

| | | | | |
|---|-------------|--|--|--|
| <p>TIC para la gestión</p> | <p>40,4</p> | <p>Indicadores de Proceso Logro: Sistemas de Información</p> | <p>25</p> <p>100</p> <p>50</p> <p>33</p> <p>33</p> | <p>La Entidad define una guía de estilo y usabilidad única, que establece los principios para el estilo de los componentes de presentación, estructura para la visualización de la información y procesos de navegación entre pantalla, entre otros. Esta guía de estilo y usabilidad debe estar participativa para cada modo tecnológico o canal utilizado por los sistemas de información y así mismo, debe estar alineada con los principios de usabilidad definidos por el Estado colombiano. Para los componentes de información, debe estar alineada con los principios de usabilidad definidos por el Estado colombiano. Para los componentes de experiencia de usuario, Para obtener el puntaje, divida el total de opciones de respuesta que cumplió la entidad sobre el total de opciones de respuesta, y luego multiplique el resultado por 100.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de sistemas de información en los que la entidad implementó la guía de estilo y las especificaciones técnicas de usabilidad, sobre el total de opciones de respuesta (4) enunciadas en los literales (a) hasta (d), y luego multiplique el resultado por 100.</p> <p>Los sistemas de información tiene habilitadas aquellas características funcionales y no funcionales, necesarias para la apertura de sus datos, de acuerdo con la legislación del Estado colombiano.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si los sistemas de información de la entidad cumplen con características que permiten la apertura de sus datos, el puntaje de la entidad es 100. De lo contrario, es 0.</p> <p>El ciclo de vida de sistemas de información se refiere al conjunto de estados en los que puede estar un sistema de información desde su creación hasta su eliminación. Esto implica, la gestión y gobierno de las etapas de los sistemas de información desde la definición de requerimientos, diseño, desarrollo, pruebas, despliegue, puesta en funcionamiento, uso, mantenimiento, hasta su eliminación.</p> <p>Para mayor información consultar la guía G.SE.01 Guía del dominio de Sistemas de Información del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, disponible en el siguiente enlace: http://www.mtrc.gov.co/arquitectura/630w3-articulo-9262.html</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de actividades realizadas por la entidad, sobre el total de actividades evaluadas (4) enunciadas en los literales a) hasta d), y luego multiplique el resultado por 100. En caso de no realizar ninguna de estas actividades, obtiene 0.</p> <p>El catálogo de los sistemas de información es un inventario detallado y documentado que contiene las fichas técnicas de los sistemas de información de una institución.</p> <p>Para mayor información consultar la guía G.SE.01 Guía del dominio de Sistemas de Información del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, disponible en el siguiente enlace: http://www.mtrc.gov.co/arquitectura/630w3-articulo-9262.html</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de actividades realizadas por la entidad, sobre el total de actividades evaluadas (3) enunciadas en los literales (a) hasta (c), y luego multiplique el resultado por 100. En caso de no realizar ninguna de estas actividades, obtiene 0.</p> <p>Se refiere a la implementación de mecanismos como políticas, parametrización de opciones de auditoría en los sistemas de información, entre otros. Que permita el registro de acciones como reacción, actualización, modificación o borrado de información, incluyendo, registro de mensajes de errores, excepciones y eventos de seguridad.</p> <p>Para mayor información, consultar la guía G.SI.02 Guía Técnica de Sistemas de Información - Trazabilidad del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, disponible en el siguiente enlace: http://www.mtrc.gov.co/arquitectura/630w3-articulo-9263.html</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si es totalmente (políticas y parametrización en más del 90% de los sistemas de información), obtiene 100 puntos. Si es parcialmente (Políticas y parametrización entre el 50 y 90% de los sistemas de información), obtiene 50 puntos. Si no implementa (Políticas y parametrización en menos del 50% de los sistemas de información), obtiene 0.