita el conflicto de intereses de los diferentes puestos.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

7	Cumplimiento	**Acuerdos de Confidencialidad y/o No Divulgación**	Disuadir cualquier acción u omisión que signifique la divulgación de información confidencial y contar con un instrumento legal que fortalezca cualquier proceso judicial que se emprenda ante una divulgación de información.	**DISEÑO:** 1. Deben existir acuerdos de confidencialidad y/o acuerdos de no divulgación suscritos con el SAT, así también con las personas físicas y morales involucradas en los procesos operativos afines con la autorización del SAT. 2. Los acuerdos deben contener claramente las responsabilidades de confidencialidad entre la organización y la persona física, así como la persona moral involucrada. 3. La responsabilidad del personal que firma debe estar vigente durante el desempeño de sus actividades. En caso de que deje de laborar en la organización, se debe considerar un periodo posterior tomando como base la LFPDPPP. 4. Los acuerdos de confidencialidad deben prever que las personas que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar la relación con la organización, de conformidad con la LFPDPPP. **IMPLEMENTACIÓN:** 1. Acuerdo de confidencialidad y/o acuerdos de no divulgación firmados por la organización con el SAT. 2. Todos los empleados y proveedores deben contar con acuerdos firmados de confidencialidad y/o no divulgación.
8	Organización de la seguridad de la información	**Contacto con Grupos Especializados en Seguridad de la Información**	Asegurar que el personal responsable de actividades relacionadas con seguridad de información se mantiene actualizado en el tema y establece relaciones con colegas que pudieran proporcionar orientación.	**DISEÑO:** 1. El personal de la organización deberá formar parte de grupos especializados en materia de seguridad informática y de la información. 2. Las asociaciones deben ser organismos reconocidos. **IMPLEMENTACIÓN:** 1. Deben existir constancias de participación en eventos, evidencia de participación en webinars o correos con boletines emitidos periódicamente por los grupos especializados en materia de seguridad informática y de la información, con una antigüedad no mayor a 6 meses, que coadyuven a los procesos en materia de seguridad informática y de la información.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

9	Seguridad ligada a los Recursos Humanos	**Procedimiento de selección de personal**	Asegurar que todo el personal que trabaje en la organización cuenta con las capacidades y competencias requeridas y no represente ninguna amenaza para la organización.	**DISEÑO:** 1. El *Procedimiento de selección de personal* deber estar formalmente documentado. 2. Debe incluir firmas de autorización. 3. Debe incluir un apartado que describa las pruebas que se realizarán al personal de acuerdo con el perfil a cubrir, tales como: a. Examen psicométrico. b. Pruebas de conocimiento. c. Entrevistas con personal especializado. 4. Debe incluir un apartado que describa la verificación y detección de antecedentes, así como posibles incidencias laborales que puedan representar un riesgo para los contribuyentes y a la organización, tales como: a. Verificación de referencias laborales. b. Incidencias o demandas laborales. c. Antecedentes penales por causas de robo o fraude. 5. El alcance de las pruebas y de la verificación de antecedentes debe estar relacionado con la sensibilidad y/o criticidad de la función. **IMPLEMENTACIÓN:** 1. Todos los empleados deben ser objeto de las pruebas y evaluaciones correspondientes durante el proceso de selección, particularmente importante en personal de TI y personal con acceso a información sensible. 2. Los expedientes del personal deben incluir evidencia de la verificación y detección de antecedentes, así como posibles incidencias laborales.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

10	Seguridad ligada a los Recursos Humanos	**Planes de Capacitación y concientización al personal en materia de Seguridad**	Asegurar que el personal cuenta con las capacidades, competencias y aptitudes para desarrollar sus actividades de forma adecuada y consciente de los riesgos de seguridad de la información que podría implicar.	**DISEÑO:** 1. Debe existir un plan anual de capacitación para el personal que participa en los productos y servicios afines a la autorización con el SAT. 2. El plan debe incluir los cursos y temas a ser impartidos para el personal relacionado con la operación referente a la autorización con el SAT. 3. El plan debe estar basado en análisis de detección de necesidades de capacitación y éstas necesidades a su vez, deben tomar en cuenta los perfiles de puesto de la organización. 4. El plan debe incluir al personal a capacitar y los cursos a los que asistirá. 5. El plan debe incluir las fechas en las que se impartirán las capacitaciones. 6. El plan debe incluir las certificaciones para empleados (en caso de aplicar). 7. Debe existir un programa anual de concientización que promueva una cultura y conciencia de seguridad de la información del personal, los cuales incluyan como mínimo: a. Descripción de actividades o campañas enfocadas al entendimiento de las políticas y las responsabilidades del empleado en la seguridad de la información. b. Fecha de ejecución de las actividades o campañas de concientización. c. Medios o herramientas para realizar la concientización. **IMPLEMENTACIÓN:** 1. Evidencia de capacitación provista al personal en los últimos 12 meses, la cual permita determinar los siguientes elementos: a. Fecha de realización de la capacitación. b. Personal que recibió la capacitación. c. Temas provistos en la capacitación, donde dichos temás deben incluir capacitación para el personal que tiene acceso a activos críticos de la operación referente a la autorización con el SAT. d. Las competencias del personal que imparte las sesiones relacionadas con la seguridad de la información. e. Las evaluaciones del personal capacitado. f. Las evaluaciones de los cursos impartidos, incluyendo los instructores participantes. 2. Evidencia de la ejecución de las actividades o campañas de concientización enfocadas a los siguientes temas: a. Entendimiento de la política de seguridad de la información. b. Participación del personal para la efectividad de la seguridad de la información y sus beneficios. c. Las implicaciones de no cumplir con los requerimientos de la seguridad de la información.
11	Relación con proveedores	**Contratos de prestación de**	Tener claridad sobre las responsabilidades y compromisos de terceros	**DISEÑO:** 1. Los servicios prestados a la organización por terceros o proveedores que accedan, procesen, almacenen, comuniquen o provean componentes de infraestructura de TI, deben contar con contratos que expongan los términos y condiciones

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

		servicios con terceros	que presten servicios a la organización y que acceda, procese, almacene, comunique o provea componentes de infraestructura de TI para la información de la Organización. Asegurar un entendimiento común de expectativas y contar con un instrumento legal que fortalezca cualquier proceso judicial que se emprenda ante un posible incumplimiento.	sobre los servicios proporcionados. 2. Los contratos deben incluir la descripción de responsabilidades u obligaciones del tercero o proveedor para el cumplimiento de requerimientos de seguridad de la información de acuerdo con su perfil y con las políticas de seguridad de la organización. 3. Los contratos deben incluir cláusulas que brinden derecho a la organización para auditar los procesos y controles del proveedor definidos en al acuerdo. 4. Los contratos deben incluir las obligaciones del proveedor a entregar de manera periódica un reporte independiente de la efectividad de los controles de seguridad de la información. 5. Los contratos deben incluir cláusulas o condiciones relevantes para la subcontratación de servicios. 6. Los contratos deben incluir los niveles de servicio comprometidos, SLA. 7. Los contratos deben incluir cláusulas de propiedad intelectual donde se especifique que la información generada, almacenada, transmitida y procesada por el tercero o proveedor, es propiedad de la organización en todo momento y que el tercero o proveedor no tiene acceso a dicha información. **IMPLEMENTACIÓN:** 1. Todos los terceros o proveedores que accedan, procesen, almacenen, comuniquen o provean componentes de infraestructura de TI, deben contar con contratos que expongan los términos y condiciones sobre los servicios proporcionados. 2. Todos los contratos deber respetar consistentemente los lineamientos definidos. 3. Todos los contratos deben estar vigentes. 4. Deben existir reportes de evaluación independiente sobre la efectividad de los controles de seguridad de la información con los que cuentan los terceros o proveedores que den servicios a la organización.
12	Seguridad ligada a los Recursos Humanos	**Procedimiento de terminación de la relación laboral**	Evitar que personal que se desvincula de la organización realice actos que afecten la seguridad de la información. Asegurar que el personal mantenga obligaciones de confidencialidad una vez concluida la relación laboral y en términos de la ley aplicable.	**DISEÑO:** 1. El *Procedimiento de terminación de la relación laboral*, debe encontrarse formalmente documentado. 2. Debe contener firmas autógrafas o e-firma de autorización. 3. Debe contener un protocolo de revisión de acuerdos de confidencialidad que mantengan la vigencia después de finalizada la relación laboral en términos de la ley aplicable. 4. Debe contener un protocolo de entrega de activos del personal dado de baja, con base en los procedimientos de devolución de activos. 5. Debe contener un protocolo de inhabilitación de accesos físicos y lógicos del personal dado de baja, con base en los procedimientos de gestión de accesos. **IMPLEMENTACIÓN:** 1. Todas las bajas de personal deben contar con evidencia de la aplicación de los protocolos definidos en el procedimiento. 2. Debe existir evidencia de la devolución de activos con base en los procedimientos establecidos. 3. Debe existir evidencia de la inhabilitación de accesos físicos y lógicos con base en los procedimientos establecidos. 4. Los contratos y los convenios de confidencialidad con los empleados desvinculados con la organización deberán conservarse durante un periodo suficiente después de la baja para proteger los intereses de la organización.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

