GUÍA / REFERENCIA PARA AUDITORÍA

ALMACENADORES DE DOCUMENTOS ELECTRÓNICOS

DIRECCIÓN GENERAL DE COMERCIO ELECTRÓNICO

VERSIÓN 3

DICIEMBRE 2022

ÍNDICE

DOCUMENTO DE REFERENCIA PARA AUDITO

REGISTRO DE ALMACENADORES (ALMACENAMIENTO POR CUENTA PROPIA)

INTRODUCCIÓN

La presente referencia tiene como sustento el marco legal del Decreto Ejecutivo 24 de 29 de marzo de 2019 y la Resolución 01 de 5 de febrero de 2020 de la DGCE. En particular, este documento sirve como referencia para la metodología y medidas a evaluar en una auditoría o evaluación de un almacenador, para que pueda registrarse o mantener su registro ante la DGCE como tal.

Esta referencia está estructurada con base en los requisitos mínimos que definen La Ley 51 de 22 de julio de 2008, modificada por la Ley 82 de 9 de noviembre de 2012 para almacenamiento tecnológico con validez legal y la reglamentación. Para cada requisito que se le exige cumplir a un almacenador, el documento describe qué debe cumplir, una forma de verificarlo y, cuando es pertinente, posibles niveles de cumplimiento con sus implicaciones.

Esta referencia también lista medidas y controles específicos consistentes con el estado del arte para los distintos aspectos y requisitos. Sin embargo, dado los principios de neutralidad tecnológica y equivalencia funcional que exige la Ley 51 de 2008 y el ritmo acelerado de cambio del estado del arte tecnológico, la aplicabilidad de la metodología, medidas y controles debe ser juzgada por el auditor en función de los objetivos del almacenador, su contexto específico y el estado del arte actual y previsto de la tecnología.

La aplicabilidad de la metodología contempla un rango mayor de opciones tecnológicas que para los prestadores de servicios, porque un almacenador no afecta directamente a terceros sino a sí mismo.

Cuando la Ley y reglamentación lo permite hay 3 niveles de medidas propuestas:

1. Para almacenamiento relevante en servicios críticos a terceros, aunque sea por cuenta propia.
2. Para almacenamiento relevante en servicios no críticos a terceros.
3. Para almacenamiento relevante esencialmente solo para el almacenador.

Esto es consistente con la Ley 82 de 9 de noviembre de 2012 que en el Artículo 5 que indica que para la integridad de un mensaje de datos el grado de confiabilidad requerido será determinado por los fines para los que se generó la información y por las circunstancias relevantes en la generación, transmisión y archivo del mensaje, así como la integridad de la información contenida y la forma como se identifique al iniciador.

Un auditor debe aplicar este principio de proporcionalidad, pero solo cuando ni el Decreto Ejecutivo 24 de 2019, ni la Resolución 01 de 2020 de la DGCE especifican o restringen formas de cumplir con los criterios de evaluación técnica en el Decreto o con los requerimientos de la resolución.

En sectores de actividad regulados, los reguladores del ramo, por especificidad, tienen la potestad de definir u omitir medidas específicas para su sector, por tanto es la intención de las auditorías autorizadas de almacenamiento tecnológico evaluar el cumplimiento con los estándares regulatorio de un sector; sin embargo, aún cuanto el regulador de un sector omita controles pertinentes para almacenamiento tecnológico, la auditoría sí debe evaluar el cumplimiento con esos controles requeridos para que un almacenador pueda registrarse ante la DGCE.

Este documento sirve como modelo de referencia para ejecutar auditorías y evaluaciones técnicas a almacenadores tecnológicos, es decir por cuenta propia, registrados o que solicitan registrarse como tal ante la Dirección General de Comercio Electrónico del Ministerio de Comercio e Industrias (DGCE).

El esquema de auditoría y evaluación técnica en este documento es solo una referencia y no una obligación. Puede haber razones válidas para desviarse de la metodología o medidas planteadas en esta referencia. Ni seguir esta referencia ni desviarse de ella exime al auditor autorizado de la responsabilidad de utilizar su conocimiento y criterio para evaluar si el almacenador tecnológico, en adelante el almacenador, demuestra el alistamiento, capacidad e intención de cumplir con los requisitos que exige la ley, las normativas y con la expectativa de cumplimiento durante el periodo proyectado hasta la siguiente auditoría.

Este documento no cubre el caso de prestadores de servicio de almacenamiento tecnológico de terceros (prestadores de servicio). Existe un documento similar para ese caso.

EVALUACION TECNICA Y AUDITORIA

1.0 Integridad de los documentos almacenados[1]

1.1 Firma electrónica digital criptográfica calificada (firma electrónica calificada).

- El depósito debe estar claramente definido.
- El almacenador debe utilizar una firma electrónica calificada como garantía de integridad del documento en el depósito. Para los metadatos se deberá asegurar su integridad con mecanismos confiables que utilice el almacenador.
- Si el certificado digital correspondiente no es de la DNFE, debe ser trazable a un prestador de servicios de certificación autorizado por la DNFE.
- La criptografía en uso debe ser criptografía fuerte, independientemente de que sea calificada.
- La firma debe proteger el documento.

1.2 Firma electrónica digital criptográfica para documento en tránsito.

- El punto de ingreso al sistema de almacenamiento tecnológico debe estar claramente definido.
- El almacenador debe utilizar una firma criptográfica como garantía de integridad del documento.
- La criptografía en uso debe ser criptografía fuerte, independientemente de que sea calificada.
- La firma criptográfica puede ser una firma electrónica calificada o no calificada.
    - Para documentos en tránsito, el almacenador puede usar el criterio de costo-efectividad al decidir o no por una firma calificada siempre y cuando la firma utilice criptografía fuerte.
    - Utilizar la firma electrónica calificada del depósito en múltiples puntos de ingreso, por ejemplo, sucursales, puede exponer innecesariamente la clave privada en dispositivos de bajo costo, lo que podría disminuir en lugar de elevar el nivel de seguridad de la operación.

[1] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.1 Integridad

- Utilizar firmas electrónicas calificadas individuales de cada uno de múltiples puntos de ingreso puede elevar los costos de operaciones sin necesariamente elevar la seguridad de la operación.
- Para múltiples puntos de ingreso, es preferible utilizar distintas firmas criptográficas, y preferiblemente efímeras o de corta validez. De esta manera, una firma comprometida tiene impacto limitado en la operación.

- La firma debe proteger el documento.
- Si la firma para un documento en tránsito no es calificada, al llegar al depósito el documento debe volver a ser firmado con una firma electrónica calificada.

    - Es esperado y deseable que existan dispositivos de costo módico para el ingreso de documentos al sistema de almacenamiento. Por tanto, la clave privada para la firma en el depósito probablemente contará con medidas de protección más robustas, consistentes con la longevidad de almacenamiento.

1.3 Tránsito desde el ingreso hasta el depósito.

- El almacenador debe proteger la integridad del documento desde que ingresa al sistema de almacenamiento, incluso antes de lograr firmarlo criptográficamente.

    - Dado el uso correcto de criptografía fuerte, el principal riesgo contra integridad es un dispositivo comprometido, por ejemplo, con código nocivo (malware) o accesos no autorizados, que permite alteraciones antes de la firma criptográfica.
    - Si el dispositivo de ingreso tiene la funcionalidad adecuada y segura, es preferible firmar el documento dentro del mismo dispositivo, lo más temprano posible en el flujo de datos capturados.
    - El dispositivo de ingreso puede actuar como un dispositivo periférico de un dispositivo más robusto que firma con la funcionalidad adecuada y segura, por ejemplo, un digitalizador conectado a una computadora que lo controla.