</p> <p>Arquitectura de Servicios Tecnológicos, también es conocida como Arquitectura de Infraestructura. Incluye todos los elementos de TI que soportan la operación de la institución, entre los que se encuentran la plataforma hardware, la plataforma de comunicaciones y el software especializado (sistema operacional, software de comunicaciones, software de integración y manejadores de bases de datos, entre otros).</p> <p>Para mayor información consultar la guía G.ST.01 Guía del dominio de Servicios Tecnológicos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, disponible en el siguiente enlace: http://www.mtrc.gov.co/arquitectura/630w3-articulo-9277.html</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la entidad posee una arquitectura de servicios tecnológicos (arquitectura de infraestructura tecnológica) documentada pero no está actualizada, obtiene un puntaje de 50. Si la tiene documentada y actualizada obtiene 100.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la entidad aplicó algunas veces metodologías de evaluación de alternativas de solución y/o tendencias tecnológicas para la adquisición de servicios y/o soluciones de TI, obtiene un puntaje de 50. Si las aplicó siempre, obtiene un puntaje de 100. Si nunca las aplicó, obtiene 0.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la entidad implementó un programa de correcta disposición final de los residuos tecnológicos, obtiene un puntaje de 100. Si no lo implementó, obtiene 0.</p> <p>La Entidad garantiza la prestación de sus Servicios Tecnológicos utilizando diferentes mecanismos como sistemas de alimentación eléctrica, mecanismos de refrigeración, soluciones de detección de incendios, sistemas de control de acceso y sistemas de respaldo que aseguran la continuidad y disponibilidad del servicio, así como la capacidad de reacción y resolución de incidentes.</p> <p>Para mayor información consultar la guía G.ST.01 Guía del dominio de Servicios Tecnológicos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, disponible en el siguiente enlace: http://www.mtrc.gov.co/arquitectura/630w3-articulo-9277.html</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la entidad definió acuerdos de nivel de servicio para los servicios tecnológicos prestados por terceros, obtiene un puntaje de 25.</p> <p>Si la entidad realizó la definición (opción a) y el seguimiento (opción b) a los acuerdos de nivel de servicio de los servicios tecnológicos prestados por terceros, obtiene 50.</p> <p>Si la entidad realizó la implementación de herramientas de gestión para el monitoreo y generación de alarmas tempranas sobre la continuidad y disponibilidad de los servicios (opción c), obtiene 25.</p> <p>Si la entidad realizó la definición y el seguimiento a los acuerdos de nivel de servicio de los servicios tecnológicos prestados por terceros, y adicionalmente, realizó la implementación de herramientas de gestión para el monitoreo y generación de alarmas tempranas sobre la continuidad y disponibilidad de los servicios, obtiene 100.</p> <p>Si la entidad realizó la proyección de la capacidad de los servicios tecnológicos, obtiene 30.</p> |
| <p>Indicadores de Proceso Logro: Servicios Tecnológicos</p> | <p>41,5</p> | <p>Indicadores de Proceso Logro: Uso y Apropiación</p> | <p>50</p> <p>66</p> <p>33</p> | <p>Selecciona las actividades realizadas por la entidad en materia de monitoreo de la Estrategia de Gobierno en línea:</p> <p>a. Definición de acuerdos de nivel de servicio para los servicios tecnológicos prestados por terceros.</p> <p>b. Seguimiento a los acuerdos de nivel de servicio de los servicios tecnológicos prestados por terceros.</p> <p>c. Implementación de herramientas de gestión para el monitoreo y generación de alarmas tempranas sobre la continuidad y disponibilidad de los servicios.</p> <p>d. Proyección de la capacidad de los servicios tecnológicos</p> <p>Hace referencia a los procesos de operación, monitoreo y supervisión de los Servicios Tecnológicos que deben atender las Entidades, con el propósito de garantizar el óptimo y permanente funcionamiento de los mismos.</p> <p>Para mayor información consultar la guía G.ST.01 Guía del dominio de Servicios Tecnológicos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, disponible en el siguiente enlace: http://www.mtrc.gov.co/arquitectura/630w3-articulo-9277.html</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de actividades realizadas por la entidad, sobre el total de actividades evaluadas (3) enunciadas en los literales a) hasta c), y luego multiplique el resultado por 100. Si no realizó ninguna de estas actividades, obtiene 0.