DOCUMENTO DE REFERENCIA PARA AUDITO

REGISTRO DE PRESTADORES DE SERVICIOS (ALMACENAMIENTO DE TERCEROS)

INTRODUCCION

La presente referencia tiene como sustento el marco legal la Resolución No. 1 de 5 de febrero de 2020 de la Dirección General de Comercio Electrónico (Gaceta No.). En particular, este documento sirve como referencia para la metodología y medidas a evaluar en una auditoría o evaluación de un prestador de servicios de almacenamiento tecnológico para terceros, 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 No. 51 de 22 de julio de 2008 modificada por la Ley No. 82 de 9 de noviembre de 2012 para almacenamiento tecnológico con validez legal y su reglamentación. Para cada requisito que se le exige cumplir a un PRESTADOR, 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 el principio de neutralidad tecnológica que exige la Ley No. 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 la oferta legal de servicios del PRESTADOR, el estado del arte actual y previsto de la tecnología y el contexto específico del PRESTADOR.

El esquema de auditoría y evaluación técnica en este documento es solo una referencia para cumplir. No es obligación seguir el presente documento ya que puede haber razones válidas para desviarse de la metodología o medidas planteadas en esta referencia, en tal caso deberá de anotarse en el informe de auditoría.

El no seguir esta referencia ni desviarse de ella EXIME AL AUDITOR AUTORIZADO de la responsabilidad de utilizar su conocimiento y criterio para evaluar si el PRESTADOR demuestra el alistamiento, capacidad e intención de cumplir con los requisitos que exige la Ley, las normativas y con la expectativa de proteger el interés de sus clientes y usuarios durante el periodo proyectado hasta la siguiente auditoría.

EVALUACION TECNICA Y AUDITORIA

1. Integridad de los documentos almacenados

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

- El depósito debe estar claramente definido.

- El Prestador debe utilizar una firma electrónica calificada como garantía de integridad del documento y sus metadatos en el depósito; es decir, para la llamada información en reposo.
- 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 y sus metadatos asociados.

1.2. Firma electrónica digital criptográfica para documento en tránsito

- El punto de ingreso al sistema de almacenamiento tecnológico debe estar claramente definido.
- El Prestador debe utilizar una firma criptográfica como garantía de integridad del documento y sus metadatos en tránsito.
- 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 Prestador 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.
    - 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 y sus metadatos asociados.
- 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 Prestador 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.

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 Prestadores 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. El Prestador puede utilizar otros mecanismos en situaciones o contextos justificados.
- 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 deben representar un grado de rendición de cuentas y trazabilidad de alto nivel.
- 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.
- 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 Prestador puede separar las responsabilidades de ingreso o captura de documentos de las responsabilidades de control sobre el sistema de firmas.
  - El Prestador 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.

2. Fidelidad de presentación

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).
- 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 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.
- El acuerdo de nivel de servicio (SLA) con el cliente debe decir claramente los parámetros de fidelidad de captura.
- 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 Prestador desea aplicar compresión, esta debe ser sin pérdida y darse después de aplicar la firma criptográfica.
  - 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

- El SLA con el cliente debe decir claramente los parámetros de fidelidad de presentación.
  - 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.

- El SLA con el cliente debe incluir las opciones de presentación de los documentos almacenados que le pertenecen o a los que tiene acceso.
  - El SLA debe indicar las opciones de formatos de presentación para documentos digitalizados para los distintos tipos de información, por ejemplo, PDF, familia Microsoft Office, familia Mac, familia Open Source, JPG, MPEGx, .wav, otros).
  - Si el Prestador no pone a disposición un formato común en el mercado, debe alertar al cliente en el SLA.
  - El SLA debe indicar que tipo de sustrato electrónico puede o debe usar el cliente para recuperar el documento, por ejemplo, USB, CD, navegador.
  - Un Prestador 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.
  - Sin embargo, su SLA debe especificar qué facilidades y servicios de presentación estarán disponibles para consultas o recuperación de documentos por el cliente.
- Para material impreso digitalizado, la geometría del material original debe poder ser identificable y reproducible.
- Si el SLA contempla la posible presentación del documento en las facilidades del prestador de servicios para consulta con validez legal, los dispositivos de presentación deben ser consistentes con los formatos y parámetros anunciados en el SLA, incluyendo parámetros de geometría.
- Un interesado autorizado debe poder reproducir un documento impreso digitalizado con la geometría original si posee los dispositivos tecnológicos adecuados.
- Para documentos de aplicaciones especializados, 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 demostrados con documentos de prueba o documentos recientes de cada tipo de información aceptado por el prestador de servicios por ejemplo impreso, audio, video.
- Revisar el SLA con los clientes y confirmar que especifica los formatos y parámetros de fidelidad de captura, almacenamiento y presentación.
- 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 SLA 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 es consistente con los parámetros mínimos de fidelidad aceptables en la industria para el tipo de información.
- Verificar la facilidad y tiempos de acceso mediante los mecanismos de consulta o recuperación de documentos indicados en el SLA es razonable según la expectativa de servicio en el mercado, por ejemplo, por internet o en dispositivos de presentación en las facilidades del Prestador.
    - La expectativa contemporánea es que los documentos estén disponibles 24x7x365 por internet con base en credenciales de acceso del cliente sin intervención manual del Prestador, con un porcentaje de disponibilidad anual aceptable en la industria.

3. Registro de tiempo

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.
    - 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 Prestador 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.

4. Uso de metadatos

4.1. Preservación y presentación de Metadatos

- El Prestador 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 cliente 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 Prestador debe incluir los metadatos obligatorios especiales que exija la ley o los reglamentos aplicables.
- El Prestador puede incluir metadatos de interés adicionales para si o para su cliente, por ejemplo, el nombre del documento, referencia del cliente, palabras claves o descripción breve del contenido.