- El recorrido del documento en tránsito no debe incluir demoras prolongadas.

    - Dado el uso correcto de criptografía fuerte, el principal riesgo contra integridad una vez firmado es una clave privada o contraseña de la clave privada comprometidas. Mientras más tiempo en tránsito más oportunidad de aprovechar estas credenciales comprometidas para alterar el documento.
    - Dada la expectativa razonable de costo-efectividad de múltiples dispositivos de ingreso, el nivel de protección de la clave privada para documentos en tránsito puede ser menor al de la clave privada para el depósito, y por tanto sujeta a mayor riesgo de compromiso.
    - Como ejemplo, si vulnerabilidades no conocidas (día cero) o falla en configuraciones permite capturar la clave privada en un dispositivo, mientras más demore el documento en llegar al depósito, mayor el riesgo de poder alterarlo y volver a firmarlo.

1.4 Demostraciones de cumplimiento.

- Estas capacidades deben ser demostrados con documentos de prueba o documentos recientes de cada medio de información aceptado por el prestador de servicios por ejemplo impreso, audio, video.
- Comprobar que las medidas y controles de seguridad en una muestra representativa de los dispositivos de ingreso son consistentes con el riesgo de la situación, para que no se puedan dar alteraciones antes de firmar el documento.
    - Revisar por ejemplo configuraciones, control de acceso, ubicación dentro de la arquitectura del sistema, disponibilidad y protección de bitácoras entre otros.
    - La sección de medidas y controles de seguridad incluye ejemplos para la seguridad de ambientes computacionales.
    - El cumplimiento con estándares FIPS o con evaluaciones EAL de suficiente nivel representan altos niveles de confiabilidad de seguridad para el propósito del sistema.
- Verificar que el documento se firma lo más temprano posible después de su ingreso.
- Verificar que la aplicación utilizada para firmar criptográficamente es aceptable para la industria, está correctamente configurada y está protegida.
    - Cumplimiento con evaluaciones EAL de nivel adecuado, por ejemplo, y evidencia de protección del ciclo de vida, por ejemplo, con firma digital criptográfica del proveedor y protección gestionada de lista blanca, representan un alto nivel de seguridad.
- Confirmar las características de las firmas criptográficas en uso para el tránsito y para el depósito: algoritmos de firma, tamaño de clave, longevidad de la firma, confiabilidad de la aplicación de firma, configuración de la aplicación de firma.
    - Confirmar que los parámetros de la firma corresponden a criptografía fuerte.
    - Para almacenadores que aceptan documentos de larga longevidad y alto valor o alto nivel crítico, es preferible que los algoritmos de firmas criptográficas se consideren resistentes a ataques cuánticos previstos (Quantum ready).
- Confirmar que las medidas de protección de las claves privadas para las firmas y para las credenciales de uso de las claves son consistentes con el riesgo de la situación.
    - Para las firmas electrónicas calificadas para el depósito, el uso de módulos de seguridad en hardware (Hardware Security Modules) representa un alto nivel de seguridad, consistente con almacenamiento tecnológico que participa en servicios críticos a terceros. El Almacenador puede utilizar otros mecanismos en situaciones o contextos justificados.
    - El uso de dispositivos externos que cumplen con el estándar FIPS-2 nivel 3 también representa un alto nivel de protección contra fraude, aunque tiene riesgos más elevados de robo o extravío. Este método es consistente con almacenamiento tecnológico que participa en servicios a terceros que no sean críticos, o en servicios críticos si la protección en torno al dispositivo externo es de alto nivel.
    - El costo de un módulo de seguridad en hardware o dispositivos externos con nivel de protección similar puede estar fuera del alcance de un rango de interesados

razonables, por ejemplo, cierto tamaño de Pymes. Cuando el almacenamiento tecnológico participa principalmente solo en la operación interna del Almacenador, almacenar la clave privada en computadoras o ambientes de bajo riesgo residual de seguridad puede ser aceptables, por ejemplo, en un servidor adecuadamente configurado y protegido, a cargo de personal competente en seguridad.

- Si la clave requiere contraseña para usarla, verificar que las contraseñas o credenciales son robustas.

- Confirmar que existe un mecanismo apropiado de custodia de la clave o claves privadas para documentos en tránsito, y para sus credenciales de uso, en caso de falla o ausencia de las personas o elementos involucrados.
    - La recuperación de claves o contraseñas en custodias debe representar un grado de rendición de cuentas y trazabilidad de alto nivel, para minimizar el riesgo de uso indebido de las claves o contraseñas.
    - La pérdida de una clave o su contraseña para uso con el depósito o tránsito, solo incomoda al Almacenador, por ejemplo, con demoras o interrupciones para poder seguir almacenando con firmas apropiadas, siempre y cuando no estén comprometidas. Por tanto, un mecanismo de custodia de claves o de sus credenciales no es esencial para Almacenadores, especialmente cuando el almacenamiento es relevante en servicios no críticos a terceros.
- Revisar la trayectoria del flujo de documentos en tránsito.
- Revisar que no haya demoras injustificadas en el tránsito.
    - Las demoras deben ser consistentes con lo esperado para un tránsito sencillo hacia el depósito.
    - El tránsito puede incluir demoras correspondientes a procesamiento adicional justificado, por ejemplo, para la extracción de metadatos, distribución de copias o manejo administrativo.
    - Evaluar la posibilidad que el documento quede sin firma de depósito por periodos prolongados, por ejemplo, semanas.
- Verificar que al recibir la firma electrónica calificada en el depósito se mantiene la trazabilidad de uso de las firmas criptográficas en tránsito.
    - Debe ser posible para un perito demostrar qué firma se utilizó en tránsito.
- Confirmar que el certificado digital de las firmas electrónicas calificadas corresponde a la DNFE o a un prestador de servicios de certificación autorizado por la DNFE.
- Analizar el riesgo de colusión entre los responsables por el ingreso de documentos y los responsables por las firmas criptográficas en uso.
    - Esta colusión podría alterar un documento y su firma de garantía de integridad.
    - El almacenador puede separar las responsabilidades de ingreso o captura de documentos de las responsabilidades de control sobre el sistema de firmas.

- El almacenador puede obtener una constancia externa de integridad tan temprano en el ciclo como sea posible. El uso del sello de tiempo de la DNFE sirve como esta constancia, si está disponible correctamente.
- El conjunto de estas medidas de separación de responsabilidades y de constancia externa representan un alto nivel de seguridad.
- Cuando el almacenador no demuestra un alto grado de conocimiento o manejo tecnológico de seguridad, el uso del sello externo de un proveedor competente con firma electrónica calificada es preferible. En este caso evaluar los riesgos de alteración en tránsito al proveedor de sello externo.

2.0 Fidelidad de presentación[2]

2.1 Fidelidad de captura.

- Si hay digitalización, verificar que la resolución de captura es suficiente para que la calidad de percepción sensorial humana sea equivalente a la del documento original, sin distorsiones.
    - La métrica y parámetros de fidelidad mínima apropiada verían según la naturaleza original del documento, por ejemplo, texto o imágenes impresas, audio, video, por ejemplo, visual o audio.
    - En el caso de material impreso, la resolución mínima de captura debe ser 200 puntos por pulgada cuadrada (200 ppp).
- Para documentos de aplicaciones especializados, por ejemplo, imágenes médicas o datos de sensores científicos, la fidelidad de captura debe ser consistente con las prácticas aceptadas de la industria.
    - Aún con material impreso, aplicaciones especializadas pueden requerir mayor resolución que todavía no esté reglamentada, por ejemplo, cartografía, imágenes impresas de rayos X, información científica.
- Cuando se desea usar compresión en los documentos, por ejemplo, por motivos de eficiencia, los algoritmos deben utilizar mecanismos de compresión sin pérdida.