</p> <p>Hace referencia a la definición y gestión de los controles y mecanismos para alcanzar los niveles requeridos de seguridad y trazabilidad de los Servicios Tecnológicos.</p> <p>Para mayor información consultar la guía G.ST.01 Guía del dominio de Servicios Tecnológicos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, disponible en el siguiente enlace: http://www.mtrc.gov.co/arquitectura/630w3-articulo-9277.html</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de actividades realizadas por la entidad, sobre el total de actividades evaluadas (8) enunciadas en los literales (a) hasta (h), y luego multiplique el resultado por 100. Si no realizó ninguna de estas actividades, obtiene 0.</p> <p>Hace referencia a las gestiones realizadas por la Entidad para definir la estrategia y prácticas concretas que apoyan la adopción del Marco y la gestión TI que requiere la institución para implementar la Arquitectura TI y preparar a la institución para abordar y adaptarse al cambio, y generar los efectos generados por este.</p> <p>Para mayor información consultar la guía G.UA.01 Guía del dominio de Uso y Apropiación del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, disponible en el siguiente enlace: http://www.mtrc.gov.co/arquitectura/630w3-articulo-9281.html</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule por separado: 1. Para obtener el puntaje, divida el número de actividades realizadas por la entidad, sobre las actividades evaluadas (5) enunciadas en los literales a) hasta e), y luego multiplique el resultado por 100. 2. Si la entidad divulgó y comunicó internamente los proyectos de TI, su puntaje es 100. De lo contrario, es 0. Luego, sume las 2 anteriores operaciones y divida en dos.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la Entidad implementó la política de reducción del uso del papel, tiene un puntaje de 100. De lo contrario, obtiene 0.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de aspectos con base en los cuales la entidad incorporó soluciones tecnológicas para la gestión de documentos, sobre el total de aspectos evaluados (4) enunciados en los literales a) hasta d), y luego multiplique el resultado por 100.</p> <p>Hacer referencia al análisis funcional y desde de las perspectivas del usuario previo a la definición y especificación de las necesidades de sistematización y apoyo tecnológico a los procesos de la institución. De tal forma, que desde su diseño se incorporen facilidades tecnológicas que contribuyan a lograr transversalidad, coordinación, asistencia, mayor eficiencia y oportunidad a nivel institucional y sectorial para obtener menores costos, mejores servicios, menores riesgos y mayor seguridad.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule por separado: 1. Si eres de la automatización de procesos y/o procedimientos, la entidad hizo una revisión de estos desde la perspectiva funcional, obtiene una puntuación de 100. En caso contrario, obtiene 0. 2. Si la entidad realizó automatización de procesos y procedimientos obtiene una puntuación de 50. Si no automatizó procesos o procedimientos obtiene 0. Luego, sume los resultados obtenidos en las 2 operaciones anteriores y divida en 2.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de objetivos del PETI alcanzados, sobre el total de objetivos definidos en el PETI, y luego multiplique el resultado por 100. (No use el símbolo % en su respuesta)</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de servicios de información dispuestos en la plataforma de interoperabilidad del Estado colombiano, sobre el total de servicios de información del catálogo de servicios de la entidad, y luego multiplique el resultado por 100. (No use el símbolo % en su respuesta)</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de sistemas de información que cuentan con mecanismos de auditoría y trazabilidad, sobre el total de sistemas de información de la entidad, y luego multiplique el resultado por 100. (No use el símbolo % en su respuesta)</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de mantenimientos preventivos realizados a los servicios tecnológicos, sobre el total de mantenimientos preventivos establecidos en el plan de mantenimiento de servicios tecnológicos, y luego