4.2. Presentación de metadatos

- El Prestador 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.
- Si el SLA contempla la posible presentación del documento almacenado en las facilidades del Prestador, 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 contemplado en el SLA.
- 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 contemplado en el SLA.
- Verificar los formatos y validez de los metadatos de los documentos para cada tipo de medio de información contemplado en el SLA.
- Evaluar el riesgo de que el sistema de manejo de metadatos pudiera perder en forma irrecuperable la asociación entre metadatos y sus documentos correspondientes.

5. Reproducción / Exportación

Este requerimiento está cubierto en la sección de fidelidad de presentación.

6. Respaldo

6.1. Plan de continuidad de negocios

- Como prestador de servicios a terceros, el Prestador 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 Prestador 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)

6.2. Plan de recuperación

- 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

6.3. Gestión de alistamiento y pruebas de recuperación

- Si el Prestador ha estado operando al menos por un año, debe mostrar evidencia de ejecución de los procedimientos de alistamiento para emergencia.
- Si el Prestador ha estado operando al menos por un año, debe mostrar evidencia de ejecución de las pruebas de recuperación.

6.4. Demostraciones de cumplimiento

- 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.

7. Jefe de archivo

7.1. Designación

- El Prestador debe designar oficialmente a un jefe de archivo, responsable por la operación de almacenamiento tecnológico.

7.2. Responsabilidades definidas

- El Prestador 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 de supervisión ejecuta el jefe de archivos.

7.3. Relación con la firma calificada

- El Prestador 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 Prestador debe especificar si el jefe de archivo 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.

8. Tiempo de conservación

8.1. Sistema de gestión de documentos

- El Prestador 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 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.
- Debe tener un proceso de gestión de plazos que permita responder al cliente 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 Prestador 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. Mecanismo de descarte

- Debe tener un proceso de aprobación de descarte de documentos claros para cuando lo solicite un cliente o se cumplan las condiciones de descarte según el SLA.
- Debe borrar la información de los documentos de terceros cuando se da su descarte.
- Debe poder aplicar borrado seguro a información confidencial descartada.
- Debe entregar al cliente notificación del descarte final de la documentación.

8.3. 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:
  - Fecha de inicio de plazo legal.
  - Fecha de ingreso al Prestador.
  - Plazos transcurridos fuera y dentro del Prestador 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, hacer forensia de borrado seguro confirmando que el algoritmo de borrado seguro es efectivo, en caso de aplicaciones no reconocidas.

9. Seguridad

9.1. Análisis de riesgo

- El Prestador debe contar con un documento de análisis de riesgos de su operación de servicios de almacenamiento tecnológico 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. Plataforma de información

- El Prestador debe 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.
- 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 Prestador debe contar con información sobre los controles de seguridad para el servicio tercerizado.

9.3. Seguridad del área y equipos

- El Prestador 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.
- Las medidas de protección física deben incluir medidas de control de acceso físico.
- Las medidas de protección física deben incluir medidas de vigilancia de acceso.

9.4. Confiabilidad (Assurance)

- El Prestador debería tener un informe de revisión de la implementación, que refleje el grado de cumplimiento con el deseño de la arquitectura.
- El informe de implementación debería reflejar el apego de los controles implementados a las especificaciones.

9.5. Gestión de seguridad

- El Prestador debe contar con un sistema de gestión de seguridad de información.
- El esquema de gestión debe 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 Prestador.
- 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.

9.6. Recurso humano

- El personal a cargo de los sistemas de información del Prestador debe ser consistentes con la funcionalidad y seguridad que requiere la plataforma de información.
- El Prestador puede tercerizar el recurso humano. En ese caso, la división de responsabilidades debe estar establecida en el equivalente a un acuerdo de nivel de servicios.
- El Prestador debe conocer suficiente sobre su recurso humano propio o sus proveedores para tener una confianza razonable que estos actuarán en forma responsable y competente.

9.7. Demostraciones de cumplimiento

- Verificar que los diseños siguientes están documentados:

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

- 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 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.
  - Políticas de seguridad, y si están oficialmente aprobadas en forma consistente con la gobernabilidad del Prestador.
- Verificar que hay evidencia o intención de acumular evidencia de la ejecución del sistema de gestión.
- 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 Prestador.
  - 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.
- 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.
- 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 Prestador
  - Los recursos previsibles del Prestador
- La sección de Medidas y Controles de este documento de referencia identifica ejemplos de buenas prácticas y de controles de seguridad de información.

10. Confidencialidad

10.1. Sistema de gestión de documentos

- El Prestador debe contar con un sistema de gestión de documentos capaz de identificar al menos dos niveles de confidencialidad de un documento, con cualesquiera términos apropiados:
  - Confidencial.
  - No-confidencial.

10.2. Mecanismo de protección de confidencialidad

- El Prestador debe contar con una política de protección de información confidencial.
- Debe haber definido cómo un cliente o el propio Prestador 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.
- 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.
  - Descripción del proceso de designación de niveles de confidencialidad de documentos.
  - Descripción del proceso de designación de control de acceso a información confidencial.
- Verificar que el análisis de riesgos aclara los riesgos de violación a la confidencialidad de información.
- Comprobar que el sistema de gestión documental 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.
- 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 y aclaran los momentos, sujetos, acciones y objetos de los eventos.