2.2 Fidelidad para documentos nativos digitales.

- Cuando el documento a almacenar ya es un documento digital la fidelidad de captura consiste en preservar la integridad del documento como fue recibido.
    - El proceso de firma criptográfica para proteger al documento en tránsito debe aplicarse al documento recibido sin alteración.
    - Si el Almacenador desea aplicar compresión, esta debe ser sin pérdida y darse después de aplicar la firma criptográfica.

[2] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.3 Registro de tiempo.

- Un documento que haya sido digitalizado previo a su ingreso al sistema de almacenamiento también es considerado nativo digital por el sistema.

2.3 Fidelidad de presentación.

- La fidelidad de presentación a terceros debe ser adecuada.
    - Para documentos digitalizados la fidelidad de presentación debe ser consistente con la fidelidad de captura.
    - Para documentos nativos digitales la fidelidad de presentación consiste en preservar la integridad del documento recibido.
- Las opciones de presentación de los documentos almacenados deben ser consistente con el objetivo declarado, a los auditores y a la DGCE, del almacenamiento tecnológico.
    - Según el objetivo declarado, por ejemplo, documentos legales, las opciones de formatos de presentación para documentos digitalizados debe resultar consistente. Ejemplo de formatos son PDF, familia Microsoft Office, familia Mac, familia Open Source, JPG, MPEGx, .wav, otros, según los objetivos.
    - Los formatos deben ser comunes en el mercado, salvo razón sustentada.
    - Un Almacenador no está obligado a contar con dispositivos de presentación en sus facilidades, por ejemplo, pantallas para imágenes médicas o planos arquitectónicos con la resolución o geometría necesarias.
- Para documentos de aplicaciones especializadas, por ejemplo, imágenes médicas o datos de sensores científicos, la fidelidad de presentación debe ser consistente con las prácticas aceptadas de la industria.

2.4 Demostraciones de cumplimiento.

- Estas capacidades deben ser demostradas con documentos de prueba o documentos recientes de cada tipo de información aceptado por el Almacenador, por ejemplo, impreso, audio, video.
- Revisar que el Almacenador ha especificado por escrito los formatos y parámetros de fidelidad de captura, almacenamiento y presentación para los objetivos de su almacenamiento tecnológico.
- Comprobar que la configuración de los dispositivos de captura de documentos de cualquier tipo de medio de información es consistente con los parámetros aceptables de fidelidad de captura para los distintos tipos de información.
- Verificar si las aplicaciones de captura o almacenamiento aplican algoritmos de compresión y en ese caso verificar que es compresión sin pérdida.
- Comprobar que la captura de una muestra de documentos de cada tipo de información cumple con la fidelidad aceptable correspondiente.
- Si el Almacenador contempla el almacenamiento de documentos de aplicaciones especiales, por ejemplo, imágenes médicas, datos industriales o científicos, confirmar que la fidelidad del documento es adecuada según las prácticas aceptadas de la industria correspondiente.

- Comprobar que la fidelidad de presentación, y por tanto de captura, en una muestra representativa de documentos de los distintos medios objeto del almacenamiento es consistente con los parámetros mínimos de fidelidad aceptables en la industria para el tipo de información.
- Verificar que la facilidad y tiempos de demora en presentar o exportar los documentos almacenados es razonable según los objetivos del almacenamiento, por ejemplo, acceso por internet, dispositivos portables de memoria, u otros.
    - Cuando el almacenamiento tecnológico participa en servicios críticos a terceros, la expectativa contemporánea es que los documentos estén disponibles 24x7x365 por internet con base en credenciales de acceso del cliente sin intervención manual del Almacenador, con un porcentaje de disponibilidad anual aceptable en la industria.
    - Cuando el almacenamiento tecnológico es relevante en servicios no críticos a terceros, es razonable que los documentos estén disponibles con demoras que no entorpezcan la calidad del servicio al cliente o usuarios del Almacenador y no mayores que los mecanismos comunes de almacenamiento físico.
    - Cuando el almacenamiento tecnológico es relevante esencialmente solo para el Almacenador, una expectativa razonable es que el Almacenador pueda entregarle el documento a un interesado autorizado dentro de 24 horas de iniciar acceso al sistema.
- Especialmente en el caso de un Almacenador pequeño, con poco personal e infraestructura, al entrevistar al personal encargado del sistema de almacenamiento, consistente con la sección 4.7, verificar que este personal entiende el concepto de fidelidad y está familiarizado con la forma de configurar y operar los dispositivos para preservarla, por ejemplo, durante las pruebas de captura y presentación de documentos.

3.0 Registro de tiempo[3]

3.1 Preservación y presentación de tiempos.

- La fecha y hora en que el documento ingresa al sistema de almacenamiento debe ser trazable (transformable) al formato Universal Time Coordinated (UTC).
    - Esta fecha y hora corresponde al momento de captura en los dispositivos de ingreso al sistema.
    - Para documentos de larga duración, por ejemplo, archivos grandes o videos, la fecha y hora de ingreso corresponde al momento en que finaliza la captura del documento.

[3] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.3 Registro de tiempo.

- Si la demora entre el ingreso y el momento de aplicar la firma criptográfica para protección en tránsito es minúscula, por ejemplo, milisegundos, la fecha y hora de ingreso puede ser el momento en que se aplica la firma.

- La fecha y hora en que el documento es almacenado en el depósito debe ser trazable (transformable) al formato Universal Time Coordinated (UTC).
    - Esta fecha y hora corresponde al momento en que se aplica la firma electrónica calificada del depósito.
- Las fechas y horas de ingreso y de firma en el depósito deben incluir día, mes, año, hora, minutos y segundos.
    - El Almacenador puede agregar precisión adicional si desea, por ejemplo, milisegundos.
    - Si la fecha y hora no están expresadas ya en UTC, deberán indicar la zona horaria trazable a UTC.
- La fecha y hora del sistema de almacenamiento debe estar sincronizado directa o indirectamente con la hora oficial de Panamá que mantiene el Centro Nacional de Metrología de Panamá (Cenamep AIP).
    - El uso del protocolo NTP configurado correctamente en una red de desempeño adecuado (demoras y disponibilidad) permite la sincronización apropiada.
    - El uso de un servicio de sellado de tiempo por un prestador de servicios de certificación de sellado de tiempo registrado en la DNFE es adecuado para la sincronización apropiada siempre y cuando las demoras y disponibilidad del servicio sean compatibles con la expectativa de la industria.

3.2 Demostraciones de cumplimiento.

- Estas capacidades deben ser demostrados con documentos de prueba o documentos recientes de cada medio de información aceptado por el prestador de servicios por ejemplo impreso, audio, video.
- Verificar la descripción, implementación y configuración del sistema que mantiene la fecha y hora en el sistema de almacenamiento.
- Verificar que las fechas y horas de ingreso y firma de depósito son trazables a UTC.
- Verificar el historial de validez (accuracy) y confiabilidad (precisión) de la bitácora de tiempos del sistema de fecha y hora del sistema de almacenamiento.
- Verificar el historial de disponibilidad de comunicación con las fuentes primarias de fecha y hora del sistema de almacenamiento y juzgar su disponibilidad futura.
- Especialmente en el caso de un Almacenador pequeño, con poco personal e infraestructura, al entrevistar al personal encargado del sistema de almacenamiento, consistente con la sección 4.7, verificar que este personal entiende el concepto de preservación del tiempo y que está familiarizado con la forma de configurar y operar los dispositivos para preservarlo, por ejemplo, durante las pruebas de captura y presentación de documentos.