multiplique el resultado por 100. (No use el símbolo % en su respuesta)</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Para obtener el puntaje, divida el número de proyectos de TI a los cuales se aplicó una estrategia de uso y apropiación, sobre el total de proyectos ejecutados durante el periodo evaluado, y luego multiplique el resultado por 100. (No use el símbolo % en su respuesta)</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la entidad desarrolló durante el periodo evaluado capacidades de gestión de TI que generen mayor eficiencia en la prestación del servicio al usuario (interno o externo) obtiene un puntaje de 100. De lo contrario, obtiene 0.</p> <p>La fase de diagnóstico de privacidad puede servir como insumo al poder identificar qué información se tiene, dónde y en cabeza de quién está.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la entidad generó un documento de diagnóstico, donde se identifica de manera clara el estado actual de la entidad en la implementación de Seguridad y Privacidad de la Información O determine el estado actual de la infraestructura tecnológica para desarrollar el plan de transición del protocolo IPv4 a IPv6, obtiene una puntuación de 50. Si generó un documento de diagnóstico, donde se identifica de manera clara el estado actual de la entidad en la implementación de Seguridad y Privacidad de la Información O determine el estado actual de la infraestructura tecnológica para desarrollar el plan de transición del protocolo IPv4 a IPv6, obtiene una puntuación de 100. Si no ha hecho ninguna de las 2 acciones, obtiene 0.</p> <p>En lo que respecta a la política de seguridad y privacidad de la información.</p> <p>a. Está establecida</p> <p>b. Se encuentra alineada con los objetivos estratégicos de la entidad</p> <p>c. Define los objetivos y se alcanza a todos los procesos de la entidad</p> <p>d. No se alcanza por una o varias de las acciones.</p> <p>La Política de Seguridad y Privacidad de la Información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.</p> <p>La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento.</p> <p>La política debe ser aprobada y divulgada al interior de la entidad. Entendase por política la declaración de la Alta Dirección de la</p> |

| | | | | |
|---|------|--|----|---|
| | | <p>entidad de su compromiso en la implementación de la seguridad y privacidad de la información.</p> <p>Durante el periodo evaluado, el documento o manual con las políticas de seguridad y privacidad de la información se encuentra:</p> <p>a. En construcción b. En revisión c. Revisado, aprobado y divulgado por el comité institucional de desarrollo administrativo o el que haga sus veces. d. No lo tiene</p> | 50 | <p>Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de Información de la Entidad, definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información. Enténdase que el Manual de Políticas contiene el conjunto de lineamientos que serán implementados en la entidad y que define la forma de implementar la seguridad y privacidad de la información en la entidad para dar cumplimiento a la declaración del compromiso de la alta Dirección de la entidad.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule por separado: 1. Si la política de seguridad y privacidad de la información se encuentra alineada con los objetivos estratégicos de la entidad (teniendo en cuenta los temas de seguridad y privacidad de la información se trata en los comités del método integrado de gestión, se hace necesario que la entidad formalice este procedimiento. Para mayor información, consulte la Guía No. 4, llamada Roles y Responsabilidad de Seguridad de la Información establece las funciones que debe tener el Comité de Desarrollo Administrativo o que haga sus veces un manual de seguridad de la información.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la Entidad cuenta con un acto administrativo a través del cual se crean o se modifican las funciones del comité institucional de desarrollo administrativo o el que haga sus veces, donde se incluyen los temas de seguridad y privacidad de la información, obtiene un puntaje de 100. En caso contrario, obtiene 0.</p> |