11. Documentación administrativa

- El Prestador 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 en los procesos de preservación de nivel de fidelidad adecuados.
  - 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.
  - 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.
  - Estados financieros según define el Decreto Ejecutivo 24 de 2019 Artículo 19, numeral 10.
  - Póliza de responsabilidad civil según define el Decreto Ejecutivo 24 de 2019 Artículo 19, numeral 11.
  - Declaración del solicitante indicando que se compromete a cumplir con las obligaciones que define el Artículo 55 de la Ley 51 de 2008.
  - Comprobante de pago de la tasa de registro de la DGCE.

MEJORES PRACTICAS Y CONTROLES CONOCIDOS A APLICAR SEGÚN LAS CIRCUNSTANCIAS

INTRODUCCION

Presentamos una guía práctica donde se enumeran y explican algunos factores que deben contemplarse al evaluar la calidad de un centro de almacenamiento tecnológico.

La evaluación de un Centro de Almacenamiento Tecnológico no puede medirse con una lista de verificación (checklist). Deben contemplarse factores humanos, factores administrativos, factores técnicos, factores económicos y factores físico-ambientales. Existen muchos grises y no tantos blancos y negros. La evaluación debe tener presente que cuando mides la fuerza de una cadena, el eslabón más débil es quién define su fortaleza.

Contrario a los parámetros de Ingeniería, en *Sistemas Informáticos* cumplir con una función no significa éxito. La métrica de *Sistemas Informáticos* da un alto valor al CÓMO se logra y al concepto de relevo. Similar a una carrera de relevo, la gerencia informática tiene éxito a la medida que opere contemplando el próximo pase de bastón. Las operaciones deben ser claras, bien definidas, y ningún individuo debe mantener feudo tecnológico. El conocimiento debe ser compartido, la organización debe insistir en la capacitación del personal de menos experiencia bajo la guia de personal más capacitado.

Es la responsabilidad de la Gerencia Central supervisar la gestión de la Gerencia Informática, pero el poder de decisión en temas informáticos es de la Gerencia Informática, las otras gerencias carecen del conocimiento técnico para evaluar sus decisiones. En cierto sentido, el Gerente Informático es rey en su feudo. El audito es un mecanismo que debe utilizar la Gerencia Central para conocer y medir el funcionamiento informático de la organización. Una organización de buenas prácticas entiende la importancia de contratar un buen auditor externo, imparcial y objetivo. El auditor debe siempre entender que su lealtad reside con la organización, aunque en muchos casos quién lo contrata es el Gerente Informático. Los informes del auditor externo deben ser objetivos y veraces, enfrenta penalizaciones económicas, cargos civiles y cargos penales.

La relación de un auditor con la Gerencia Informática debe ser positiva pero distante, carente de fraternidad. Un buen audito es objetivo y crítico en sus hallazgos, define vulnerabilidades, evita incidentes y conduce a un mejoramiento en el nivel de servicio.

El auditor debe presentar informe considerando criterios de documentación, eficiencia, rendimiento, adecuación de recursos de presupuesto, de recurso humano, de seguridad y de espacios físicos. **El auditor debe ser enérgico y no debe tolerar la falta de cumplimiento de los hallazgos del previo informe de auditoría.** El auditor considera cada uno de los 16 puntos definidos a continuación, sustenta su análisis, define y cataloga las faltas encontradas, señala las vulnerabilidades que continúan sin corregir desde el último audito, y concluye aprobando o enumerando las correcciones necesarias para cumplir con el mandato legal de la DGCE.

PRACTICAS Y CONTROLES

1. Seguridad Física y Ambiental

El propósito es evaluar la seguridad de acceso y protección física, y protección ambiental de servidores, equipos de seguridad de redes y unidades de almacenamiento enterprise. A continuación, algunos puntos a considerar.

1.1. Área Segura

❑Seguridad física

- ❑ ¿Quién es la persona responsable de la seguridad del área?
- ❑ ¿Existe un perímetro o barrera física que protege el hardware de ataques desde el exterior o interior del edificio?
- ❑ ¿El acceso al área está restringido? ¿siempre cerrado bajo cerradura?
- ❑ ¿El acceso al área está controlada por alarma?
- ❑ ¿Se utiliza un control de acceso electrónico para entrar al área?
- ❑ ¿El control de acceso es por individuo y genera un LOG auditable?
- ❑ ¿El área mantiene cámaras que graban y tienen disponible por lo menos siete días de grabaciones?
- ❑ ¿El área mantiene cámaras que son monitoreadas para detectar irregularidades en el acceso al área?
- ❑ ¿Cuál es el procedimiento que define como trabajar en el área segura?

❑Seguridad ambiental

- ❑ ¿El área segura tienen temperatura ambiental adecuada?
- ❑ ¿El área segura tiene control de humedad adecuado?
- ❑ ¿El área segura tiene o tuvo problemas de filtración de agua?

1.2. Equipos de Redes

❑ Los equipos deben estar protegidos de acceso por personal no autorizado.

❑ El cableado de redes debe estar protegido de intercepción, daños ambientales o daños físicos.

❑ El cableado de redes debe cumplir con los requerimientos técnicos, calidad de cableado. Cada vez que se instalan cables de redes, ¿se ha certificado el cableado?

1.3. Electricidad

Servidores, Equipos de Seguridad de Redes y Unidades de Almacenamiento Enterprise.

❏ ¿Existe más de un proveedor? ¿Hay redundancia?

❏ ¿Existe una planta eléctrica de respaldo?, ¿Está en buenas condiciones?

❏ ¿La planta eléctrica entra en línea automáticamente?

❏ ¿El cableado eléctrico desde el punto donde entra a la edificación hasta dónde llega a los equipos es de buena calidad? ¿La instalación de las cajas de fusibles (breakers) es de buena calidad?