4.0 Uso de metadatos4

4.1 Preservación y presentación de Metadatos.

- El Almacenador debe preservar los metadatos requeridos para el documento en forma separable del documento que ingresó al sistema de almacenamiento, para no distorsionarlo.
- Los metadatos deben incluir el origen del documento.
    - La fuente debe ser la persona, natural o jurídica, o el dispositivo que generó el documento.
    - Si es una persona natural con cédula panameña debe incluir el nombre y el número de cédula.
    - Si es una persona jurídica panameña debe incluir el nombre y el número de Registro Único de Contribuyente (RUC).
    - Si es una persona natural extranjera sin cédula panameña o una persona jurídica extranjera debe incluir el nombre, información de identidad y tipo de información de identidad, por ejemplo, pasaporte, número de contribuyente, número de seguro social, dominio de nombre, u otro.
    - Si la fuente es un dispositivo, puede incluir el nombre, pero debe incluir una identificación efímera del dispositivo, por ejemplo, una dirección IP estática, o el número MAC correspondiente si la dirección es dinámica.
    - El contexto de la naturaleza del almacenamiento tecnológico debe servir de guía para evaluar si el tipo de identificación almacenado es adecuado.
- Los metadatos deben incluir el destino del documento, es decir la identidad del repositorio y su afiliación a persona natural o jurídica.
    - Se presume que el depósito es un dispositivo o una facilidad en línea y requiere la información correspondiente a un dispositivo fuente.
- Los metadatos deben incluir fecha y hora de ingreso al sistema de almacenamiento.
- Los metadatos deben incluir fecha y hora de ingreso al depósito.
- En áreas con legislación especial como documentos de valor histórico, el Almacenador debe incluir los metadatos obligatorios especiales que exija la ley o los reglamentos aplicables.
- El Almacenador puede incluir metadatos de interés adicionales para si, para sus clientes o usuarios de servicios, por ejemplo, el nombre del documento, referencia del cliente, palabras claves o descripción breve del contenido.

4.2 Presentación de metadatos.

- El Almacenador debe ser capaz de exportar los metadatos almacenados en formatos comunes de la industria para las aplicaciones que no sean especializadas.
- Un documento y sus metadatos deben poder ser presentados en forma que permita distinguir fácilmente los metadatos de su documento asociado.

[4] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.4 Uso de Metadatos.

- Si la operación de almacenamiento tecnológico contempla la posible presentación del documento almacenado en las facilidades del Almacenador, el dispositivo de presentación debe poder presentar los metadatos en forma comprensible y separada del documento correspondiente.
- Un interesado autorizado debería poder consultar los metadatos de un documento sin tener que recibir el documento.

4.3 Demostraciones de cumplimiento.

- Estas capacidades deben ser demostradas con documentos de prueba o documentos recientes de cada medio de información aceptado por el prestador de servicios por ejemplo impreso, audio, video.
- Confirmar la capacidad de capturar o preservar los metadatos requeridos del documento que ingresa, para cada tipo de medio de información consistente con los objetivos del almacenamiento tecnológico.
- Confirmar que las firmas para proteger documentos en tránsito y en el depósito también protegen a los metadatos.
- Confirmar la capacidad de presentar los metadatos en forma separable del documento que ingresa, para cada tipo de medio de información consistente con los objetivos del almacenamiento tecnológico.
- Verificar los formatos y validez de los metadatos de los documentos para cada tipo de medio de información consistente con los objetivos del almacenamiento tecnológico.
- Evaluar el riesgo de que el sistema de manejo de metadatos pudiera perder en forma irrecuperable la asociación entre metadatos y sus documentos correspondientes.
- Especialmente en el caso de un Almacenador pequeño, con poco personal e infraestructura, al entrevistar al personal encargado del sistema de almacenamiento, verificar que este personal entiende el concepto de preservación y protección de metadatos, y que está familiarizado con la forma de configurar y operar los dispositivos para lograrlo, por ejemplo, durante las pruebas de captura y presentación de documentos.

5.0 Reproducción / Exportación[5]

- En el caso de audio o video, los algoritmos para representar la información deben ser adecuados para la calidad de percepción de la aplicación deseada según las prácticas aceptadas en la industria y sus parámetros deben estar configurados en forma y consistentes con esa calidad deseada.
- Para material impreso digitalizado, la geometría del material original debe poder ser identificable y reproducible.
- Un interesado autorizado debe poder reproducir un documento impreso digitalizado con la geometría original si posee los dispositivos tecnológicos adecuados.

[5] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.5 Reproducción / Exportación.

6.0 Respaldo[6]

6.1 Continuidad en servicios críticos a terceros.

- La gestión de continuidad y contingencia es uno de los criterios de evaluación técnica que exige el Decreto Ejecutivo 24 de marzo de 2019, Ministerio de Comercio e Industria.
- Documentación de las medidas de continuidad en cuanto a la disponibilidad de respaldos y suministro de energía es parte de la documentación administrativa que exige la Resolución 01 de febrero 2020, Dirección General de Comercio Electrónico, Ministerio de Comercio e Industria.
- Cuando el almacenamiento tecnológico participa en servicios críticos a terceros el Almacenador debe contar con un plan de continuidad de negocios.
- El Almacenador debe ser capaz de mantener los documentos accesibles a sus clientes en forma consistente con las expectativas del mercado.
    - Esto es consistente con buenas prácticas de seguridad de información para proveedores de servicios a terceros.
    - Este documento de referencia trata en esta sección de respaldo toda la práctica de continuidad de negocios en forma específica.
    - Ver la expectativa de facilidad y tiempos de acceso en las demostraciones de cumplimiento de fidelidad de presentación.
- El Almacenador debe contar con un plan de continuidad de negocios.
- El plan de continuidad de negocios debería seguir estándares o guías internacionales como el ISO 22301 o el Business Continuity Institute
- Como mínimo, el plan debe incluir
    - Un análisis de riesgos de continuidad
    - Un análisis de impacto en el negocio
    - Una descripción de la plataforma del servicio, que puede ser la misma que para el requisito de seguridad
    - El plan de continuidad temporal en caso de incidente
    - Un plan de recuperación, incluyendo el plan de pruebas de recuperación
    - El plan o procedimientos de gestión de continuidad (alistamiento)
- Si el Almacenador ha estado operando al menos por un año, debe mostrar evidencia de ejecución de los procedimientos de alistamiento para emergencia.
- Si el Almacenador ha estado operando al menos por un año, debe mostrar evidencia de ejecución de las pruebas de recuperación.

[6] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.6 Respaldo.