13	Seguridad física y ambiental	**Escritorio limpio y equipo desatendido**	Eliminar la vulnerabilidad de que exista información o accesos a información, que puedan ser explotadas y divulgar información confidencial o inclusive alteración o destrucción de información.	**DISEÑO:** 1. Deben existir guías *o procedimientos* con el detalle para orientar al personal para el cumplimiento del escritorio limpio y equipo desatendido. 2. Los procedimientos deben ser consistentes con la política establecida. **IMPLEMENTACIÓN:** 1. Las áreas de trabajo deben encontrarse libres de documentos con información sensible, información de autenticación, medio de almacenamiento extraíbles. 2. La pantalla de inicio de sesión no debe contar con información sensible. 3. La política debe ser del conocimiento de todo el personal. 4. El equipo de estar configurado para entrar en suspensión o apagarse después de un determinado tiempo. 5. Deben realizase actividades de supervisión para verificar el cumplimiento de la política.
14	Gestión de activos	**Procedimiento de clasificación y etiquetado de la información**	Asegurar que la información de la organización se encuentre adecuadamente clasificada que permitan establecer pautas para su correcto manejo durante su ciclo de vida, y que aseguren los niveles de confidencialidad, integridad y disponibilidad para cada clasificación definida.	**DISEÑO:** 1. Se debe presentar un *Procedimiento de Clasificación y Etiquetado de la Información.* 2. El procedimiento debe incluir firmas autógrafas o e-firma de autorización. 3. El procedimiento debe incluir un protocolo de clasificación de información de acuerdo con su relevancia y sensibilidad, tomando en consideración lo establecido en la política definida para tal propósito. 4. El procedimiento debe incluir las responsabilidades sobre la clasificación y etiquetado de información física y digital, definidos en la matriz RACI, el organigrama con descripción de funciones o el listado de puestos y detalles de actividades. 5. El procedimiento debe incluir la descripción de actividades que indiquen cómo realizar el etiquetado de información física y lógica. 6. El procedimiento debe incluir las responsabilidades del etiquetado de la información física y digital, definidos en una matriz RACI, el organigrama con descripción de funciones o el listado de puestos y detalles de actividades. 7. El procedimiento debe incluir la definición de controles de seguridad de acuerdo con la clasificación y etiquetado de información. 8. El procedimiento debe especificar las ubicaciones físicas y lógicas para el almacenamiento de información física y electrónica. 9. Como mínimo se deberá considerar lo establecido en la LFPDPPP y el artículo 69 del CFF. **IMPLEMENTACIÓN:** 1. Toda la información aplicable deberá ser clasificada con forme al procedimiento definido. 2. La clasificación de la información debe ser documentada. 3. EL etiquetado de información, debe permitir la generación de evidencia de dicho etiquetado para efectos de auditoría y/o supervisión.
15	Gestión de activos	**Procedimiento de gestión de activos**	Asegurar que los activos generen el valor esperado, que se encuentran protegidos físicamente, que se mantienen disponibles y en condiciones funcionales y que las licencias de software son suficientes y	**DISEÑO:** 1. El *Procedimiento de la gestión de activos* debe encontrarse formalmente documentado. 2. Debe incluir firmas autógrafas o e-firma de autorización. 3. Debe especificar las responsabilidades de la gestión del ciclo de vida de los activos en cuanto a la adquisición, uso, mantenimiento, monitoreo y destrucción en una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades. 4. Debe especificar las condiciones para la instalación/ingreso de activos en el centro de datos y oficinas de la organización.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

			cumplen con los términos de licenciamiento del proveedor.	5. Debe especificar todas aquellas medidas de protección y seguridad de los activos que son trasladados fuera de las instalaciones de la organización. 6. Debe incluir las actividades de baja de equipos en las oficinas de la persona moral y el centro de datos. 7. Debe incluir actividades de gestión y actualización del inventario de activos. 8. Debe incluir actividades de mantenimiento preventivo de activos. 9. Debe incluir actividades de gestión de medios extraíbles donde se considere la autorización, administración de acuerdo con su clasificación, rehuso y eliminación segura, todo esto mediante procedimientos formales. 10. Debe incluir actividades de control y mantenimiento de licencias de software adquiridas. **IMPLEMENTACIÓN:** 1. El equipo debe recibir mantenimiento preventivo de acuerdo con el plan definido para tal efecto, debiendo existir un registro del trabajo realizado considerando un periodo mínimo de 12 meses. 2. Deben existir contratos de servicios de mantenimiento cuando los activos se encuentren bajo la gestión de un tercero. 3. Debe existir un registro de todas las licencias de software adquiridas, incluyendo software de carácter general, antivirus, bases de datos, herramientas de desarrollo. 4. La gestión de medios extraíbles debe realizarse de acuerdo con el procedimiento definido.
16	Gestión de activos	**Inventario de Activos (tangibles y no tangibles)**	Contar con información completa y actualizada sobre los activos de información que permita identificarlos, protegerlos y gestionarlos durante todo su ciclo de vida.	**DISEÑO:** 1. Debe existir un *Inventario de activos tangibles y no tangibles*, formal y documentado. a. Debe incluir un identificador único del activo. b. Debe incluir la dirección IP del activo. c. Debe incluir las características de marca, modelo, número de serie y versión. d. Debe incluir la ubicación del activo. e. Debe incluir al propietario del activo. f. Debe incluir al responsable o custodio del activo. **IMPLEMENTACIÓN:** 1. El inventario debe mantenerse actualizado. 2. El inventario debe contener todos los activos tangibles y no tangibles. 3. Todos los activos deben contener toda la información requerida. 4. El inventario debe manejarse como información confidencial.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

17	Gestión de activos	**Procedimiento de destrucción o borrado seguro de información**	Evitar que información confidencial contenida en medios de almacenamiento sea divulgada en forma indebida una vez terminado su ciclo de vida útil.	**DISEÑO:** 1. Debe existir un *procedimiento formalmente documentado para la destrucción y borrado seguro de información* de los contribuyentes o del SAT. 2. Debe incluir firmas autógrafas o e-firma de autorización. 3. Debe especificar las responsabilidades para la destrucción o borrado seguro de activos de información, mediante una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades. 4. Debe incluir un protocolo de solicitud de destrucción o borrado de información. 5. Debe incluir un protocolo de autorización para la destrucción o borrado seguro de información. 6. Debe especificar la documentación o formatos requeridos para llevar a cabo la destrucción o borrado de información. 7. En su caso, el proveedor de servicios en la nube deberá contar con procedimientos formales de borrado seguro de los medios cuando ya no son utilizados, dicha documentación deberá ser presentada en el anexo técnico que forma parte del contrato. **IMPLEMENTACIÓN:** 1. Todos los dispositivos que sean reasignados o dados de baja contarán con el tratamiento de destrucción o borrado de acuerdo con el presente procedimiento. 2. Todas las acciones de destrucción o borrado de información deberán generar evidencia del presente procedimiento.
18	Gestión de activos	**Procedimiento de devolución de activos**	Evitar que sea divulgada información confidencial contenida en activos o que a través de estos se pueda tener acceso a dicha información.	**DISEÑO:** 1. Debe existir un *procedimiento formalmente documentado para la devolución de activos*. 2. Debe incluir firmas autógrafas o e-firma de autorización. 3. Debe incluir las responsabilidades para la devolución de activos mediante una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades. 4. Debe incluir la descripción de activos tangibles y no tangibles a devolver, de acuerdo con el puesto. 5. Debe incluir las condiciones en las que se entregan los activos tangibles y no tangibles. 6. Debe incluir un protocolo de verificación de acceso a equipos de cómputo, equipos móviles, accesos a sistemas de información, acceso a herramientas, entre otros. 7. Debe incluir un procedimiento de sanitización de la información en los equipos. 8. Debe ser aplicable para el personal que deja de pertenecer a la organización y para el personal que cambia de funciones. **IMPLEMENTACIÓN:** 1. Todos los dispositivos que sean devueltos deben ser objeto del procedimiento especificado. 2. Todas las devoluciones de activos deberán generar evidencia de dicha acción.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