2. Recurso Humano

2.1. Auditor externo

Para salvaguardar la integridad de los informes, habrá una rotación de auditor. El Prestador de Servicios de Almacenaje no podrá utilizar al mismo auditor o empresa de auditores consecutivamente, lo podrá volver a contratar cada tres años.

Para salvaguardar la imparcialidad de los informes, no podrá existir un nexo familiar entre (a) el auditor, propietarios o gerentes de la empresa de auditoría, y (b) los propietarios, gerentes, o personal de informática de la organización a auditar. El nexo familiar incluye tanto al nexo del individuo como al nexo de su familia inmediata. Por ejemplo, existe un nexo familiar si la esposa/hijo/padre/abuelo del propietario de la empresa de auditoría es prima/hermana de la esposa/hijo/padre/abuelo del propietario de la organización a auditar.

2.2. Profesionalismo

La organización requiere de personal poseedor de dos distintas habilidades para el buen funcionamiento del *Centro de Almacenamiento* .

La primera habilidad es el profesionalismo administrativo del liderazgo, el uso de buenas prácticas. Un bajo nivel administrativo se evidencia con la presencia de feudos, contratos de mantenimiento expirados, contratos de soporte técnico expirados, licencias expiradas, ...

La segunda es el profesionalismo técnico del liderazgo y del personal. Un bajo nivel técnico concluye en malas decisiones estratégicas y sobrecostos cuantificados en los contratos de servicios. El CHIEF ENTERPRISE ARCHITECT tiene que poseer un alto nivel técnico, un alto nivel administrativo no es calificativo para este cargo.

Al ejecutar la evaluación no solo se debe considerar la calificación del personal, sino también su ejecución. Es decir, no solo si el personal tiene los diplomas que sustenta que es un profesional, si no también si domina las funciones técnicas de su día a día.

Una buena administración verifica el cumplimiento de sus procedimientos y mantiene al personal conocedor de sus políticas y procedimientos a través de seminarios y cursos.

2.2.1. Evaluación administrativa del liderazgo

❑ Educación Administrativa (PMI, MBA, …)
❑ Universidad, Nombre de Diploma
❑ Diplomados Administrativos
❑ Certificaciones Administrativas: emisor, horas, tema
❑ Educación Informal considerada de mediano o alto nivel
❑ Experiencia, considerando el éxito o fracaso de sus pasadas experiencias.
❑ ¿El liderazgo es competente en su función?

2.2.2. Evaluación técnica del personal, incluyendo el liderazgo técnico

❑ Educación en Sistemas Informáticos
    ❑ Universidad, Nombre de Diploma
    ❑ Diplomados en Sistemas Informáticos
    ❑ Certificaciones en Sistemas Informáticos, siempre y cuando la persona sea conocedor y competente en la materia
❑ Educación Informal considerada de mediano o alto nivel
❑ Experiencia, trayectoria técnica, que hizo, que sabe hacer.
❑ ¿El personal es competente en su función?

2.2.3. Evaluar si el personal ha sido instruido en las Políticas de la organización

❑ ¿Cómo se verificó que el personal aprendió y conoce las políticas de la organización?

El personal es conocedor de

    ❑ Políticas de Uso
    ❑ Políticas de Seguridad
    ❑ Políticas de Seguridad Informática incluyendo vulnerabilidades de Ingeniería Social

❑Marco Legal de

    ❑ Almacenamiento
    ❑ Privacidad y Protección de Datos Personales
    ❑ Firma Electrónica y Digitalización de la Información
    ❑ La protección física y uso exclusivo del *Dispositivo Seguro para la Creación de Firma Electrónica*

2.2.4. La organización tiene asignadas las siguientes funciones

❑ Jefe de Archivo
❑ Encargado de cada Servidor

- ❑ Encargado de UPDATES a servidores
- ❑ Encargado de Seguridad
- ❑ Encargado de Auditar Seguridad
- ❑ Encargado de Almacenaje
- ❑ Encargado de Auditar Almacenaje
- ❑ Encargado de los equipos de seguridad de redes
- ❑ Encargado de UPDATES a cada software crítico o de seguridad
- ❑ Encargado de cada unidad de almacenamiento enterprise
- ❑ Encargados de BACKUP
- ❑ Encargado de cada DB-software
- ❑ Encargado de Seguridad de Redes
- ❑ Encargado de Monitoreo y análisis de Riesgos y Vulnerabilidades
- ❑ Encargado de Monitoreo y análisis de SIEM
- ❑ Encargado de Monitoreo y análisis de AUDIT-LOG de DATOS
- ❑ Encargado de Monitoreo y análisis de SCAP / STIG
- ❑ Encargado de Monitoreo y análisis de BUGTRAQ
- ❑ Encargado de Monitoreo y análisis de BASELINES de sistemas
- ❑ Encargado de Monitoreo y análisis de BASELINES de equipos de redes y seguridad

3. Hardware

El Inventario del HARDWARE debe mantenerse asociado al Inventario de SOFTWARE. Ambos inventarios deben mantenerse actualizados. Todo equipo debe tener físicamente su etiquetado de inventario (TAG), conociéndose su ubicación, jurisdicción y costo. Esta información básica es requerida por temas contables. Debemos conocer especificaciones del HARDWARE para comprender el nivel de seguridad de redes, el rendimiento de los equipos y la vulnerabilidad a fallas. Recomendamos la utilización de herramientas enterprise tipo ASSET MANAGEMENT.

3.1. Seguridad de redes

La carencia de un completo conocimiento actualizado de todo equipo que se conecta a la RED indica una vulnerabilidad a la seguridad. No se puede proteger lo que no se conoce.