6.2 Continuidad en servicios no críticos a terceros.

- Cuando el almacenamiento tecnológico participa en servicios no críticos a terceros el Almacenador debería contar con una planificación por escrito de contingencia y preferiblemente con un Plan de Continuidad de negocios.
    - En servicios no críticos a terceros, una falla de continuidad afecta principalmente la reputación del Almacenador y no a terceros.
    - Si el Almacenador no es un sujeto regulado más allá que por los requisitos de registro en la DGCE, no es la intención exigir estándares de continuidad que no se le exigen a negocios no digitales.
    - Si el Almacenador es un sujeto regulado más allá que por los requisitos de registro en la DGCE, el regulador del ramo es quien tiene la responsabilidad por hacer valer sus reglamentos.
- La planificación debería incluir
    - Una descripción de los sistemas o dispositivos de respaldo, que puede ser la misma que para el requisito de seguridad
    - Las acciones principales a tomar en caso de incidente
    - Un plan de recuperación

6.3 Continuidad en servicios esencialmente solo para el Almacenador.

- Cuando el almacenamiento tecnológico es relevante esencialmente solo para el Almacenador, debería contar al menos con una descripción escrita del proceso de respaldos.
- La descripción debería incluir
    - Los dispositivos de respaldo
    - Los dispositivos de continuidad de energía, si existen
    - El proceso de respaldo, incluyendo frecuencia y responsable
    - El proceso de restauración, incluyendo responsable

6.4 Contingencia y recuperación en servicios críticos a terceros.

- Como mínimo, el plan de recuperación debe incluir:
    - Referencia a la descripción de la plataforma tecnológica de los servicios de almacenamiento tecnológico.
    - Declaración de tiempos de recuperación
    - Procedimiento de recuperación
    - Designación del equipo de recuperación de emergencias
    - Plan de pruebas de recuperación

6.5 Contingencia y recuperación en servicios no críticos a terceros.

- Como mínimo, el plan de recuperación debe incluir:
    - Referencia a la descripción de la plataforma tecnológica de los servicios de almacenamiento tecnológico.
    - Procedimiento de recuperación
    - Responsables por la recuperación

6.6 Contingencia y recuperación en servicios esencialmente solo para el Almacenador.

- Está cubierto en la sección 6.3 de continuidad.

6.7 Demostraciones de cumplimiento en servicios críticos a terceros.

- Verificar la estructura organizacional de gobernabilidad en cuanto a continuidad de negocios: cadena de responsabilidades, procedimientos de aprobación de cambios.
- Verificar que existe un plan de continuidad de negocios aprobado oficialmente.
- Verificar que cumple con el contenido mínimo y evaluar tanto su pertinencia al servicio como su validez práctica.
- Verificar evidencia de la ejecución de gestión de alistamiento, si aplica.
- Verificar evidencia de la ejecución de pruebas de recuperación, si aplica.
- Evaluar la capacidad del prestador de servicios de implementar su propio plan de continuidad de negocios.

6.8 Demostraciones de cumplimiento en servicios no críticos a terceros.

- Verificar la cadena de responsabilidades sobre continuidad y contingencia.
- Verificar la planificación de continuidad y contingencia, preferiblemente que exista un plan de recuperación.
- Si hay plan de recuperación, verificar si contiene el contenido mínimo esperado y evaluar tanto su pertinencia al servicio como su validez práctica.
- Evaluar la capacidad del Almacenador de implementar su propia planificación de continuidad y contingencia.

6.9 Demostraciones de cumplimiento en servicios esencialmente solo para el Almacenador.

- Verificar si la descripción del proceso de respaldo contiene el contenido mínimo esperado y evaluar tanto su pertinencia al servicio como su validez práctica.
- Evaluar la capacidad del Almacenador de implementar su propio proceso de respaldo.

7.0 Jefe de archivo[7]

7.1 Designación.

- El Almacenador debe designar oficialmente a un Jefe de archivo, responsable por la operación de almacenamiento tecnológico.
- En el caso de operaciones pequeñas con poco personal y en las cuales el almacenamiento no participa en servicios críticos a terceros, la designación puede ser simplemente una nota firmada por el responsable del negocio o parte de la información oficial por aportar a la DGCE.

7.2 Responsabilidades definidas.

- El Almacenador debe definir las responsabilidades del Jefe de archivo
- Las responsabilidades deben incluir velar por la validez de los procesos de digitalización, por la fidelidad de captura, almacenamiento y reproducción, y por la operación correcta de los mecanismos de firmas electrónicas en uso.
- Las responsabilidades deben dejar claro si son directas o qué nivel jerárquico y supervisión ejecuta el Jefe de archivos.
- En el caso de operaciones pequeñas con poco personal, es de esperar que el Jefe de archivo sea responsable directo por todas las responsabilidades.

7.3 Relación con la firma calificada

- El Almacenador debe especificar la relación entre el Jefe de archivos y la firma electrónica calificada para garantizar la integridad en el depósito, por ejemplo, si el Jefe de archivo está en control de la clave privada de la firma electrónica calificada o de las otras firmas, o si es un supervisor y delega el control de la clave privada, o si supervisa la operación de alguna manera.
- El Almacenador debe especificar si el Jefe de Archivos es representante legal de la organización o tiene poder legal para representar a la organización externamente.

7.4 Demostraciones de cumplimiento.

- Verificar si hay documentos que designan oficialmente al Jefe de archivos y que definen sus responsabilidades. Verificar la coherencia de sus contenidos.
- Entrevistar al Jefe de archivo y corroborar si comprende su propio proceso de almacenamiento tecnológico y los mecanismos de cumplimiento con los requisitos.
- Evaluar si el Jefe de archivo comprende suficientemente bien el proceso de digitalización, si aplica, para poder certificar que un documento digitalizado realmente corresponde al documento físico original.

[7] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.7 Jefe de archivo.

8.0 Tiempo de conservación[8]

8.1 Sistema de gestión de documentos en servicios críticos a terceros.

- El Almacenador debe contar con un sistema de gestión de documentos, capaz de indicar el tiempo transcurrido y plazos de conservación de documentos que exijan las Leyes o regulaciones correspondientes.
- Debe tener un procedimiento para determinar la fecha y hora de inicio de plazos legales de conservación, si aplica.
    - La fracción del plazo de conservación transcurrida previa al ingreso al sistema de almacenamiento puede incluir cumplimiento como documento físico y como documento digitalizado.
- Debe tener un proceso de gestión de plazos que permita responder cuánto tiempo falta para cumplir el plazo y alertarlo cuando se cumple.
- El proceso de gestión de plazos debe poder aclarar la fracción del plazo cumplida antes de que el documento ingresara al Almacenador y el tiempo adicional transcurrido desde que ingresó.
- La información de tiempo transcurrido y plazos debe contar con protección de integridad y persistencia (continuidad).

8.2 Sistema de gestión de documentos en servicios no críticos a terceros.

- Preferiblemente, el Almacenador debería contar con un sistema de gestión de documentos, capaz de indicar el tiempo transcurrido y plazos de conservación de documentos que exijan las Leyes o regulaciones correspondientes.
- Debería tener un procedimiento para determinar al fecha y hora de inicio de plazos legales de conservación, si aplica.
    - La fracción del plazo de conservación transcurrida previa al ingreso al sistema de almacenamiento puede incluir cumplimiento como documento físico y como documento digitalizado.
- Debería tener un proceso de gestión de plazos que permita responder cuánto tiempo falta para cumplir el plazo y alertar cuando se cumple.
- El proceso de gestión de plazos debería poder aclarar la fracción del plazo cumplida antes de que el documento ingresara al Almacenador y el tiempo adicional transcurrido desde que ingresó.
- La información de tiempo transcurrido y plazos debería contar con protección de integridad y persistencia (continuidad).

8.3 Sistema de gestión de documentos en servicios esencialmente solo para el Almacenador.

- El Almacenador debería tener una bitácora capaz de indicar el tiempo transcurrido y plazos de conservación de documentos que exijan las Leyes o regulaciones correspondientes.

[8] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.8 Tiempo de conservación.

- Debería tener un procedimiento para determinar al fecha y hora de inicio de plazos legales de conservación, si aplica.