| Indicadores de Proceso Logro: Definición del marco de seguridad y privacidad de la información y de los sistemas de información | 41,7 | <p>La entidad debe desarrollar una metodología de gestión de activos de información que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.</p> <p>Para mayor información consulte la Guía No. 5 - Gestión De Activos, disponible en el siguiente enlace: https://www.mincit.gov.co/gestionei/5/articulos/5482_G5_Gest_Clasificacion.pdf</p> <p>Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genera, obtiene, adquiere, transforma o controla en su ciudad de tal.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule por separado: 1. Si la entidad cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos, en construcción, obtiene un puntaje de 25. Si cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos, en revisión, obtiene 50. Si la entidad cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos, en aprobación, obtiene 75. Si la entidad cuenta con una metodología de gestión de activos de información donde se tienen en cuenta aspectos como: cumplimiento legal, fechas de actualización, propietarios y criticidad de los activos, revisada, aprobada y divulgada por comité institucional de desarrollo administrativo o el que haga sus veces, obtiene 100. En caso contrario, obtiene 0. 2. Si la entidad cuenta con un inventario de activos de información acorde a la metodología planteada, obtiene un puntaje de 100. Si está en desarrollo o en proceso de elaboración de un inventario de activos de información acorde a la metodología planteada, obtiene un puntaje de 50. De lo contrario, obtiene 0. Luego, suma los resultados obtenidos en las 2 operaciones anteriores y divide en 2</p> | 50 | <p>La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que están expuestos los activos, así como la declaración de aplicabilidad. Para consagrar una integración adecuada entre el MSPSI y la guía de gestión del riesgo anterior por el DAPP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo arrojados por esta entidad.</p> <p>Para la elaboración del plan de tratamiento de riesgos y la declaración de aplicabilidad, puede emplearse la Guía No. 8 - Controles de seguridad, disponible en el siguiente enlace: https://www.mincit.gov.co/gestionei/8/articulos/5482_G8_Controles_Seguridad.pdf</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule por separado: 1. Si la entidad contó con la metodología formalizada para la gestión de los riesgos de seguridad y privacidad de la información (opción 1), con el plan de tratamiento del riesgo establecido (opción 2) y con la declaración de aplicabilidad de la información (opción 3), obtiene un puntaje de 100. Si la entidad contó con la metodología formalizada para la gestión de los riesgos de seguridad y privacidad de la información (opción 1), con un avance del plan de tratamiento del riesgo (opción 2), y con la declaración de aplicabilidad en desarrollo (opción 3), obtiene 75. Si la entidad contó con las 3 opciones de respuesta, pero con una combinación diferente a las señaladas anteriormente, obtiene 50. Si la entidad contó con 2 de las opciones de respuesta, cualquier combinación, obtiene 25. Si la entidad contó con 1 opción de respuesta, obtiene 12,5. Si no contó con ninguna opción de respuesta obtiene 0. 2. Si la entidad realizó la identificación, análisis y evaluación de los riesgos de seguridad y privacidad de la información conforme a la metodología planteada, obtiene un puntaje de 100. Si está en desarrollo o en proceso, obtiene 50. De lo contrario, obtiene 0. 3. Si el documento del plan de diagnóstico y estrategia de transición de IPv4 a IPv6, se encuentra en construcción, obtiene un puntaje de 25. Si está en revisión, obtiene 50. Si está en aprobación, obtiene 75. Si ya está revisado, aprobado y divulgado por el comité institucional de desarrollo o el que haga sus veces, obtiene 100. Luego, suma los resultados obtenidos en las 3 operaciones anteriores y divide en 3.</p> |
| Seguridad y privacidad de la información | 18,2 | <p>La entidad formuló un plan de capacitación, sensibilización y comunicación de las políticas y buenas prácticas que mitiguen los riesgos de seguridad de la información a los que están expuestos los funcionarios</p> <p>Para estructurar dicho plan puede utilizar la Guía No. 14 - plan de comunicación, sensibilización y capacitación, disponible en el siguiente enlace: https://www.mincit.gov.co/gestionei/14/articulos/5482_G14_Plan_comunicacion_sensibilizacion.pdf</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule por separado: 1. Si la entidad contó con un plan de capacitación, sensibilización y comunicación de las políticas y buenas prácticas que mitiguen los riesgos de seguridad de la información a los que están expuestos los funcionarios, obtiene un puntaje de 100. En caso contrario, obtiene 0. 