19	Organización de la seguridad de la información	**Procedimiento de gestión de equipos móviles**	Asegurar que el empleo de dispositivos móviles no genere amenazas o vulnerabilidades para la seguridad de información de los contribuyentes y se preserven los niveles de riesgo requeridos por la organización.	**DISEÑO:** 1. Debe existir un *procedimiento documentado para gestionar dispositivos móviles,* teléfono celular, tableta, entre otros, utilizados en el manejo de información de los contribuyentes por medio de correo electrónico, aplicativos, entre otros. 2. Debe contener firmas autógrafas o e-firma de autorización. 3. Debe contener roles y responsabilidades para el uso de equipos móviles en cuanto a la adquisición, autorización, configuración y uso, mediante una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades. 4. Debe contener formatos para la autorización para el uso de equipos móviles. 5. Debe especificar una línea base de configuración de equipos móviles. 6. Debe definir controles de protección de equipos móviles, tales como: a. Requerimientos de protección física. b. Restricción de instalación de software. c. Restricción de la conexión a servicios de información y aplicaciones Web. d. Controles de acceso. e. Técnicas criptográficas. f. Protección contra malware. g. Deshabilitación, borrado o bloqueo automático. **IMPLEMENTACIÓN:** 1. Todos los dispositivos móviles deben ser gestionados con base en el procedimiento especificado. 2. Todas las autorizaciones de dispositivos móviles deberán generar evidencia de dicha acción. 3. Debe existir evidencia de la implementación de los controles para la protección de equipos móviles.
20	Control de accesos	**Procedimiento de gestión de cuentas privilegiadas**	Asegurar que las contraseñan poseen y preservan las características requeridas. Asegurar que las contraseñas solo se entregan a los usuarios autorizados y Asegurar que las contraseñas preservan su confidencialidad.	**DISEÑO:** 1. Debe existir un *procedimiento documentado para de restricción, asignación y uso de cuentas privilegiadas*. 2. Debe incluir firmas autógrafas o e-firma de autorización. 3. Debe incluir un protocolo de autorización para la generación de cuentas privilegiadas. 4. Debe incluir un protocolo para la asignación de cuentas privilegiadas. 5. Debe incluir protocolos para restricción de actividades de cuentas privilegiadas. 6. Debe describir las condiciones de uso de cuentas privilegiadas. 7. Debe incluir un procedimiento de supervisión o monitoreo de la actividad de cuentas privilegiadas. **IMPLEMENTACIÓN:** 1. Todas las cuentas privilegiadas deben haber seguido el protocolo de autorización. 2. La revisión de actividades de cuentas privilegiadas debe realizarse de forma consistente y generar evidencia de la misma.
21	Control de accesos	**Control de accesos lógicos**	Asegurar que los usuarios autorizados tienen acceso a los sistemas y servicios predefinidos de acuerdo con los privilegios asignados y evitar el acceso de usuarios no autorizados.	**DISEÑO:** 1. Debe existir un *Procedimiento de control de accesos*. 2. Debe Incluir firmas autógrafas o e-firma de autorización. 3. Debe incluir un protocolo para solicitud y autorización de accesos a sistemas de información, redes, sistemas operativos, software, activos tangibles y no tangibles incluyendo los relacionados a los servicios en la nube. 4. Debe incluir un protocolo de inhabilitación de derechos de acceso a sistemas, redes, servicios de red y servicios en la nube, aplicado en la terminación laboral y ante cambios de actividades, roles y responsabilidades del personal interno y

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

				externo. 5. Debe incluir restricciones de acceso a la información con base en perfiles. 6. Para los accesos a sistemas de información y servicios de nube, debe incluir: a. Condiciones para realizar el bloqueo o inhabilitación de accesos a los sistemas por intentos fallidos de acceso. b. Condiciones para realizar el bloqueo o inhabilitación de accesos a cuentas que presentes periodos de 90 días de inactividad. c. Protocolo de revisión de los permisos y niveles de accesos de los usuarios por lo menos cada 6 meses, para determinar que son correspondientes a sus actividades, roles, responsabilidades y que siguen siendo vigentes. 7. Para accesos remotos debe incluir: a. Condiciones para otorgar accesos remotos a los sistemas de la organización bajo circunstancias de excepción y con un estricto proceso de autorizaciones y monitoreo. b. Requerimientos tecnológicos para accesos remotos a los sistemas de la organización. c. Aprovisionamiento para el acceso. 8. La administración de accesos para los ambientes de desarrollo, pruebas y producción debe ser independiente del presente proceso. **IMPLEMENTACIÓN:** 1. Debe existir un registro central de derechos de acceso asignados a usuarios para el acceso a sistemas de información, redes, sistemas operativos, software y activos. 2. Todas las cuentas deben contar con los formatos correspondientes para solicitar accesos debidamente llenados y firmados. 3. Debe existir un registro de inhabilitación de derechos de acceso. 4. Debe existir evidencia de la actualización de privilegios en cuentas como resultado de cambios de puesto, ascensos o terminación laboral. 5. Se debe realizar una revisión cada 6 meses para validar que los permisos y niveles de acceso de las cuentas de usuarios en los sistemas de información y servicios en la nube, corresponden a sus actividades, roles y responsabilidades. Esta revisión debe generar evidencia. 6. Todos los aplicativos que se encuentran involucrados en los procesos relacionados con los productos y servicios relativos a la autorización que tienen con el SAT, deben contar con mecanismos automáticos de control de acceso para usuarios internos y externos, los cuales deben generar pistas de auditoría. 7. Deben existir mecanismos de bloqueo o inhabilitación por intentos fallidos de acceso y por períodos extensos de inactividad a partir de 90 días.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

22	Control de accesos	**Procedimiento de gestión de contraseñas**	Asegurar que las contraseñan poseen y preservan las características requeridas. Asegurar que las contraseñas solo se entregan a los usuarios autorizados y asegurar que las contraseñas preservan su confidencialidad.	**DISEÑO:** 1. Debe existir un *Procedimiento de gestión de contraseñas* documentado formalmente. 2. Debe incluir firmas autógrafas o e-firma de autorización. 3. Debe incluir reglas para la creación de contraseñas de primer acceso o por defecto para usuarios regulares y con accesos privilegiados, considerando la longitud mínima, histórico, caracteres permitidos, etc. 4. Debe incluir un protocolo de entrega de información de autenticación por primera vez y ante solicitudes de cambio de información de autenticación para usuarios regulares y con accesos privilegiados. 5. Debe incluir reglas en los activos que requieran contraseña para que se realice el cambio obligatorio después de acceder por primera vez. 6. Debe incluir algoritmos de cifrado de contraseñas para su almacenamiento, por ejemplo: SHA-256, SHA-512, entre otros. 7. Debe incluir reglas en los activos para la composición de contraseñas, que excluyan palabras comunes, que no permitan que contenga datos del usuario, que omitan palabras del teclado como QWERTY o números consecutivos, que manejen una longitud mínima de 8 caracteres para usuarios regulares y contraseña mínimo de 12 caracteres para las cuentas con accesos privilegiados. **IMPLEMENTACIÓN:** 1. Todas las reglas deben encontrase implementadas en la organización: a. Reglas para la creación de contraseñas de primer acceso o por defecto. b. Reglas en los activos que requieran contraseña para que se realice el cambio obligatorio después de acceder por primera vez. c. Reglas en los activos para la composición de contraseñas mediante valores alfanuméricos y caracteres especiales. d. Reglas en los activos para el manejo de una longitud mínima de 8 caracteres para usuarios regulares y de 12 para las cuentas con accesos privilegiados. 2. Debe existir evidencia de la entrega de información de autenticación a través de medios seguros y acuses de recepción por parte del usuario. 3. Debe existir evidencia del cifrado de información utilizado para el almacenamiento de contraseñas.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

23	Adquisición, desarrollo y mantenimiento de sistemas	**Procedimientos de desarrollo seguro y acceso al código fuente**	Evitar que se realicen desarrollo de soluciones que no sigan los estándares y requerimientos de seguridad de la organización. Evitar que se realicen modificaciones no autorizados al código fuente de aplicaciones. Preservar la propiedad intelectual de la organización.	**DISEÑO:** 1. Debe existir un *Procedimiento de desarrollo seguro y acceso al código fuente.* 2. Debe incluir firmas autógrafas o e-firma de autorización del documento. 3. Debe incluir requerimientos específicos de seguridad para la fase de diseño, pruebas y liberación de cada desarrollo. 4. Debe incluir formatos para la aprobación de desarrollos internos o subcontratados. 5. Debe incluir un protocolo de ejecución de pruebas o revisiones previas a la liberación de desarrollos, para garantizar la ausencia de código malicioso, así como el cumplimiento con estándares de codificación segura establecidos en la política de desarrollo seguro. 6. Debe incluir protocolo para administrar y autorizar acceso al código fuente. 7. Debe incluir los formatos para la autorización de acceso al código fuente. 8. Debe especificar los controles de seguridad requeridos para la gestión del código fuente a continuación: a. Aplicación de algoritmos de integridad al código fuente SHA-256. b. Controles de acceso al código fuente. c. Control de versiones. d. Definir repositorios y librerías seguros. **IMPLEMENTACIÓN:** 1. Deben existir formatos de aprobación de los desarrollos internos o subcontratados. 2. Evidencia de las liberaciones de desarrollos o cambios donde han sido objeto de pruebas previas para garantizar la ausencia de código malicioso intencional o no intencional, así como el cumplimiento con estándares de codificación segura establecidos en la política de desarrollo seguro. 3. Se deben generar registros lógicos del personal autorizado que accede al código fuente. 4. El código fuente de las aplicaciones debe contar con controles de seguridad implementados que incluyan: a. Aplicación de algoritmos de integridad al código fuente SHA-256. b. Controles de acceso al código fuente. c. Control de versiones. d. Repositorios y librerías seguros.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