8.4 Mecanismo de descarte en servicios críticos a terceros.

- El proceso de descarte de documentos físicos almacenados aparece en el Decreto Ejecutivo de 24 de 2019, Artículo 12.
- El Almacenador debe tener un proceso de aprobación de descarte de documentos claros para cuando se cumplan las condiciones de descarte.
    - En cuanto a el procedimiento que indica el Decreto Ejecutivo de 24 de 2019, Artículo 12, numeral 3, no hay cliente que firme el acta.
- Debería borrar la información de los documentos de terceros cuando se da su descarte.
- Debe poder aplicar borrado seguro a información confidencial descartada.
- Debe mantener información del descarte final de la documentación, según indica el Decreto Ejecutivo de 24 de 2019, Artículo 12, numeral 6.
- Para operaciones de poca complejidad o personal que no participen en servicios críticos a terceros, el proceso de descarte de documentos físicos digitalizados que describe el Decreto Ejecutivo de 24 de 2019, Artículo 12, puede ser simple e informal siempre y cuando cumpla con el contenedor sellado, el inventario y el acta de descarde que exige el Decreto, aunque sean innecesarios.

8.5 Demostraciones de cumplimiento.

- Verificar que existe un proceso de descarte y verificar su descripción.
- Verificar la información de seguimiento a plazos de descarte de documentos para una muestra de documentos existentes o para documentos de prueba, cuando en el objeto del almacenamiento tecnológico apliquen plazos de descarte relevantes:
    - Fecha de inicio de plazo legal.
    - Fecha de ingreso al Almacenador.
    - Plazos transcurridos fuera y dentro del Almacenador consistentes con las fechas.
    - Fecha de plazo legal.
    - Saldo de tiempo hasta el cumplimiento del plazo.
- Verificar disponibilidad y configuración de la aplicación o herramienta de borrado de información.
- Verificar disponibilidad y configuración de la aplicación o herramienta de borrado seguro.
- Verificar flujo de información confidencial hacia el borrado seguro.
- Si es posible, y si es pertinente según la complejidad de la operación, hacer forensia de borrado seguro confirmando que el algoritmo de borrado seguro es efectivo, en caso de aplicaciones no reconocidas.

9.0 Seguridad[9]

9.1 Análisis de riesgo en servicios críticos para terceros.

- El Almacenador debe contar con un documento de análisis de riesgos de su almacenamiento tecnológico para los servicios críticos a terceros
- El análisis de riesgos debe contener al menos:
    - Riesgos de continuidad del negocio
    - Riesgos de seguridad informática
    - Valoración de riesgos
- El análisis de riesgo de continuidad del negocio puede estar separado, por ejemplo, como parte del plan de continuidad de negocios
- Preferiblemente, el análisis de riesgos debería contener, adicionalmente:
    - Descripción o mención de la relación entre objetivos del servicio y los riesgos
    - Evidencia de gestión de riesgos

9.2 Análisis de riesgo en servicios no críticos para terceros o en servicios propios.

- En estos dos casos el impacto de los riesgos en terceros es bajo o nulo, por tanto, el estándar de documentación no debe ser mayor que el de negocios físicos y es mejor tratarlo como preferencia por buenas prácticas de negocio.
    - Esta documentación no es un requisito explícito en la reglamentación. Su relevancia o no para aprobar la auditoría debe depender del objetivo del servicio y contexto del Almacenador.
- Cuando el almacenamiento tecnológico participa en servicios no críticos para terceros, sí sería preferible contar con un análisis de riesgo documentado.
    - Para Almacenadores de gran escala, el contenido podría ser similar al caso para servicios críticos para terceros (sección 7.1).
- En cualquiera de los dos casos, servicios no críticos para terceros o esencialmente solo para el Almacenador, si el Almacenador no cuenta con un análisis de riesgo o no está documentado, sería preferible que contara al menos con un documento que identifique los principales riesgos de continuidad y de seguridad de información.

[9] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.9 Seguridad.

9.3 Plataforma de información en servicios críticos a terceros

- El Almacenador debería contar con una descripción de la arquitectura de seguridad de la plataforma de información.
- Debe contar con el detalle de la infraestructura que implementa esta arquitectura.
- Debe contar con inventario o lista de los activos considerados críticos, que incluya al menos canales de comunicación, dispositivos y aplicaciones.
- Debe contar con una especificación de los controles de seguridad en la arquitectura, incluyendo el esquema de control de acceso.
- Los controles de seguridad deben incluir mecanismos de trazabilidad de los eventos en la plataforma de información, por ejemplo, bitácoras, y su protección.
- Esta información previa puede estar en un solo documento o por separado.
- En caso de que la seguridad dependa de servicios tercerizados, el Almacenador debe contar con información sobre los controles de seguridad para el servicio tercerizado.

9.4 Plataforma de información en servicios no críticos a terceros.

- El Almacenador debería contar con una descripción de la arquitectura de seguridad de la plataforma de información.
- Debe contar con una descripción razonable de la infraestructura que implementa su arquitectura.
- Debería contar con inventario o lista de los activos considerados críticos, que incluya al menos canales de comunicación, dispositivos y aplicaciones.
- Debería contar con una especificación de los controles de seguridad en la arquitectura, incluyendo el esquema de control de acceso.
- Los controles de seguridad deberían incluir mecanismos de trazabilidad de los eventos en la plataforma de información, por ejemplo, bitácoras, y su protección.
- Esta información previa puede estar en un solo documento o por separado.
- En caso de que la seguridad dependa de servicios tercerizados, el Almacenador debería contar con información sobre los controles de seguridad para el servicio tercerizado.

9.5 Plataforma de información en almacenamiento esencialmente solo para Almacenador.

- El Almacenador debería contar con el detalle de la infraestructura que implementa esta arquitectura.
- Debería contar con una especificación de los controles de seguridad en la arquitectura, incluyendo el esquema de control de acceso.

9.6 Seguridad del área y equipos.

- El Almacenador debe contar con una descripción de las medidas de protección física del área y equipos.
- Los aspectos de protección física de disponibilidad del área y equipos pueden estar en el Plan de Continuidad de Negocios.
- Para almacenamiento tecnológico en servicios críticos para terceros, las medidas de protección física deben incluir medidas de control de acceso físico.

- Para almacenamiento tecnológico en servicios críticos para terceros, las medidas de protección física deben incluir medidas de vigilancia de acceso.

9.7 Confiabilidad (Assurance)

- Confiabilidad (Assurance) se refiere a la confianza en la implementación de los controles definidos y es el sujeto de los niveles de evaluación en la guía internacional Common Criteria (Evaluation Assurance Level).
    - El aspecto de confiabilidad no es un requisito explícito en la reglamentación, pero aún para Almacenadores que no son prestadores de servicio de almacenamiento digital a terceros, confiabilidad es una buena práctica, especialmente si el almacenamiento tecnológico participa en servicios críticos para terceros.
- Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, el Almacenador debería tener un informe de revisión de la implementación, que refleje el grado de cumplimiento con el diseño de la arquitectura (informe de confiabilidad de implementación).
    - El informe de implementación debería reflejar el apego de los controles implementados a las especificaciones.
    - En el caso de almacenamiento tecnológico que solo participa en servicios no críticos para terceros o que es esencialmente solo para el Almacenador, también es preferible que cuente con un informe de confiabilidad de implementación.
- Cuando el Almacenador no cuenta con un informe de confiabilidad de implementación, sería preferible que contara al menos con un documento que describa el proceso de implementación.
    - Por ejemplo, si fue contratada, quiénes implementaron, qué se les especificó y si hay constancia de entrega a satisfacción.

9.8 Gestión de seguridad.

- Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, el Almacenador debería contar con un sistema de gestión de seguridad de información.
- El esquema de gestión debería especificar:
    - La evidencia necesaria para demostrar la gestión.
    - Los responsables por la ejecución de la gestión a nivel de supervisión y a nivel operativo.
    - Un proceso de rendición de cuentas consistentes con el análisis de riesgo y la gobernabilidad del Almacenador.
- El esquema de gestión debería establecer:
    - Políticas de seguridad de la información.
    - Revisión de configuración de los ambientes computacionales.