Se debe conocer y evaluar la calidad de los equipos de seguridad de redes, los firewalls, los equipos SIEM (SIEM HARDWARE), la seguridad Wi-Fi, los switches con capacidad de microsegmentación o capacidad de server load, o capacidad de POLICY-BASED SWITCHING, …

3.2. Rendimiento - Performance

3.2.1. COMUNICACIÓN

La capacidad de los equipos de comunicación debe conocerse entre

❏ servidores

❏ servidores y las unidades de almacenamiento externa

❏ servidores y la LAN

❏ servidores y la WAN / INTERNET

3.2.2. CPU

La capacidad de un CPU no se define con la velocidad del reloj (medida en GHz), la familia (por ejemplo intel i9), o la generación a la cual un CPU pertenece. Utilizar tales métricas impide la comparación entre familias o fabricantes de procesadores. La única métrica es benchmarks.

Cuando un software ejecuta, utiliza 1 CORE del CPU, por tanto el rendimiento del software depende del poder computacional de 1 CORE, llamado SINGLE THREAD BENCHMARK. También debemos saber cuántos COREs requiere el software para brindar capacidad de servicio. Primero decides el poder computacional requerido, el SINGLE THREAD BENCHMARK, y luego, dependiendo del nivel de servicio, decides la cantidad de COREs requeridos.

Problemas de rendimiento ocurren cuando el SINGLE THREAD BENCHMARK es bajo, o cuando existen pocos COREs para el nivel de capacidad de servicio requerido. También debe considerarse cómo el fabricante de software define su costo. Si el fabricante define el costo del software por la cantidad de COREs, se desperdicia mucho dinero:

❏Al utilizar un CPU de bajo SINGLE THREAD BENCHMARK que utiliza muchos COREs para mantener un nivel de servicio.

❏Cuando el CPU tiene muchos COREs disponibles pero el nivel de servicio requiere de pocos.

3.2.3. RAM / SSD / HDD

El poder computacional de cada servidor o la velocidad de las unidades de almacenamiento enterprise están directamente influenciadas por

❏ RAM - La carencia de RAM degrada el sistema y lo lleva a un ciclo de PAGINACIÓN (hard PAGE-FAULTS). También es importante saber la velocidad del RAM (DDR2-800, DDR3-1600, DDR4-25600, ..)

❏ SSD - la utilización de memoria SSD para mejorar la velocidad de PAGINACIÓN. Existen grandes variantes de rendimiento entre las tecnologías SATA, y las diversas generaciones de PCIe (PCIe gen 2, gen 3, gen 4, ..).

❏ HDD con sus variantes de RPM y sus variantes de interface (Sata, SCSI, SAS, ..)

Se puede medir y comparar la velocidad de los SSD/HDD utilizando herramientas de benchmark. Esta información puede ser utilizada para identificar cuellos de botellas (bottlenecks) o la necesidad de tecnologías de mejor rendimiento.

3.3. Alta Disponibilidad - Vulnerabilidades

Para asegurar la disponibilidad de los servicios deben conocerse

❏ GARANTÍA. En caso de existir algún problema físico, el equipo está bajo garantía para ser reparado.

❏ END-OF-LIFE. El equipo pasó su vida útil y el fabricante no garantiza la disponibilidad de repuestos. Equipo tiene que ser desechado.

❏ ON-LINE UPS. La calidad de la electricidad puede vulnerar los equipos, la tecnología ON-LINE elimina la posibilidad de daños originados por la calidad eléctrica. Solamente este tipo de tecnología debe ser utilizada en Servidores, Unidades de Almacenamiento Enterprise y Equipos de Seguridad de Redes.

3.4. Inventario de Activos

El inventario de activos es requerido por el sistema contable de la organización y es necesario para el mantenimiento y para optimizar el nivel de servicio (rendimiento) y costo.

Un inventario de activos que conoce pocas características de los equipos cumple con el propósito contable, pero impide el análisis para mejorar rendimiento y costos.

Para todos los equipos, se debe conocer el TAG de inventario, costo, fabricante, modelo, nivel de firmware, MAC, IP, nivel de software, expiración de garantía, empresa encargada de mantenimiento preventivo, expiración de contrato de mantenimiento, expiración de acceso a updates, end-of-life (eol), end-of-service-life (eosl) y la unidad UPS ON-LINE asociada al equipo.

A continuación, características útiles a conocer:

3.4.1. Servidores, Desktops, Laptops, Tabletas

❏ Procesador - CPU SINGLE THREAD benchmark

❏ Procesador - Cantidad de COREs

❏ RAM - slots vacios

❏ RAM - capacidad utilizada en cada slot

❏ RAM - capacidad máxima por slot

❏ HDD / SSD - capacidad de cada uno

❏ HDD / SSD - interface / velocidad de cada uno

❏ HDD / SSD - disponibilidad de expansión

❏ Tipo de interface a unidad de almacenamiento externa

❏ TARJETA DE REDES - velocidad

❏ MANTENIMIENTO PREVENTIVO - fecha

3.4.2. UPS

❏ Capacidad en VA (volt-ampere)

❑ Fecha de reemplazo de garantía
❑ MANTENIMIENTO PREVENTIVO - fecha

3.4.3. Unidades de Almacenamiento Externo

❑ Surface Test - fecha
❑ S.M.A.R.T. Test - fecha
❑ RAM - slots vacios
❑ RAM - capacidad utilizada en cada slot
❑ RAM - capacidad máxima por slot
❑ HDD / SSD - capacidad de cada uno
❑ HDD / SSD - interface / velocidad de cada uno
❑ HDD / SSD - disponibilidad de expansión
❑ Tipo de interface externa

3.4.4. SWITCH

❑ Interface externa
❑ Port Mirroring
❑ POE
❑ Opera en cual layer 2,3,4,4-7

3.4.5. ROUTERS / ACCESS POINTS

❑ Interface externa
❑ Tipo: wiFi 1, .. wiFi 6
❑ WPA3-AES, WPA2-AES con KRACK patch ?