2. Para obtener el puntaje, divida el número de actividades realizadas por la entidad en materia de aprobación de la Estrategia de Gobierno en línea, sobre el total de aspectos evaluados (1) elevados en 4 hasta 4 y luego multiplique el resultado por 100. Luego, suma los resultados obtenidos en las 2 operaciones anteriores y divide en 2</p> | 50 | <p>La entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, usuarios) de la entidad.</p> <p>Para estructurar dicho plan puede utilizar la Guía No. 14 - plan de comunicación, sensibilización y capacitación, disponible en el siguiente enlace: https://www.mincit.gov.co/gestionei/14/articulos/5482_G14_Plan_comunicacion_sensibilizacion.pdf</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule por separado: 1. Si la entidad realizó la identificación, análisis y evaluación de los riesgos de seguridad y privacidad de la información conforme a la metodología planteada, obtiene un puntaje de 100. Si está en desarrollo o en proceso, obtiene 50. De lo contrario, obtiene 0. 2. Si el documento del plan de diagnóstico y estrategia de transición de IPv4 a IPv6, se encuentra en construcción, obtiene un puntaje de 25. Si está en revisión, obtiene 50. Si está en aprobación, obtiene 75. Si ya está revisado, aprobado y divulgado por el comité institucional de desarrollo o el que haga sus veces, obtiene 100. Luego, suma los resultados obtenidos en las 3 operaciones anteriores y divide en 3.</p> |
| Indicadores de Proceso Logro: Plan de seguridad y privacidad de la información y de los sistemas de información | 30,0 | <p>Seleccione las actividades realizadas por la entidad en materia de apropiación de la Estrategia de Gobierno en línea:</p> <p>a. Divulgación de las políticas, buenas prácticas o directrices relacionadas con seguridad de la información a través de sitio Web o intranet b. Divulgación de las políticas, buenas prácticas o directrices relacionadas con seguridad de la información a través de eventos especiales relacionados con seguridad. c. Divulgación de las políticas, buenas prácticas o directrices relacionadas con seguridad de la información a través de medios físicos (volantes, cartones, etc.) d. Divulgación de las políticas, buenas prácticas o directrices relacionadas con seguridad de la información a través de medios digitales (webinars, correo, presentaciones, etc.)</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Si la entidad realizó alguna de las acciones que están entre los numerales (a) hasta (e), obtiene un puntaje de 20. Si realizó 2 de estas acciones, obtiene 40. Si realizó 3 de estas acciones obtiene 60. Si realizó 4 de estas acciones, obtiene 80. Si realizó 5 acciones, obtiene 100. Si no realizó ninguna de las acciones, obtiene 0.</p> | 40 | <p>La entidad debe definir sus fortalezas de acuerdo a las actividades realizadas para implementar los temas de seguridad y privacidad de la información incluyendo IPv6.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Si la entidad realizó alguna de las acciones que están entre los numerales (a) hasta (e), obtiene un puntaje de 20. Si realizó 2 de estas acciones, obtiene 40. Si realizó 3 de estas acciones obtiene 60. Si realizó 4 de estas acciones, obtiene 80. Si realizó 5 acciones, obtiene 100. Si no realizó ninguna de las acciones, obtiene 0.</p> |
| Indicadores de Proceso Logro: Monitoreo y mejoramiento continuo | 37,5 | <p>Respecto al plan de tratamiento de riesgos de seguridad y privacidad de la información, indique las acciones realizadas por la entidad:</p> <p>a. Está considerando el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en el plan de tratamiento de riesgos. b. Generó y aprobó el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en el plan de tratamiento de riesgos. c. Está considerando los informes relacionados con la implementación de los controles de seguridad y privacidad de la información. d. Generó y aprobó los informes relacionados con la implementación de los controles de seguridad y privacidad de la información. e. Está definiendo los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPSI es eficiente, eficaz y efectiva. f. Definió y aprobó los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPSI es eficiente, eficaz y efectiva.