24	Seguridad física y ambiental	**Sistema CCTV (Circuito Cerrado de Televisión)**	Disuadir la intención de accesos físicos no autorizados o de daño a instalaciones. Contar con evidencia para requerimientos de investigación o para procesos judiciales.	**DISEÑO:** 1. La organización debe contar con un sistema de CCTV en las oficinas de operación y el centro de datos. 2. Las características técnicas de los equipos deben permitir al menos lo siguiente: a. Almacenamiento de historial de grabación de los últimos 30 días. b. Debe tener una resolución de imagen suficiente para el reconocimiento de individuos e investigación de eventos. c. Almacenamiento en ubicación física fuera de las instalaciones principales. d. Controles de acceso a los archivos de grabación. 3. El personal responsable de su operación debe haber sido capacitado en la operación del equipo. **IMPLEMENTACIÓN:** 1. Todo el equipo de CCTV debe encontrarse funcionando adecuadamente con base en las especificaciones técnicas requeridas. 2. El personal responsable debe ser capacitado anualmente, tanto sobre la operación del sistema CCTV como en temas relacionados con atención de emergencias. 3. En el caso del centro de datos contratado con un tercero debe existir un contrato y sus anexos o documentos que permitan identificar que se cuenta con este tipo de controles. 4. En caso de contar con infraestructura en la nube, deben existir contratos firmados con los proveedores en la nube o el anexo técnico correspondiente donde se especifique que cuenta con ese tipo de controles.
25	Seguridad física y ambiental	**Control de Accesos Físicos**	Evitar la posibilidad de daño físico a instalaciones, robo de equipo o dispositivos, espionaje industrial o actos de ingeniería social.	**DISEÑO:** 1. Debe existir un *Procedimiento de control de accesos físicos a oficinas de operación y centro de datos con los siguientes elementos:* a. Firma autógrafa o e-firma de autorización. b. Debe incluir el alcance de aplicación del procedimiento. c. Debe incluir los roles y responsabilidades para el control de accesos mediante una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades. d. Debe incluir los protocolos de autorización a solicitudes de acceso. e. Debe incluir los tiempos de respuesta a las solicitudes de acceso. f. Debe incluir un protocolo de inhabilitación de derechos de acceso de personal interno y externo. g. Debe incluir el registro de inhabilitación de derechos de acceso. h. Debe indicar los controles de acceso físico. **IMPLEMENTACIÓN:**

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

				1. Los controles de acceso físico a las oficinas de operación y centro de datos deben estar implementados y funcionando de acuerdo a lo descrito en el procedimiento, para impedir el acceso a personas que no cuenten con autorización, acceso a equipo de cómputo y medios de almacenamiento extraíbles sin autorización. 2. Debe existir un registro permanente del personal autorizado para acceder a las instalaciones. 3. Deben existir bitácoras de acceso a las oficinas de operación y en el centro de datos las cuales deberán estar bajo resguardo. 4. Deben existir perímetros de seguridad en las oficinas de operación y en el centro de datos, entre ellos paredes perimetrales, puertas de acceso controlado, cercas electrificadas o estructuras metálicas que impidan el acceso libre a las instalaciones, personal de seguridad y/o recepción. 5. En el caso del centro de datos contratado con un tercero debe existir un contrato con sus anexos y documentos formales que permitan identificar que se cuentan con este tipo de controles. 6. En caso de contar con infraestructura en la nube, la organización debe contar con contratos firmados con el o los proveedores en la nube o documentación formal que avale que cuenta con estos controles.
26	Seguridad física y ambiental	**Señalización**	Prevenir o disuadir accesos no autorizados a las áreas restringidas. Facilitar la evacuación del personal en caso de eventos de contingencia. Facilitar las acciones de las brigadas de emergencia y prestación de primeros auxilios.	**DISEÑO:** 1. La organización debe contar con señalización en las oficinas de operación y centro de datos que definan de forma clara lo siguiente: a. Áreas de acceso restringido. b. Rutas de evacuación. c. Ubicación de equipo de emergencia. **IMPLEMENTACIÓN:** 1. La organización debe preservar en buen estado y de forma visible la señalización correspondiente a las oficinas de operación y centro de datos, así mismo el equipo de emergencia debe contar con la vigencia para su funcionamiento adecuado. Nota 1: En el caso del centro de datos contratado con un tercero se puede presentar el contrato con sus anexos y documentos que permitan identificar que se cuentan con este tipo de controles. Nota 2: En caso de contar con infraestructura en la nube, la organización deberá presentar contratos firmados con los proveedores en la nube o documentación formal donde se especifique que cuenta con ese tipo de controles.
27	Seguridad física y ambiental	**Medidas de protección contra las amenazas externas o causadas por el medio ambiente**	Evitar daños a las instalaciones y al personal, así como evitar la pérdida de información y/o la interrupción de los servicios.	**DISEÑO:** 1. La organización debe tener identificadas medidas y controles contra incendios, inundaciones, terremotos y cualquier otro fenómeno meteorológico que ponga en riesgo la operación en las oficinas de operación y el centro de datos. 2. Estos controles deben estar relacionados con los riesgos identificados en el análisis de riesgos de la organización. **IMPLEMENTACIÓN:** 1. Todas las medidas y controles implementados contra incendios, inundaciones, terremotos y cualquier otro fenómeno meteorológico deben encontrarse en buen estado y funcionando adecuadamente. 2. Todos los contrales que por su naturaleza lo requieran, deben contar con mantenimiento preventivo como mínimo cada 12 meses. 3. En el caso del centro de datos contratado con un tercero debe existir un contrato con sus anexos y documentos formal que permitan identificar que se cuentan con este tipo de controles. 4. En caso de contar con infraestructura en la nube, la organización deberá contar con contratos firmados con el proveedor en la nube y documentación formal donde se especifique que cuenta con ese tipo de controles.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

28	Seguridad física y ambiental	**Aire acondicionado**	Evitar daños a los equipos o interrupciones en la operación debido a cambios en la temperatura y humedad.	**DISEÑO:** 1. La organización debe contar con un sistema de aire acondicionado en el centro de datos con las características y capacidades necesarias para brindar el servicio requerido. 2. La organización debe contar con planos que permitan identificar el sistema de aire acondicionado instalado en el centro de datos. **IMPLEMENTACIÓN:** 1. El equipo de aire acondicionado debe funcionar adecuada y consistente en el centro de datos. 2. El equipo de aire acondicionado debe recibir mantenimiento preventivo y verificación cada 12 meses. 3. En el caso del centro de datos contratado con un tercero debe existir un contrato con sus anexos y documentos formales que permitan identificar que se cuentan con este tipo de controles. 4. En caso de contar con infraestructura en la nube, la organización deberá contar con contratos firmados con el proveedor en la nube y documentación formal donde se especifique que cuenta con ese tipo de controles.
29	Seguridad física y ambiental	**Instalación eléctrica**	Evitar interrupciones en el servicio, daño a los equipos o incendios debido a fallas en la instalación eléctrica.	**DISEÑO** 1. La organización debe contar con planos de la instalación eléctrica de las oficinas de operación y centro de datos que describan los requerimientos eléctricos para equipos entre ellos plantas de luz, balanceadores de carga eléctrica. **IMPLEMENTACIÓN** 1. La organización debe realizar revisiones a la infraestructura eléctrica por lo menos cada 6 meses para garantizar un funcionamiento adecuado. 2. Los planos o memoria técnica deben mantenerse actualizados cada vez que se modifique la instalación eléctrica. 3. En el caso del centro de datos contratado con un tercero debe existir un contrato con sus anexos y documentos formales que permitan identificar que se cuentan con este tipo de controles. 4. En caso de contar con infraestructura en la nube, la organización debe contar con contratos firmados con el proveedor en la nube y documentación formal donde se especifique que cuenta con ese tipo de controles.
30	Seguridad física y ambiental	**Planes y contratos de mantenimiento**	Asegurar el buen funcionamiento de los equipos relacionados con las actividades del negocio.	**DISEÑO:** 1. La organización debe contar con un plan de mantenimiento anual para los activos de soporte a la operación relativa a la autorización con el SAT, que contenga fechas y periodicidad de los mantenimientos, los cuales deben abarcar por lo menos la plantas de luz, balanceadores de carga eléctrica, extintores, sistemas de supresión, sistemas de enfriamiento y aire acondicionado. **IMPLEMENTACIÓN:** 1. Todos los activos de soporte a la operación deben presentar servicios de mantenimiento al menos de forma anual. 2. El plan de mantenimiento debe mantenerse actualizado para asegurar que todos los equipos son incluidos reflejando la alta y baja de equipos. 3. En el caso del centro de datos contratado con un tercero se debe contar con el contrato y anexos así como documentos formales que permitan identificar que se cuentan con este tipo de controles. 4. En caso de contar con infraestructura en la nube, la organización deberá contar con contratos firmados con el proveedor en la nube y documentación formal donde se especifique que cuenta con ese tipo de controles.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