3.4.6. HARDWARE DE SEGURIDAD DE REDES

❑ Tipo: firewall, siem, ..
❑ Características de seguridad del equipo

3.4.7. IMPRESORAS

❑ Tipo: Laser monocromatica, laser a colores, ink jet, thermal, dot-matrix, ..
❑ Dimensión máxima de papel
❑ One sided, two sided
❑ DPI
❑ ppm

3.4.8. SCANNER

- ❏ Flatbed, feeder-only, flatbed con feeder
- ❏ Flatbed: dimensión máxima de papel
- ❏ Feeder: dimensión máxima de papel
- ❏ DPI
- ❏ ppm
- ❏ One sided, two sided

4. Software

El Inventario del SOFTWARE debe mantenerse asociado al Inventario de HARDWARE. Ambos inventarios deben mantenerse actualizados. Recomendamos la utilización de herramientas tipo ASSET MANAGEMENT.

4.1. Ambientes Homogéneos y Actualizados

Los diversos softwares deben mantenerse homogéneos, al mismo nivel de producto y actualizados con las últimas versiones del software. Un ambiente heterogéneo incrementa vulnerabilidad, complejidad y costo de administración. Debemos evaluar el nivel de conocimiento técnico del personal encargado de cada *Enterprise Software.*

4.2. Licencias

Las licencias de los Enterprise Software deben estar actualizadas/vigentes, no pueden haber caducado. Para evaluar una eficiente administración, debe considerarse un buen manejo del costo de software.

- ❏ ¿Se utilizan todas las licencias adquiridas?
- ❏ ¿Se justifica esa cantidad de licencias?
- ❏ ¿Hay buena disponibilidad en el mercado de personal capacitado?
- ❏ ¿Se utiliza software que debiese ser reemplazado por un producto con mejores ventajas
- ❏ Cómo el fabricante de software define el costo de la licencia
    - ❏ costo en base a USUARIOS, CPUs, COREs, ...
    - ❏ costos de adquisición
    - ❏ costos de cambio a una nueva versión del producto
    - ❏ costo de acceso a actualizaciones del producto
    - ❏ costo de soporte técnico

4.3. Inventario de Activos

El inventario de activos es requerido por el sistema contable de la organización y es necesario para el mantenimiento y para optimizar costos.

Un inventario de activos que conoce pocas características de los equipos cumple con el propósito contable pero impide el análisis para administrar el mantenimiento y optimizar costos.

Para todo enterprise software, se debe conocer el TAG de inventario del software, tag de inventario de hardware asociado al software, número de licencia, costo, fabricante, nivel de producto, nivel de versión de producto, fecha de su baseline, expiración de accesos a updates, expiración de contrato de servicio técnico, empresa encargada de servicio técnico, end-of-support (eof).

A continuación, características útiles a conocer

4.3.1. Sistema Operacional y VM (virtual machine)

- ❑ Procesador - CPU SINGLE THREAD benchmark
- ❑ Procesador - Cantidad de COREs
- ❑ RAM - capacidad utilizada
- ❑ HDD / SSD - capacidad asignada
- ❑ HDD / SSD - interface / velocidad asignada
- ❑ HDD / SSD - capacidad disponible

4.3.2. Enterprise Software

Tipo: asset management, DBs, Firewalls, malware defense, ...

4.3.3. Documentación

Para cada software, debe existir

- ❑ Un manual de instalación
- ❑ Un manual de usuario
- ❑ Un manual técnico donde se define
    - ❑ La arquitectura
    - ❑ Los elementos de seguridad
        - ❑ Uso de certificados
        - ❑ Uso de criptografía
    - ❑ API
    - ❑ Uso de DB

4.4. Control de cambios (versión)

Debe existir software de control de cambios (versión) para

- ❑ Baselines de
    - ❑ Seguridad
    - ❑ Configuración
- ❑ DATA - cuando así quede clasificada
- ❑ Desarrollo de software

5. Redes

Analizar la

❏ topología de la red LAN y WAN,

❏ utilizando la información del inventario de hardware, y

❏ conociendo los servicios de comunicación WAN / INTERNET contratados, para evaluar la capacidad de nivel de servicio.

La utilización de MAC FILTERING eleva el control administrativo de la red, no su seguridad.

6. Usuarios y Privilegios

6.1. Acuerdo de Usuario - User Agreement

Todos los usuarios del sistema deben conocer y firmar, el temario incluye

❏ Política de acceso local

❏ Política de acceso remoto incluyendo uso de MFA (multi factor authentication)

❏ Política de seguridad física

❏ Política de seguridad

❏ Política de uso de email incluyendo cuando no abrir un mensaje

❏ Política de acceso web

❏ Politica de acceso inalambrico

❏ Uso de dispositivos externos (flash drives)

❏ Confidencialidad de la Información

❏ Custodia y uso exclusivo de *Dispositivo Seguro para la Creación de Firma Electrónica*

6.2. Acuerdo de Usuario Privilegiado - User Agreement

Todo usuario privilegiado también debe conocer y firmar la política de uso restrictivo de cuenta privilegiada.

6.3. Controles Administrativos

Deben ser homogéneos y centralizados para equipos, acceso a redes y aplicaciones.