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la entidad generó y aprobó el plan control operacional, en el cual se indica la metodología para implementar las medidas de seguridad definidas en el plan de tratamiento de riesgos (opción a), está considerando los informes relacionados con la implementación de los controles de seguridad y privacidad de la información (opción c), está definiendo los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPSI es eficiente, eficaz y efectiva (opción e) y aprobó los indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPSI es eficiente, eficaz y efectiva (opción f), obtiene 100. Si la entidad realizó 3 acciones en combinaciones distintas a las anteriores, obtiene 50. Si la entidad realizó 2 acciones en combinaciones, obtiene 25. Si la entidad realizó 1 acción, obtiene 12,5. Si no hizo ninguna acción, obtiene 0.</p> | 25 | <p>La entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, usuarios) de la entidad.</p> <p>Para estructurar dicho plan puede utilizar la Guía No. 14 - plan de comunicación, sensibilización y capacitación, disponible en el siguiente enlace: https://www.mincit.gov.co/gestionei/14/articulos/5482_G14_Plan_comunicacion_sensibilizacion.pdf</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la Entidad realizó la Formación del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información (opción a), obtiene 25. Si la entidad realizó la Formación y la ejecución del plan de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información, sin tener en cuenta la caracterización de grupos locales (Usuarios, Directivos, Técnicos y Terceros) obtiene 50. El proceso de seguimiento y monitoreo del MSPSI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule de forma separada: 1. Si se revisaron periódicamente los compromisos establecidos para ejecutar el plan de tratamiento de riesgos (opción a) obtiene un puntaje de 100. 2. Si la entidad realizó seguimiento a la medición de efectividad de los controles (opción b), O determinó la eficacia en la gestión de incidencias de seguridad de la información en la entidad (opción c) obtiene un puntaje de 100. 3. Si la entidad formalizó el plan de seguimiento, evaluación y análisis de resultados del MSPSI, teniendo en cuenta los indicadores de gestión y cumplimiento (opción d) O si la entidad formalizó los planes de auditoría para la revisión y verificación de la gestión de la seguridad y privacidad de la información al interior de la entidad (opción e) obtiene un puntaje de 100. 4. Si la entidad realizó seguimiento y control a la implementación del MSPSI, por parte del comité institucional de desarrollo administrativo o el que haga sus veces (opción f) obtiene un puntaje de 100. Luego, suma los resultados obtenidos en las 4 operaciones anteriores y divide en 4. Si la entidad no realiza ninguna de estas actividades, obtiene 0.</p> |
| | 50 | <p>Respecto a la implementación de acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la información, la entidad:</p> <p>a. Determina las posibles acciones correctivas derivadas de los hallazgos o debilidades identificadas en la evaluación del desempeño de la seguridad y privacidad de la información al interior de la entidad. b. Implementa las acciones correctivas y los planes de mejora de la seguridad y privacidad de la información al interior de la entidad. c. Determina si las acciones correctivas aplicadas son las adecuadas para gestionar los hallazgos y debilidades identificadas en seguridad y privacidad de la información al interior de la entidad.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule de forma separada: 1. Si la entidad determinó las posibles acciones correctivas derivadas de los hallazgos o debilidades identificadas en la evaluación del desempeño de la seguridad y privacidad de la información al interior de la entidad, obtiene 100. En caso contrario, obtiene 0. 2. Si la entidad implementó las acciones correctivas y los planes de mejora de la seguridad y privacidad de la información al interior de la entidad, obtiene un puntaje de 100. En caso contrario, obtiene 0. 3. Si la entidad determinó si las acciones correctivas aplicadas son las adecuadas para gestionar los hallazgos y debilidades identificadas en seguridad y privacidad de la información al interior de la entidad, obtiene un puntaje de 100. De lo contrario, obtiene 0. Luego, suma los resultados de las 3 operaciones realizadas anteriormente y divide en 3.