31	Seguridad física y ambiental	**Ubicación segura del centro de datos**	Reducir la probabilidad de que algún accidente interrumpa la operación.	**DISEÑO:** 1. Como parte de un análisis de riesgos, la organización debe contar con estudios topográficos, mapas satelitales y planos de la zona en que se encuentra el centro de datos para identificar posibles amenazas físicas. 2. Los documentos proporcionados deberán resaltar zonas de peligro entre ellos gasolineras, gaseras, minas, acometidas de cableado de electricidad y gas o cualquier otro elemento que represente un riesgo para el centro de datos. 3. En caso que el centro de datos sea de un tercero se debe presentar contratos y anexos, así como documentación formal que permitan identificar lo relativo al control. 4. En caso de contar con infraestructura en la nube, la organización deberá presentar contratos firmados con el proveedor en la nube, anexos y documentación formal donde se especifique que cuenta con lo relacionado al presente control. **IMPLEMENTACIÓN:** 1. La ubicación del centro de datos de la organización debe situarse al menos a 100 metros de distancia de las zonas de riesgo identificadas en su análisis de riesgos. 2. Si el centro de datos se tiene a través de un proveedor se debe contar con contratos vigentes, anexos y documentación formal que garanticen la existencia de estos controles. 3. En caso de contar con infraestructura en la nube, la organización deberá contar con contratos firmados vigentes con el proveedor en la nube, anexo técnico y documentación formal donde se especifique que cuenta con ese tipo de controles. Nota: Para las organizaciones donde el centro de datos se encuentre ubicado en alguna zona de riesgo, deberá implementar controles adicionales o reforzar los actuales, a fin de evitar la interrupción de los servicios y pérdida de información en la operación relativa a la autorización con el SAT.
32	Seguridad en la operación	**Procedimiento de gestión de cambios**	Evitar que se realicen cambios no autorizados que afecten la seguridad de información y la continuidad del servicio.	**DISEÑO:** 1. Debe presentar un *Procedimiento de control de cambios a los sistemas, aplicativos e infraestructura donde se* asegure que solo se llevan al cabo cambios autorizados: a. Debe incluir firma autógrafa o e-firma de autorización. b. Debe incluir la estimación y evaluación de impacto de cambios, incluyendo impactos a la seguridad de la información. c. Debe incluir un protocolo de autorización formal de los cambios. d. Debe requerir un plan de pruebas funcionales y operacionales. e. Debe incluir formatos de petición de cambios y/o control de cambios. f. Debe incluir un protocolo de liberación de cambios. g. Debe incluir un protocolo de revisiones post-implementación para verificar que los requisitos del cambio, los beneficios esperados y las expectativas de las partes interesadas se han cumplido así como la mitigación de riesgos de seguridad clave. h. Debe incluir un protocolo de retorno de cambios en caso de falla. i. Debe incluir un registro del control de versiones para desarrollos. **IMPLEMENTACIÓN:** 1. Todos los cambios deben seguir el procedimiento establecido e incluir la documentación que soporte la autorización. 2. Se debe incluir evidencia de los resultados de las pruebas funcionales y operacionales realizadas a todos los cambios. 4. Se deben realizar revisiones post - implementación a los cambios en operación. 5. En caso de excepciones al proceso, éstas deben ser autorizadas por el personal facultado para ello.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

33	Seguridad en la operación	**Estudio de Capacidad Tecnológica y Operativa**	Asegurar que la organización cuenta con la capacidad tecnológica y operativa suficiente para proporcionar los servicios requeridos por los contribuyentes ahora y en el futuro.	**DISEÑO:** 1. Se debe presentar un *Estudio de capacidad tecnológica y operativa:* a. Debe incluir firma autógrafa o e-firma de autorización. b. Debe incluir una evaluación de la capacidad tecnológica y operativa actual y prevista a 12 meses, que contenga: * Para la capacidad tecnológica: i) Capacidad de almacenamiento de información. ii) Capacidad de procesamiento de información. iii) Capacidad de conexión a internet. iv) Características tecnológicas de la infraestructura que la organización requiere para brindar el servicio a los contribuyentes. * Para la capacidad operativa: i) Volumen de operación de acuerdo a su proyección de negocio. ii) Cantidad de personal requerido para la operación y la descripción de su perfil. **IMPLEMENTACIÓN:** 1. El estudio de capacidad se debe actualizar cada 12 meses. 2. La arquitectura tecnológica vigente deben corresponder a las especificaciones del estudio de capacidad. 3. La organización debe contar con mecanismos de monitoreo del rendimiento de la Infraestructura o cualquier otro mecanismo que permita a la organización conocer el nivel de desempeño de dicha infraestructura y actuar de manera preventiva en caso de requerir cambios o aumento de capacidades.
34	Seguridad en la operación	**Solución de protección contra código malicioso**	Asegurar que la información, aplicaciones y la capacidad de procesamiento no sean afectados por código malicioso.	**DISEÑO:** 1. Conforme a la metodología que sigue la organización para la adquisición tecnológica y el desarrollo de soluciones de seguridad tecnológica, se deben incorporar todas aquellas soluciones a los activos de la infraestructura que servirá en la operación relativa a la autorización con el SAT. **IMPLEMENTACIÓN:** 1. Se debe contar con evidencia vigente de la solución para la detección, prevención y recuperación contra código malicioso, implementada a todos los activos tecnológicos que dan soporte a dicha operación con las últimas actualizaciones de manera automática.
35	Seguridad en la operación	**Separación de ambientes de desarrollo, pruebas y producción.**	Evitar que se realicen cambios no autorizados a los sistemas o cambios o consultas no autorizados a la información en ambientes productivos, ya sean voluntarios o accidentales.	**DISEÑO:** 1. La organización debe contar con documentación de la arquitectura tecnológica en donde se especifique la separación de los ambientes de desarrollo, prueba y producción, incluyendo diagramas de interconexión de los sistemas, diagramas de infraestructura físico y/o diagramas de infraestructura lógica donde se identifique la existencia y separación de los ambientes mencionados. 2. Dichos diagramas deberán contar con los activos tangibles y no tangibles relacionados en el inventario, que sirven de base a la operación relativa a la autorización del SAT. **IMPLEMENTACIÓN:** 1. Los ambientes de desarrollo, pruebas y producción se deben presentar separados física o lógicamente, actualizados a lo dispuesto en el inventario de activos. 2. La organización debe asegurar que el ambiente de pruebas tiene las mismas características del ambiente productivo para asegurar que las pruebas realizadas generan resultados fidedignos.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

36	Seguridad en la operación	**Documentación técnica de aplicativos**	Asegurar que la atención a incidentes y cambios relativos a las aplicaciones se realicen en los tiempos requeridos minimizando el impacto en posibles riesgos de seguridad con la final de asegurar que la arquitectura de la solución facilite y contribuya en la identificación de vulnerabilidades.	**DISEÑO:** 1. Se debe presentar documentación técnica de los aplicativos relacionados con la operación y gestión de los productos y servicios relativos a la autorización del SAT, con los elementos siguientes: a. Debe incluir diagramas de flujos de datos. b. Debe incluir un modelo y un diccionario de datos. c. Debe incluir un diagrama que muestre la arquitectura de los aplicativos. **IMPLEMENTACIÓN:** 1. La organización debe presentar documentación técnica actualizada de los aplicativos relacionados con la operación de los productos y servicios relativos a la autorización del SAT, y reflejan todos los cambios realizados a los aplicativos.
37	Seguridad en la operación	**Aislamiento de información**	Evitar que la información de los procesos críticos sea modificada, destruida o divulgada de forma indebida mediante accesos a través de otras aplicaciones o servicios de la organización.	**DISEÑO:** 1. La documentación de diseño de la arquitectura tecnológica debe especificar la separación física y lógica de la información de los procesos relacionados con los productos y servicios relativos a la autorización del SAT, de otros procesos de negocio de la misma organización. **IMPLEMENTACIÓN:** 1. Se debe presentar evidencia de la configuración vigente de la infraestructura de los procesos relacionados a los productos y servicios relativos a la autorización del SAT, donde se observe la separación de otros procesos de negocio de la misma organización. 2. Se debe presentar evidencia del uso exclusivo de recursos y activos para los procesos críticos, de forma independientemente a procesos de negocio adicionales existentes en la organización.
38	Seguridad en la operación	**Sincronización de relojes**	Contar con una referencia de fecha y horario que garantice la precisión de los registros de auditoría y que permita realizar un monitoreo confiable de los sistemas relacionados a las actividades del negocio.	**DISEÑO:** 1. El diseño de arquitectura tecnológica de la organización debe considerar la sincronización de los sistemas e infraestructura que soporta los procesos relacionados con los productos y servicios relativos a la autorización del SAT, mediante un servidor de NTP, Network Time Protocol, sincronizado con GPS, Global Positioning System. 2. La organización debe contar con documentación de pruebas funcionales realizados al servidor de NTP sincronizado con GPS. **IMPLEMENTACIÓN:** 1. Los sistemas e infraestructura que soporta los procesos relacionados con los productos y servicios autorizados por el SAT, mantienen una sincronización usando un servidor de NTP (Network Time Protocol) sincronizado con GPS (Global Positioning System). 2. En caso de contar con infraestructura en la nube, la organización deberá contar con evidencia de los mecanismos que utiliza para sincronizar los relojes locales con el reloj de los servicios en la nube que utilice.
39	Seguridad en la operación	**Procedimiento de gestión de vulnerabilidades técnicas**	Asegurar que se tienen identificadas todas las vulnerabilidades relacionadas con seguridad	**DISEÑO:** 1. Se debe presentar un *Procedimiento de gestión de vulnerabilidades técnicas* que describa la manera en que la organización gestiona las vulnerabilidades técnicas de los activos relacionados con las sistemas, equipos de empleados y equipos de red que incluya:

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

			de información y que dichas vulnerabilidades son eliminadas o suficientemente controladas.	a. Firma autógrafa o e-firma de autorización. b. Calendarización de análisis de vulnerabilidades y pruebas de penetración. c. Protocolo de análisis de vulnerabilidades y pruebas de penetración. d. Lineamientos para el diseño de planes de remediación. e. Protocolo de autorización del uso de herramientas para el análisis de vulnerabilidades, pruebas de penetración, monitoreo de actividades y cualquier otra herramienta que pueda ser configuradas para omitir los controles de seguridad de los sistemas. **IMPLEMENTACIÓN:** 1. La organización debe realizar un análisis de vulnerabilidades y pruebas de penetración a la infraestructura que soporta los procesos relacionados con los productos y servicios relativos a la autorización del SAT cada 12 meses. 2. Debe existir un reporte de los hallazgos identificados, explicando con claridad los hallazgos, sus consecuencias potenciales y su nivel de prioridad. 3. Debe existir un plan de remediación de los hallazgos detectados en dichas pruebas de seguridad, el cual debe contener fechas, responsables y actividades de remediación. 4. Debe existir evidencia de la remediación de los hallazgos detectados conforme al plan establecido con las fechas de ejecución y los resultados de las actividades realizadas. 5. Debe existir una lista actualizada de herramientas autorizadas para el análisis de vulnerabilidades y pruebas de penetración.
40	Seguridad en la operación	**Control de Actualizaciones**	Asegurar el buen desempeño de los equipos. Asegurar la compatibilidad operativa y viabilidad del soporte técnico por parte de los proveedores. Realizar oportunamente la corrección de vulnerabilidades seguridad que puedan afectar a la información.	**DISEÑO:** 1. Se debe presentar un *Procedimiento para el control de actualizaciones que incluya lo siguiente:* a. Firma autógrafa o e-firma de autorización. b. Roles y responsabilidades para evaluar e implementar actualizaciones definidos en una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades. c. Protocolo para la selección de actualizaciones. d. Protocolo de evaluación de funcionalidad de los sistemas con actualizaciones en ambiente de pruebas y documentación de resultados. e. Protocolo de liberación de actualizaciones. **IMPLEMENTACIÓN:** 1. Todas las actualizaciones deben seguir el procedimiento definido y estar documentadas. 2. Todos los activos deben contar con las últimas actualizaciones de seguridad y actualización de los programas de acuerdo con su versión. Nota: Se debe presentar evidencia vigente de dichas actualizaciones
41	Seguridad en la operación	**Bitácoras**	Contar con registros de los eventos relevantes de los activos relacionados a la operación de los productos	**DISEÑO:** 1. Se debe presentar un *Procedimiento de acceso a bitácoras que incluya los siguientes elementos:* a. Firma autógrafa o e-firma de autorización. b. Roles y responsabilidades para la autorización de acceso a las bitácoras definidos en una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades o relación de custodios para acceder a dichas

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

			y servicios relativos a la autorización del SAT.	bitácoras. c. Protocolo de autorización de acceso. **IMPLEMENTACIÓN:** 1. Deben existir bitácoras o registros de los activos relacionados con la infraestructura que soporta la operación de los productos y servicios relativos a la autorización del SAT, de los sistemas, aplicaciones, bases de datos, sistemas operativos, equipos de red, incluyendo ambientes virtualizados y cualquier otro activo en la nube. 2. Dichas bitácoras o registros deben ser resguardadas, durante 6 meses como mínimo, en lugares seguros o como respaldos fuera de sitio o algún otro esquema de resguardo mediante el cual sólo el personal autorizado pueda tener acceso. 3. Las bitácoras de los sistemas, deberán contener los siguientes atributos: i. Fecha y hora ii. Usuario que realiza la actividad. iii. IP origen. iv. Folio o identificador. v. Detalle de la actividad para los siguientes registros: - Registro de intentos de acceso fallidos. - Registro de accesos exitosos. - Registro de cierre de sesión por inactividad y por parte del usuario. - Registro de errores y/o excepciones. - Registro de actividad de los usuarios en el sistema.
42	Seguridad en la operación	**Monitoreo de Eventos**	Identificar cualquier evento de seguridad de información dentro de los parámetros de tiempo predefinidos, alertar oportunamente a los responsables y/o activar medidas predefinidas.	**DISEÑO:** 1. Se debe presentar un *Procedimiento de monitoreo de eventos con los siguientes elementos:* 2. Firma autógrafa o e-firma de autorización. 3. Listado de eventos de seguridad a monitorear, considerando como mínimo lo siguiente: a. Identificación de eventos de alto impacto. b. Uso de cuentas privilegiadas. c. Acceso a información con clasificación alta de confidencialidad. d. Comportamiento anormal de los equipos. 4. Debe especificar mecanismos físicos o lógicos para realizar el monitoreo. 5. Roles y responsabilidades del monitoreo de eventos de seguridad definidos en una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades. **IMPLEMENTACIÓN:**

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

				1. Los monitoreos de eventos se realizan conforme a lo definido en el procedimiento. 2. Se deben presentar evidencia de los monitoreos especiales para eventos de seguridad de alto impacto. 3. Se debe generar evidencia de las bitácoras o registros, físicos o digitales, de los eventos de seguridad que son monitoreados, resguardados durante 6 meses en lugares seguros fuera de sitio o en algún otro esquema de resguardo mediante el cual sólo el personal autorizado pueda tener acceso. 4. En caso de contar con servicios en la nube, el proveedor del servicio en la nube debe proporcionar a la organización la documentación de las capacidades de monitoreo de eventos del servicio de nube contratado.
43	Seguridad en la operación	**Línea Base de Seguridad**	Definir la configuración mínima de seguridad que debe ser observada en la organización. Orientar al personal en la implementación de controles de seguridad para asegurar el cumplimiento del objetivo de control.	**DISEÑO:** 1. Se debe presentar una *Línea base de seguridad* definida para ser aplicada a los activos tecnológicos relacionados con los productos y servicios relativos a la autorización del SAT que incluya: a. Firma autógrafa o e-firma de autorización. b. Debe incluir las siguientes configuraciones para *servidores productivos*: i. Especificaciones de configuración de contraseña para el acceso a BIOS. ii. Especificaciones de inhabilitación de unidades de CD, DVD, disco duro externo, memorias Flash USB o cualquier otro medio de almacenamiento removible. iii. Especificaciones de particionado de instalación exclusiva del sistema operativo utilizado por la organización. iv. Especificaciones de revisión de configuración de puertos, servicios y usuarios. v. Especificaciones de inhabilitación de puertos, servicios y usuarios no requeridos para los productos y servicios autorizados por el SAT. vi. Actividades de revisión de recomendación de seguridad del fabricante, análisis e implementación de acuerdo con las políticas de la organización y requerimientos de la infraestructura. vii. Restricciones para la instalación de software. c. Debe incluir las siguientes configuraciones para *aplicativos*: i. Implementación de autenticación de los usuarios internos o clientes. ii. Implementación de mecanismo de no repudio de transacciones.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