USUARIOS

❏ Monitoreo de Usuarios

❏ Validación centralizada única de acceso a los sistemas y la red

❏ Remoción de cuentas inactivas

❏ Cuando un usuario entra al sistema (hace LOGIN en el sistema), se le debe mostrar la fecha y hora de su última entrada

❏ Diferentes personas no pueden compartir una cuenta de usuario

- ❏ Los usuarios no pueden tener sesiones recurrentes
- ❏ Passwords
    - ❏ Uso de STRONG PASSWORDS
    - ❏ Política de expiración de passwords
    - ❏ Política de LOCKOUT

USUARIOS PRIVILEGIADOS

- ❏ Monitoreo de usuarios privilegiados
- ❏ Cada usuario debe tener diferentes perfiles (cuentas de usuario) para los diferentes ambientes de producción, preproducción, prueba y desarrollo. Debe existir una LOG de acceso a cada ambiente.
- ❏ Política de Privilegios Mínimos (LEAST PRIVILEGE)
- ❏ Política de Separación de Privilegios (SEPARATION OF PRIVILEGE). El administrador de la red no debe tener acceso a la data en producción, el administrador de la base de datos debe tener accesos restringidos, ...
- ❏ Alertas de accesos remoto de usuarios privilegiados
- ❏ Los proveedores deben tener acceso limitado a datos y archivos en producción
- ❏ Uso de autenticación MFA (multi factor authenticacion)

7. Mantenimiento Preventivo

7.1. Condiciones ambientales y de limpieza

El área de servidores, los servidores, los equipos de seguridad y las unidades de Almacenamiento Enterprise deben mantenerse limpios y en área con condiciones adecuadas de limpieza, humedad y temperatura. Los abanicos de estas unidades deben mantenerse limpios y libres de mugre.

7.2. Vida Útil

Hay que descartar equipos Enterprise cuando el fabricante no provea de repuestos (end-of-life). Igualmente hay que descartar SOFTWARE cuando el fabricante cese de proveer actualizaciones (end-of-service-life).

7.3. Electricidad

En caso de existir una planta eléctrica, se le debe dar mantenimiento preventivo para mantenerla óptimamente operativa. En el caso de los *Enterprise UPS,* debe verificarse su buen estado y corregir las indicaciones de su diagnóstico. Para las otras UPS, se les debe hacer una prueba de carga (load testing) para garantizar que cumplen con la duración requerida.

7.4. Uso de Time Server

Los servidores y equipos deben mantenerse sincronizados en la hora correcta.

7.5. Integridad física de los discos (HDD / SSD)

En las unidades de almacenamiento tipo Enterprise, con auto diagnóstico, verificar su buen estado y corregir las indicaciones de su diagnóstico. Éstas deben mantenerse bajo contrato de mantenimiento. En las otras, consultar su condición S.M.A.R.T. y utilizar herramientas tipo SURFACE SCAN. Luego de verificar la buena salud física de los discos, verificar la salud de los *Enterprise Filesystems* utilizando herramientas como "fschk".

7.6. Actualizaciones de SOFTWARE

Los servidores, equipos de seguridad de redes y software *Enterprise* deben mantenerse con las últimas actualizaciones para minimizar vulnerabilidades de seguridad, preferiblemente automatizar el instalar las actualizaciones a diario. Se debe mantener un LOG de instalaciones para cada software.

7.7. DB

- ❏ Reorganizar páginas indice
- ❏ Reconstruir indices
- ❏ Remover espacios vacios
- ❏ Respaldo de base de datos y su LOG
- ❏ Verificación interna de consistencias buscando errores de DATA
- ❏ Limpieza

8. Respaldo (Backup) - Plan de Continuidad

La definición de una política integral de respaldos y sus procedimientos es esencial para la continuidad de la organización. Debe existir un calendario agendando la generación de cada respaldo, y un CATÁLOGO actualizado de todos los respaldos disponibles, con su fecha de retención.

8.1. Clasificación

Dependiendo de los requerimientos específicos de cada tipo de data, los backups

- ❏ Pueden ser completos o incrementales (full or incremental),
- ❏ su regularidad puede ser diaria, semanal, mensual, ...

Las políticas y procedimientos varían dependiendo del tipo de información a respaldar. Verificar que las políticas y procedimientos de backup son adecuados para cada uno de los siguientes tipos

- ❏ Sistemas operacionales (O/S)
- ❏ Máquinas virtuales (VMs)
- ❏ Las distintas Bases de Datos (DBs) y sus LOGs
- ❏ Los ambientes de desarrollo, prueba, preproducción y producción.
- ❏ Los distintos *Enterprise Software*
- ❏ Los baselines: de seguridad, de configuración y de rendimiento

❑ Los LOGs: de acceso, de seguridad y de vulnerabilidad

❑ Para DATOS, según cada CRITERIO DE CLASIFICACIÓN

8.2. Ejecución

❑ PERSONAL

- ❑ Debe ser metódico, confiable y dedicado
- ❑ No debe tener acceso a la información
- ❑ Debe utilizar cuentas exclusivas para tal propósito, generando LOG auditable
- ❑ ¿Quién está encargado de la verificación de los backups?
- ❑ ¿Quién está encargado de la custodia de los backups?
- ❑ ¿Deben ser distintos a quién hace los backups?

❑ PROCEDIMIENTOS

- ❑ Debe ejecutarse cumpliendo con las políticas y procedimientos
- ❑ Deben hacerse por lo menos dos copias de cada backup, cada una en una ubicación geográfica diferente, cada uno cumpliendo con los niveles de protección física y ambiental.