- Revisión de la gestión de usuarios y privilegios de acceso.
- Revisión de la fortaleza y precisión de perímetros externos e internos.
- Proceso de control de cambios.
- Proceso de respaldo de información.
- Revisión de protección de información confidencial.
- Proceso de descarte de información o dispositivos.
- Vigilancia y gestión de incidentes de seguridad.

- En el caso de almacenamiento tecnológico en servicios no críticos para terceros, sería preferible que el Almacenador cuente con un sistema de gestión de seguridad de información. El contenido debería incluir

    - Los responsables por la ejecución de la gestión a nivel de supervisión y a nivel operativo.
    - Revisión de configuración de los ambientes computacionales.
    - Revisión de la gestión de usuarios y privilegios de acceso.
    - Proceso de respaldo de información.
    - Revisión de protección de información confidencial.
    - Proceso de descarte de información o dispositivos.

- En el caso de almacenamiento tecnológico en servicios esencialmente solo para el Almacenador, sería preferible que contara con un proceso documentado o al menos una descripción del proceso de gestión de seguridad de información. Sería preferible que el contenido incluyera.

    - Los responsables por la ejecución de la gestión a nivel de supervisión y a nivel operativo.
    - Proceso de respaldo de información.
    - Revisión de protección de información confidencial.
    - Proceso de descarte de información o dispositivos.

9.9 Recurso humano.

- El personal a cargo de los sistemas de información del Almacenador debe ser consistentes con la funcionalidad y seguridad que requiere la plataforma de información.
- El Almacenador puede tercerizar el recurso humano. Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, en ese caso la división de responsabilidades debería estar establecida en el equivalente a un acuerdo de nivel de servicios.
- En cualquiera de los casos, sea en servicios críticos a terceros, o servicios no críticos a terceros, o esencialmente solo para el Almacenador, este debe conocer suficiente sobre su recurso humano propio o sus proveedores para tener una confianza razonable que estos actuarán en forma responsable y competente.

9.10 Demostraciones de cumplimiento en servicios críticos para terceros.

- Verificar cuales de los diseños siguientes están documentados:

- El análisis de riesgo. Debe tenerlo.
- La arquitectura de seguridad. Debe tenerlo.
- La especificación de la infraestructura. Debe tenerlo.
- La especificación de los controles digitales y físicos. Debe tenerlo.

- Verificar que hay evidencia de confiabilidad de la implementación. Debería tenerlo.
- Hacer pruebas funcionales de una muestra de los controles de seguridad más críticos y confirmar su correcta implementación y funcionamiento.
- Evaluar si:
  - El análisis de riesgos es consistente con los objetivos del servicio.
  - El análisis de riesgos es consistente con el nivel de alcance, claridad y profundidad esperado en la industria.
  - El diseño de la arquitectura, la especificación de infraestructura y la especificación de controles digitales y físicos es consistente con el análisis de riesgos y la naturaleza de los activos críticos, con base en el estado del arte razonable para la operación.
  - El diseño de la arquitectura, la especificación de infraestructura y la especificación de controles digitales y físicos es consistente con el nivel de alcance, claridad y profundidad esperado en la industria, con base en el estado del arte razonable para la operación.
  - La evidencia de la confiabilidad de implementación se apega a la arquitectura, infraestructura y controles especificados, y si las posibles discrepancias encontradas son irrelevantes, subsanables o requieren reimplementaciones mayores fuera del alcance de la auditoría.

- Verificar que los diseños siguientes están documentados:
  - El sistema de gestión de seguridad. Debe tenerlo.
  - Políticas de seguridad, y si están oficialmente aprobadas en forma consistente con la gobernabilidad del Almacenador. Debe tenerlas.

- Verificar que hay evidencia o intención de acumular evidencia de la ejecución del sistema de gestión. Debe tenerlas.
- Evaluar si el sistema de gestión de seguridad de información:
  - Aclara responsabilidades.
  - Aclara el esquema de rendición de cuentas.
  - Aclara procesos o mecanismos de gestión.
  - Aclara las evidencias de la ejecución de estos procesos y responsabilidades.
  - Tiene procesos consistentes con la especificación de la arquitectura, infraestructura y controles de seguridad.

- Evaluar si los procesos o mecanismos de gestión son consistentes con:
  - Los objetivos del servicio y el contexto del Almacenador.
  - El análisis de riesgos.
  - El diseño de la arquitectura de seguridad.
  - Las especificaciones de la infraestructura y controles de seguridad.

- Verificar y analizar la documentación sobre el personal a cargo de la plataforma de información y del funcionamiento del servicio. Debe tenerla.
- Entrevistar a una muestra del personal a cargo, especialmente personal en puestos sensibles según el Decreto 24 de 29 de marzo de 2019, y evaluar si corresponden al grado de responsabilidad y competencia que requiere el servicio.
- Verificar y analizar la documentación sobre los proveedores de servicios tercerizados de cualquier funcionalidad crítica. Debe tenerla.
- Entrevistar a una muestra de proveedores de servicios tercerizados, especialmente los de reputación o historial menos conocido, y evaluar si corresponden al grado de responsabilidad y competencia que requieren sus servicios tercerizados.
- Evaluar si el conjunto de la arquitectura, con su infraestructura y controles implementados, el sistema de gestión de seguridad de información y el recurso humano, incluyendo elementos internos y tercerizados, son consistentes con:
    - Los objetivos del servicio
    - El análisis de riesgos
    - El contexto del Almacenador
    - Los recursos previsibles del Almacenador
- La sección de Medidas y Controles de este documento de referencia identifica ejemplos de buenas prácticas y de controles de seguridad de información.

9.11 Demostraciones de cumplimiento en servicios no críticos para terceros.

- Verificar que los diseños siguientes están documentados:
    - La especificación de la infraestructura. Debe tenerla.
    - La especificación de los controles digitales y físicos. Debería tenerla.
- Verificar que hay evidencia de confiabilidad de la implementación.
- Hacer pruebas funcionales de una muestra de los controles de seguridad más críticos y confirmar su correcta implementación y funcionamiento.
- Evaluar si:
    - El diseño de la arquitectura, la especificación de infraestructura y la especificación de controles digitales y físicos es consistente con el nivel de alcance, claridad y profundidad esperado en la industria, con base en el estado del arte razonable para la operación.
- Verificar que los diseños siguientes están documentados:
    - El sistema de gestión de seguridad. Debe tenerlo.
    - Políticas de seguridad. Es preferible tenerlas.
- Evaluar si el sistema de gestión de seguridad de información:
    - Aclara procesos o mecanismos de gestión.

- Aclara las evidencias de la ejecución de estos procesos y responsabilidades.
- Tiene procesos consistentes con la especificación de la arquitectura, infraestructura y controles de seguridad.

- Verificar y analizar la documentación sobre el personal a cargo de la plataforma de información y del funcionamiento del servicio. Debe tenerla.
- Entrevistar a una muestra del personal a cargo, especialmente personal en puestos sensibles según el Decreto 24 de 29 de marzo de 2019, y evaluar si corresponden al grado de responsabilidad y competencia que requiere el servicio.
- Verificar y analizar la documentación sobre los proveedores de servicios tercerizados de cualquier funcionalidad crítica. Es preferible tenerla.
- Entrevistar a una muestra de proveedores de servicios tercerizados, especialmente los de reputación o historial menos conocido, y evaluar si corresponden al grado de responsabilidad y competencia que requieren sus servicios tercerizados.
- Evaluar si el conjunto de la arquitectura, con su infraestructura y controles implementados, el sistema de gestión de seguridad de información y el recurso humano, incluyendo elementos internos y tercerizados, son consistentes con:
  - Los objetivos del servicio
  - El análisis de riesgos, si lo tiene.
  - El contexto del Almacenador
  - Los recursos previsibles del Almacenador
- La sección de Medidas y Controles de este documento de referencia identifica ejemplos de buenas prácticas y de controles de seguridad de información.