				iii. Protección contra inyección de código. iv. Inicio de sesión seguro para usuarios internos y externos. v. Validación de datos de entrada/salida para evitar errores en el procesamiento de la información. vi. Manejo de errores dentro del aplicativo. vii. Terminación de sesiones por inactividad después de 10 minutos. viii. Medidas que contrarrestan ataques asociados al control de acceso. ix. Implementación de certificados para el cifrado de la información tanto para su intercambio como para el transporte, TLS. d. Debe incluir las siguientes configuraciones para *equipos de empleados*: i. Protección del BIOS. ii. Limitación de derechos de acceso para modificación del sistema operativo. iii. Configuración de bloqueo automático por tiempo de inactividad. iv. Restricción de instalación de programas. v. Inhabilitación de puertos físicos utilizados en transferencia de información o almacenamiento salvo autorización formal. vi . Configuraciones de seguridad del fabricante las cuales no deben derivar en incumplimiento de políticas de la organización. vii. Inhabilitación de usuarios por defecto del sistema operativo. e. Debe incluir las siguientes configuraciones para *equipos de red*:
				i. Configuración de registros de actividades. ii. Configuración de gestión de tráfico de paquetes. iii. Controles de seguridad en redes expuestas e internas en las oficinas de la operación y centro de datos. iv. Segregación de redes. f. Debe incluir las siguientes configuraciones para *máquinas virtuales* relacionadas con los servicios de *nube*: i. Inhabilitación de puertos, protocolos y servicios innecesarios en la operación. ii. Configuración de registros de actividades. iii. Habilitación de software antimalware. iv. Configuraciones de seguridad del fabricante para el endurecimiento, *hardening*, de las máquinas virtuales. **IMPLEMENTACIÓN:** 1. Todos activos tecnológicos relacionados con los procesos de negocio de los productos y servicios autorizados por el SAT deberán apegarse a las especificaciones de la línea base de seguridad ya mencionada, presentando evidencia vigente de su implementación.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

44	Cifrado	**Controles de Cifrado**	Evitar que se presente divulgación de información y de datos personales de los contribuyentes, mediante el cifrado tanto en su almacenamiento, tránsito y medios que los contengan.	**DISEÑO:** 1. Se debe presentar un *Procedimiento de cifrado de información y gestión de llaves con los elementos siguientes*: a. Firma autógrafa o e-firma de autorización. b. Roles y responsabilidades para el cifrado de la información definidos en una matriz RACI, u organigrama con descripción de funciones o listado de puestos y detalles de actividades. c. Definición de algoritmos de cifrado utilizados. d. Protocolo de implementación de algoritmos de cifrados. e. Protocolo de administración de llaves utilizadas en los controles de cifrado para la generación, uso, resguardo, disposición, incluyendo métodos para tratar con la protección de llaves criptográficas y la recuperación de información cifrada en el caso de pérdida, compromiso o daño de dichas llaves. f. Protocolo de resguardo de certificados. g. Dispositivos involucrados en el registro, transmisión, procesamiento y almacenamiento de información de los contribuyentes. **IMPLEMENTACIÓN:** 1. Los algoritmos de cifrado de información confidencial y de datos personales de los contribuyentes deben estar implementados y funcionar correcta y consistentemente. 2. Debe realizarse un monitoreo del cifrado de la información y su correcto funcionamiento. 3. En caso de detectar desviaciones se debe generar un reporte. 4. Debe existir un registro del personal que puede acceder a las llaves criptográficas.
45	Cifrado	**Controles para los servicios expuestos**	Proteger la información de los contribuyentes contra actividad fraudulenta, revelación y modificación no autorizada.	**DISEÑO:** 1. El diseño de arquitectura tecnológica de la organización deberá Incluir *mecanismos de control para servicios expuestos* incluyendo controles de seguridad contra fraudes y filtración de información, así como controles para evitar la transmisión incompleta de transacciones, alteración de mensajes, revelación de información. 2. La empresa debe contar con documentación de las pruebas realizadas a estos componentes para verificar su correcto funcionamiento. 3. Cuando resulte aplicable, estos controles deberán estar relacionados con los procedimientos manuales que sean necesarios. **IMPLEMENTACIÓN:** 1. Los servicios que se encuentren expuestos para el consumo por parte de usuarios y clientes, deberán contar con mecanismos de criptografía que funcionen correcta y consistentemente. 2. Se deberá de utilizar un algoritmo de cifrado considerando lo establecido en el procedimiento de cifrado de información y gestión de llaves. 3. Se deberá presentar evidencia vigente relativa a dichos controles para los servicios expuestos.
46	Seguridad en las telecomunicaciones	**Mecanismos para la seguridad de las redes**	Asegurar que la información y los servicios de la red están protegidos contra ciberataques o accesos no autorizados. Asegurar que los niveles de servicio de red son	**DISEÑO:** 1. Se debe presentar un *Procedimiento de gestión de la seguridad en las redes* que describa los elementos siguientes: a. Firma autógrafa o e-firma de autorización. b. Roles y responsabilidades para la gestión de la seguridad de las redes, administración de equipos de red, accesos a servicios de red, monitoreo de redes, definidos en una matriz RACI, organigrama con descripción de funciones o listado de puestos y detalles de actividades. c. Controles de autenticación, encripción y niveles de acceso implementados en redes cableadas e inalámbricas así

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

			cumplidos. Asegurar que los proveedores proporcionan los servicios de red acordados de forma contractual. Las redes deben estar segmentadas para proteger el flujo de información y evitar la posibilidad de que usuarios tengan acceso a información o recursos para los cuales no cuentan con privilegios.	como la protección de los sistemas y aplicativos. d. Definir los niveles de servicio con proveedores externos que brindan los servicios de red para la organización. e. Definición de los eventos de red a ser monitoreados. f. Diagramas de interconexión de los activos que soportan los procesos de negocio y procesos en la nube, que permitan identificar la segmentación de redes. Dichos diagramas deberán contar con los elementos siguientes: - Identificador del activo. - Dirección IP del activo. **IMPLEMENTACIÓN:** 1. Los controles de autenticación, encripción y niveles de acceso implementados en redes cableadas e inalámbrica deben funcionar y ser efectivos en su propósito. 2. Los dispositivos de seguridad perimetral que apliquen listas de control de accesos deben funcionar y ser efectivos en su propósito. 3. Los equipos para la prevención y detección de intrusos, así como la evidencia de la configuración de dichos equipos deben estar en operación y ser efectivos en su propósito. 4. Se debe presentar evidencia vigente de los mecanismos de seguridad para las redes que tienen parte en el proceso de los productos y servicios relativos a la autorización del SAT.
47	Seguridad en las telecomunicaciones	**Medidas de protección en la transferencia de información**	Asegurar que la transferencia de información está protegida contra intercepción, copia no autorizada, modificación, borrado, pérdida, transmisión de código malicioso.	**DISEÑO:** 1. La organización debe contar con una descripción de *controles para la protección de transferencia de información* contra intercepción, copia no autorizada, modificación, borrado, pérdida y transmisión de código malicioso. 2. Los controles deben incluir la seguridad para la información involucrada en mensajería electrónica. 3. La organización debe contar con documentación que compruebe la efectividad de los controles. **IMPLEMENTACIÓN:** 1. La organización debe comprobar que cuenta con controles implementados y en operación para la protección de transferencia de información contra intercepción, copia no autorizada, modificación, borrado, pérdida, transmisión de código malicioso, incluyendo controles de seguridad para la información involucrada en mensajería electrónica. 2. La organización deberá contar con acuerdos firmados de transferencia de información con terceros involucrados en el procesamiento de información relacionada con los productos y servicios autorizados por el SAT, dichos acuerdos deberán cubrir la transferencia segura de información de negocio entre la organización y los terceros.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

48	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**Plan de Continuidad del Negocio (BCP)**	Asegurar que la organización actuará de forma predefinida y coordinada en caso de un evento disruptivo para mantener su operación y recuperarse dentro de los tiempos predefinidos y con afectaciones dentro de niveles aceptables. Asegurar que los recursos operativos que soportan los procesos definidos como críticos, sean recuperados ante algún evento disruptivo dentro de los tiempos predefinidos y dentro de los niveles aceptables para la organización.	**DISEÑO:** 1. Debe existir un *Plan de Continuidad del Negocio (BCP)* debidamente documentado: 2. Debe incluir firma autógrafa o e-firma de autorización. 3. Debe incluir los objetivos del BCP. 4. Debe incluir el Análisis de Impacto al Negocio con la identificación de los procesos críticos a recuperar en caso de una contingencia, que incluyan por lo menos los procesos que soportan la entrega de productos y servicios autorizados por el SAT. 5. Debe especificar el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO) de los procesos críticos identificados. 6. Debe especificar los requerimientos de recuperación, tales como activos, recursos humanos, materiales e información que dan soporte a los procesos críticos. 7. Debe definir escenarios de interrupción de los procesos que contempla el BCP, fenómenos sociales, climatológicos, entorno tecnológico de la organización, indisponibilidad de la infraestructura en la nube o cualquier otro supuesto que afecte la continuidad de la prestación del servicio. 8. Debe incluir roles y responsabilidades para la activación, ejecución, comunicación, gestión, revisión y documentación del plan, definidos en una matriz de asignación de responsabilidades u organigrama con descripción de funciones o listado de puestos y detalles de actividades. 9. Debe incluir protocolos de activación, ejecución y finalización del plan. 10. Debe incluir un *plan de pruebas del BCP* con los siguientes elementos: a. Periodicidad de realización de pruebas BCP, por lo menos una vez al año. b. Alcance de las pruebas que contemple: i. Procesos a probar. ii. Áreas y personal participante, incluyendo proveedores involucrados. iii. Escenarios a probar. c. Tipo de prueba del BCP a desarrollar. 11. Debe haberse capacitado todo el personal responsable en los planes de recuperación. **IMPLEMENTACIÓN:** 1. El BCP debe mantenerse actualizado para reflejar todos los cambios, incluyendo: a. Cambios en la organización. b. Cambios en los procesos. c. Cambios en la tecnología. d. Cambios en la normativodad. 2. El BCP debe haberse probado en los últimos 12 meses, debiéndose generar un reporte de los resultados de la prueba que contenga al menos: a. Personal que participó en la prueba, incluyendo proveedores. b. Incidentes prensentados. c. Eficiencia de la comunicación durante la pruebas funcionales y pruebas totales. d. Medición del tiempo objetivo de recuperación (RTO) de los procesos para pruebas funcionales y pruebas totales. e. Conclusiones o áreas de oportunidad identificadas.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