</p> | 50 | <p>Los instrumentos que deben consultar las entidades para esta etapa son: Resultados de la ejecución del Plan de Revisión y Seguimiento, a la implementación del MSPSI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPSI. Para mayor información, consulte la Guía No. 17 - Mejora Continua, disponible en el siguiente enlace: https://www.mincit.gov.co/gestionei/17/articulos/5482_G17_Mejora_continua.pdf</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Calcule de forma separada: 1. Si la entidad determinó las posibles acciones correctivas derivadas de los hallazgos o debilidades identificadas en la evaluación del desempeño de la seguridad y privacidad de la información al interior de la entidad, obtiene 100. En caso contrario, obtiene 0. 2. Si la entidad implementó las acciones correctivas y los planes de mejora de la seguridad y privacidad de la información al interior de la entidad, obtiene un puntaje de 100. En caso contrario, obtiene 0. 3. Si la entidad determinó si las acciones correctivas aplicadas son las adecuadas para gestionar los hallazgos y debilidades identificadas en seguridad y privacidad de la información al interior de la entidad, obtiene un puntaje de 100. De lo contrario, obtiene 0. Luego, suma los resultados de las 3 operaciones realizadas anteriormente y divide en 3.</p> |

| | | | | |
|---|--|---|--|---|
| <p style="text-align: center;">Indicadores de resultado Seguridad y Privacidad de la Información</p> | <p>La entidad contó con un proceso de identificación de infraestructura crítica, lo aplicó y comunicó los resultados a las partes interesadas</p> | <p>Esta pregunta se puede responder con base a la valoración de activos que está haciendo en la entidad puesto que hasta este año se finalizó el catálogo de infraestructuras críticas y se inicia con su identificación oficial.</p> <p>Es una pregunta informativa sobre identificación y clasificación de activos.</p> <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial Si la entidad a entidad contó con un proceso de identificación de infraestructura crítica, lo aplicó y comunicó los resultados a las partes interesadas, obtiene un puntaje de 100. De lo contrario obtiene 0.</p> <p>Se hace necesario que las entidades y el Colciert tengan un mayor relacionamiento, así que debemos empezar a medir la efectividad de la comunicación y así poder tener acciones de mejora al respecto.</p> | <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si demoró minutos, obtiene un puntaje de 100. Si demoró horas, obtiene 75. Si demoró días, obtiene 50. Si demoró semanas, obtiene 25. (Si la Entidad no ha recibido reporte de COLCERT esta actividad no aplica. En consecuencia, no deberá tenerse en cuenta para el cálculo de los indicadores de resultado de Seguridad y Privacidad de la Información)</p> | |
| | <p>Indique si el tiempo en promedio que demoró la entidad en corregir sus vulnerabilidades luego de ser reportadas por el COLCERT tardó: a. Minutos b. Horas c. Días d. Semanas e. La entidad no ha recibido reporte de COLCERT</p> | <p>Es necesario que las entidades midan y gestionen sus incidentes de seguridad y privacidad de la información, de la misma forma es necesario hacer una medición contra de los mismos para tener una base consolidada.</p> | <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la Entidad no ha identificado incidentes, esta actividad no aplica. En consecuencia, no deberá tenerse en cuenta para el cálculo de los indicadores de resultado de Seguridad y Privacidad de la Información.</p> | <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la entidad intercambia información de incidentes de seguridad con la entidad cabeza de sector o de ser necesario con el Colciert, obtiene 100. De lo contrario, obtiene 0.</p> |
| | <p>La entidad intercambia información de incidentes de seguridad con la entidad cabeza de sector o de ser necesario con el Colciert</p> | <p>Es necesario que las entidades midan y gestionen sus incidentes de seguridad y privacidad de la información, de la misma forma es necesario hacer una medición contra de los mismos para tener una base consolidada.</p> | <p>FORMA DE ASIGNAR EL PUNTAJE: Entidades del orden nacional y territorial: Si la Entidad no ha identificado incidentes, esta actividad no aplica. En consecuencia, no deberá tenerse en cuenta para el cálculo de los indicadores de resultado de Seguridad y Privacidad de la Información.</p> | |