9.12 Demostraciones de cumplimiento en servicios esencialmente solo para Almacenador.

- Verificar que los diseños siguientes están documentados:
  - La especificación de la infraestructura. Debe tenerla.
  - La especificación de los controles digitales y físicos. Debería tenerla.
- Verificar que hay evidencia de confiabilidad de la implementación.
- Hacer pruebas funcionales de una muestra de los controles de seguridad más críticos y confirmar su correcta implementación y funcionamiento.
- Evaluar si:
  - El diseño de la arquitectura, la especificación de infraestructura y la especificación de controles digitales y físicos es consistente con el nivel de alcance, claridad y profundidad esperado en la industria, con base en el estado del arte razonable para la operación.
- Verificar que los diseños siguientes están documentados:
  - El sistema de gestión de seguridad. Debe tenerlo.

- Verificar y analizar la documentación sobre el personal a cargo de la plataforma de información y del funcionamiento del servicio. Debe tenerla.
- Entrevistar a una muestra del personal a cargo, especialmente personal en puestos sensibles según el Decreto 24 de 29 de marzo de 2019, y evaluar si corresponden al grado de responsabilidad y competencia que requiere el servicio.
- Evaluar si el conjunto de la arquitectura, con su infraestructura y controles implementados, el sistema de gestión de seguridad de información y el recurso humano, incluyendo elementos internos y tercerizados, son consistentes con:
    - Los objetivos del servicio
    - El análisis de riesgos, si lo tiene.
    - El contexto del Almacenador
    - Los recursos previsibles del Almacenador
- La sección de Medidas y Controles de este documento de referencia identifica ejemplos de buenas prácticas y de controles de seguridad de información.

10.0 Confidencialidad[10]

10.1 Sistema de gestión de documentos.

- Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, debe contar con un sistema de gestión de documentos o con un proceso documentado capaz de identificar al menos dos niveles de confidencialidad de un documento, con cualesquiera términos apropiados:
    - Confidencial.
    - No-confidencial.
- Cuando el almacenamiento tecnológico participa en servicios no críticos para terceros, debe contar con un proceso documentado capaz de identificar al menos dos niveles de confidencialidad de un documento, con cualesquiera términos apropiados: Confidencial y No-confidencial.
- Cuando el almacenamiento tecnológico es esencialmente solo para el Almacenador, es preferible contar al menos con un proceso documentado capaz de identificar al menos dos niveles de confidencialidad de un documento, con cualesquiera términos apropiados: Confidencial y No-confidencial.

[10] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.10 Confidencialidad.

10.2 Mecanismo de protección de confidencialidad.

- En los casos de servicios críticos o no críticos para terceros, el Almacenador debe haber definido cómo un cliente o el propio Almacenador declaran el nivel de confidencialidad de un documento.
- Los controles de seguridad deben incluir controles de protección de confidencialidad de documentos o metadatos en tránsito y en reposo, para los casos en que haga falta.
- Debe haber un proceso y mecanismos de control de acceso a información confidencial.
- Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, debe contar con una política de protección de información confidencial.
- Cuando el almacenamiento tecnológico participa en servicios no críticos para terceros, debería contar con una política de protección de información confidencial.
- Cuando el almacenamiento tecnológico es esencialmente solo para el Almacenador, sería preferible contar con una política de protección de información confidencial.
- Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, los controles o mecanismos de trazabilidad de eventos deben ser capaces de identificar claramente los momentos, sujetos, acciones y objetos en los eventos de acceso a información confidencial.

10.3 Demostraciones de cumplimiento.

- Verificar que los elementos siguientes están documentados:
    - Política de protección de información confidencial, según el tipo de servicio en que participa el almacenamiento tecnológico.
    - Descripción del proceso de designación de niveles de confidencialidad de documentos.
    - Descripción del proceso de designación de control de acceso a información confidencial.
- Verificar si el análisis de riesgos, si existe, aclara los riesgos de violación a la confidencialidad de información.
    - Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, debería aclararlos.
- Comprobar que el sistema de gestión documental o el proceso de manejo de información confidencial es capaz de implementar el proceso de designación de niveles de confidencialidad y control de acceso a información confidencial.
- Verificar que la especificación de la arquitectura, infraestructura y controles de seguridad especifican controles de protección de información confidencial consistentes con el análisis de riesgos, tanto para documentos o metadatos en tránsito como en reposo, según sea el caso.
- Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, verificar la evidencia de confiabilidad de la implementación de los controles de protección de información confidencial.

- En las pruebas funcionales de una muestra de los controles de seguridad, incluir pruebas de los controles de protección de información confidencial, tanto en tránsito como en reposo, para confirmar su correcta implementación y funcionamiento.
- Verificar que los mecanismos de trazabilidad de eventos relacionados con información confidencial funcionan.
    - Cuando el almacenamiento tecnológico participa en servicios críticos para terceros, verificar que aclaran los momentos, sujetos, acciones y objetos de los eventos.

11.0 Documentación administrativa[11]

- El Almacenador debe contar con la siguiente documentación administrativa:
    - Constancia de contar con una firma electrónica calificada
    - Títulos académicos, certificados de entrenamiento o diplomas de cursos del recurso humano con responsabilidades en el servicio de almacenamiento tecnológico. Estas calificaciones deben ser evaluadas en función de los roles del personal.
    - Plan de control de calidad de los procesos de preservación del nivel de fidelidad adecuado, tanto en captura como en presentación.
    - Nombre del Jefe de archivos u oficina que ostenta la custodia de los documentos almacenados tecnológicamente.
    - Descripción de las instalaciones físicas que correspondan al servicio de almacenamiento tecnológico.
    - Registro a la fecha de las auditorías efectuadas al sistema de almacenamiento tecnológico, fechas en que fueron realizadas, constancia de registros o sus renovaciones ante la Dirección General de Comercio Electrónico y si alguna vez el registro ha sido revocado o suspendido.
    - Declaración de prácticas de almacenamiento tecnológico con las informaciones solicitadas en el Artículo 47 de la Ley 51 de 2008
- La siguiente documentación ya está contemplada en la verificación de cumplimiento de requisitos técnicos
    - Documentación que acredite que los estándares técnicos utilizados cumplen con los requisitos técnicos mínimos de almacenamiento tecnológico. Esta auditoría, de ser aprobada, es equivalente a dicha acreditación independientemente de otras acreditaciones disponibles o ausencia de ellas.
    - Especificaciones técnicas de software y/o hardware involucrados en el proceso de digitalización.
- La siguiente documentación no es verificada por esta auditoría, pero debe ser entregada a la Dirección General de Comercio Electrónico:
    - Poder y solicitud de registro mediante abogado.

[11] Resolución No. 1 del 5 de febrero de 2020 (MICI). 5. Garantías Mínimas para el Almacenamiento Tecnológico de Documentos.5.11 Documentación administrativa.

- Certificación del Registro Público (no más de tres meses de expedida), en la cual conste el nombre de la sociedad, representante legal, directores, dignatarios, apoderados, capital social y vigencia.
- Fotocopia de la cédula o pasaporte del solicitante y del representante legal si es una persona jurídica.
- Resultado final de esta auditoría, entregado a la Dirección General de Comercio Electrónico directamente por los auditores.
- Nota: algunas de las solicitudes de documentación en esta sección pueden haber entrado en contradicción actualmente con la Ley 144 de 2020 que exige que las instituciones públicas no soliciten información que ya se encuentre en posesión del gobierno.