49	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**Plan de Recuperación de Desastres (DRP)**	Asegurar que los recursos tecnológicos que soportan la operación de los procesos definidos como críticos sean recuperados de forma planeada ante algún evento disruptivo, dentro de los tiempos predefinidos y los niveles aceptables para la organización.	**DISEÑO:** 1. Debe existir un *Plan de Recuperación de Desastres (DRP)* debidamente documentado: 2. Debe incluir firma autógrafa o e-firma de autorización. 3. Debe incluir los objetivos del DRP. 4. Debe incluir roles y responsabilidades para la activación, ejecución, comunicación, gestión, revisión y documentación del plan, definidos en una matriz de asignación de responsabilidades u organigrama con descripción de funciones o listado de puestos y detalles de actividades. 5. Debe incluir los requerimientos de recuperación, relacionados con los escenarios de interrupción del entorno tecnológico definidos en el BCP. 6. Debe incluir los requerimientos tecnológicas para la ejecución del plan en esquemas *on premise* y servicios contratados con proveedores en la nube: arquitectura, componentes redundantes, capacidades de procesamiento, personal, información y todo lo necesario para garantizar la continuidad del servicio. 7. Debe incluir los protocolos de activación, ejecución y finalización del plan. 8. *Plan de pruebas del DRP* debe probarse por lo menos de forma anual, con el siguiente alcance: a. Procesos a probar. b. Áreas y personal participante, incluyendo proveedores involucrados. c. Escenarios tecnológicos a probar. d. Generar un reporte indicando el tipo de prueba a desarrollar. **IMPLEMENTACIÓN:** 1. El DRP de la organización se debe probar cada 12 meses, aun cuando no hubiesen existido cambios, debiéndose generar un reporte de los resultados de la prueba que contenga al menos: a. Personal que participó en la prueba, incluyendo proveedores. b. Incidentes presentados. c. Eficiencia de la comunicación durante las pruebas funcionales y pruebas totales. d. Tiempo de recuperación de los procesos para pruebas funcionales y pruebas totales. e. Conclusiones o áreas de oportunidad identificadas.
50	Seguridad en la operación	**Procedimiento de respaldos**	Asegurar que se cuente con información suficiente, completa y actualizada para restaurar la operación de la organización como	**DISEÑO:** 1. Debe existir un *Procedimiento de respaldos*, debidamente documentado: 2. Debe incluir firma autógrafa o e-firma de autorización. 3. Debe incluir un listado de información y sistemas sujetos al procedimiento de respaldo. 4. Debe incluir un protocolo para selección y autorización de medios de respaldo o repositorios en la nube donde se colocarán dichos respaldos.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

			respuesta a un evento disruptivo.	5. Debe incluir un protocolo de generación de respaldos. 6. Debe especificar la periodicidad de la realización de los tipos de respaldos. 7. Debe incluir un protocolo de autorización para acceso a respaldos y supervisión. 8. Debe incluir un protocolo para la destrucción de respaldos. 9. Debe incluir las medidas de protección de respaldos contra pérdida, destrucción, falsificación, publicación no autorizada y acceso no autorizado. 10. Debe incluir las medidas de protección de respaldos en sitios de almacenamiento final. 11. Debe incluir la identificación de la ubicación física o en la nube de los respaldos. 12. Debe especificar la necesidad de realizar una prueba cada 12 meses y la información que deberá documentarse como resultado de la misma. 13. En caso de que el respaldo de información forme parte de los servicios de nube contratados, el proveedor de servicios en la nube debe proporcionar las especificaciones de sus capacidades de copia de seguridad que brinda a la organización, cumpliendo con los atributos de diseño del presente control. **IMPLEMENTACIÓN:** 1. Los respaldos deben realizarse de acuerdo a lo especificado en el procedimiento y contar con medidas de protección contra pérdida, destrucción, falsificación, publicación no autorizada y acceso no autorizado. 3. Deben realizarse pruebas periódicas de recuperación de los respaldos conforme al plan de pruebas definido y generar un reporte con los resultados obtenidos, indicando al menos: a. Fecha y hora de la prueba b. Responsable de la ejecución y autorización de las pruebas. c. Identificador del medio de respaldo a probar. 4. En caso de que el respaldo de información forme parte de los servicios de nube contratados, el proveedor de servicios en la nube debe proporcionar evidencia del cumplimiento de los atributos de diseño, implementación y prueba del presente control.
51	Cumplimiento	**Auditorías de seguridad de la información**	Contar con una opinión objetiva e independiente que asegure que no se han presentado eventos de seguridad sin el conocimiento de la organización y que se opera dentro de los niveles de riesgo aceptables por la dirección.	**DISEÑO:** 1. Deben existir auditorías periódicas de seguridad de la información. 2. Las auditorías deben respetar los estándares profesionales de auditoría de sistemas de información, especificando al menos lo siguiente: a. Debe ser realizada manteniendo la Independencia organizacional. b. Debe ser realizada manteniendo la independencia profesional. c. Debe realizarse por personal certificado. d. Debe basarse en un plan de auditoría. e. Debe contar con una adecuada supervisión del trabajo. f. Debe generar un reporte de auditoría. g. Debe generar actividades de seguimiento. **IMPLEMENTACIÓN:** 1. Debe haberse realizado una auditoría cada 12 meses. 2. Debe haberse generado un reporte de auditoría firmado por un auditor certificado. 3. Deben existir papeles de trabajo de la auditoría, los cuales deben incluir lo siguiente: a. Objetivos de la revisión. b. Alcance de la revisión. c. Metodología utilizada.

Mayo de 2022	**MATRIZ DE CONTROL**	Versión 2

				d. Descripción detallada de las actividades realizadas. e. Diseño de pruebas para determinar el cumplimiento. f. Personal involucrado en la revisión. g. Hallazgos identificados. h. Recomendaciones para corregir y mitigar los hallazgos. i. Desviaciones o incidentes en la ejecución de la auditoría. 4. Deben existir planes de seguimiento a los hallazgos identificados en la revisión, que incluya: a. Actividades a realizar. b. Personal responsable de atender las no conformidades. c. Fechas de compromiso. 5. En todos los planes de seguimiento de auditorías anteriores, debe existir evidencia de la atención a los hallazgos.
52	Cumplimiento	**Responsiva sobre el cumplimiento con leyes y regulaciones aplicables**	Contar con evidencia formal del compromiso de la organización respecto al cumplimiento de la ley. Deslindar responsabilidades del SAT en caso de cualquier incumplimiento por parte de la organización.	**DISEÑO** 1. Debe existir una carta responsiva mediante la cual, la organización asume la responsabilidad respecto al cumplimiento legal en su relación con el SAT. 2. El documento debe incluir la firma del representante legal de la organización. 3. Debe especificar que la organización conoce y respetará el apego a las leyes aplicables vigentes. 4. Debe especificar que se conoce la responsabilidad de verificar el cumplimiento de dichas leyes. 5. Debe especificar que se exime al SAT de cualquier responsabilidad derivada del incumplimiento de las leyes aplicables. 6. Debe especificar que conoce y dará cumplimiento a la normatividad reglamentaria y administrativa. **IMPLEMENTACIÓN:** 1. La carta responsiva debe mantenerse vigente, con una fecha de emisión no mayor a 12 meses y reflejar cualquier cambio en la relación con el SAT.

Nota: Para efectos de la presente matriz, se entiende por:
Centro de datos: Espacio destinado para el procesamiento de datos e información.
Cifrado: Protección de información mediante codificación para evitar el acceso no autorizado (sinónimo de encripción).