❑ CRIPTOGRAFÍA

- ❑ Debe utilizar criptografía de llave pública (criptografía asimétrica) con un nivel de criptografía equivalente a AES-128, o superior
- ❑ ¿Cuál es el control de las llaves de criptografía?
- ❑ ¿Cómo se utilizan las llaves de criptografía?

8.3. Almacenaje

❑ PROTECCION

- ❑ ¿Están protegidos de robos?
- ❑ ¿Están protegidos de incendios, humedad o daños de agua?
- ❑ En caso de daños de agua, humedad o fuego, ¿Están geográficamente distantes de las unidades de almacenamiento?

❑ RETENCIÓN

- ❑ ¿Cuál es la política de retención para cada tipo de backup?
- ❑ ¿La política de retención se cumple fielmente?

8.4. Restauración / Recuperación (Restore)

❑ Planes y procedimientos de contingencia para la continuidad del negocio identificando el personal responsable de su ejecución.

❑ SIMULACRO. Utilizando ambiente de prueba, se debe verificar el procedimiento de restauración midiendo los tiempos de recuperación.

❑ ¿Los tiempos de restauración de los diversos sistemas son adecuados?

❏ Análisis de incidentes que activaron el plan de contingencia
- ❏ ¿Por qué los sistemas fallaron?
- ❏ ¿Cuánto tiempo tomó la recuperación?
- ❏ ¿Hubo éxito completo de recuperación?
- ❏ ¿Hubo pérdida de DATA?
- ❏ ¿Hubo daños económicos?
- ❏ ¿Hubo consecuencias para la operación de la organización?
- ❏ ¿Qué dificultades surgieron al ejecutar el procedimiento de recuperación?
- ❏ Las lecciones aprendidas deben ser prontamente incorporadas a los procedimientos de contingencia.

9. Seguridad Informática

La evaluación de seguridad debe tener presente que cuando mides la fuerza de una cadena, el eslabón más débil es quién define su fortaleza. El auditor debe considerar cuando un hallazgo o la presencia de múltiples hallazgos rompen la cadena de seguridad protectora.

Un aspecto crítico de seguridad es mantener actualizado el sistema operacional, el software del hardware de seguridad de redes, y el software de seguridad de redes. Se recomienda automatizar la instalación de estas actualizaciones, deben hacerse a diario. Eliminar del sistema todo software carente de acceso a actualizaciones.

La Seguridad va más allá de esto o aquello, debe fomentarse una cultura de seguridad. El recurso humano debe ser conocedor, estar comprometido y creer en la importancia de Seguridad.

9.1. Estrategia

La seguridad inicia creando un plan o estrategia, diseñando y documentando procedimientos de Seguridad. Cuáles son los procedimientos definidos e implementados de

❏ Seguridad Física del hardware

❏ Seguridad Ambiental del hardware

❏ *Custodia y uso de Dispositivo Seguro para la Creación de Firma Electrónica*

❏ CONFIGURACIÓN DE SEGURIDAD - BASELINE
- ❏ Previo a ser conectado a la red, todo hardware debe ser instalado según configuración predefinida de seguridad.
- ❏ Debe existir un procedimiento para cuando se requiere modificar una configuración predefinida. La nueva configuración debe ser llevada a un ambiente de prueba y luego a un ambiente de

preproducción, antes de llevarla a producción. El procedimiento debe incluir LOG de registro y la destrucción de la DATA del ambiente de prueba.

- ❑ USUARIOS
  - ❑ acceso según sus roles y responsabilidades
  - ❑ acceso local
  - ❑ acceso remoto
  - ❑ asignar o revocar derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios
  - ❑ uso de cuentas privilegiadas
  - ❑ Limitaciones a usuarios de proveedores
- ❑ REDES
  - ❑ Microsegmentación o segregación de acuerdo a áreas de responsabilidad, definiendo zonas de seguridad, considerando
    - ❑ Dominio,
    - ❑ Grupos de servicio,
    - ❑ Grupos de usuarios,
    - ❑ Ubicación geográfica
    - ❑ transferencia de información
    - ❑ uso de la web
    - ❑ uso de correo electrónico
- ❑ DATOS
  - ❑ uso de criptografía, o uso de herramientas CHECKSUM, comparando el valor con su valor original/previo.
  - ❑ Su protección y retención
  - ❑ Proceso de verificación de data o metadatos (QUALITY PROBING)
  - ❑ Privacidad de la Información
  - ❑ INPUT SANITIZATION

9.2. Prevención - Controles Implementados

¿La Seguridad también es como una cebolla, cuantas capas son suficientes para que el núcleo esté protegido? siempre se puede agregar una capa más.

Debe haber rotación de personal asignado a procesos sensitivos.

Algunas funciones no deben recaer en la misma persona cuando exista conflicto de interés. La víctima y el investigador de un incidente, el auditor y el dueño del proceso, el administrador del sistema y quien autoriza

los accesos, el administrador del sistema y el usuario, quien hace el backup y quien lo almacena, quien administra los LOGs y quién custodia y almacena los LOGs, ...

Debe existir una separación física y lógica de ambientes de desarrollo, prueba, preproducción y producción.

9.2.1. Correo electrónico

❏ SPF - sender policy framework
❏ SEG - secure email gateway
❏ Email filtering
❏ Malware defense
❏ Spam blocking

9.2.2. LAN y WAN / INTERNET

Pensando en una cebolla, un atacante puede penetrar una capa de seguridad al utilizar una vulnerabilidad conocida. Si la próxima capa de seguridad es de un distinto fabricante, el atacante tendrá que también encontrar una segunda vulnerabilidad en el segundo fabricante. Se recomienda utilizar equipos de distintos fabricantes en los distintos niveles de seguridad.

❏ ¿Tienen personal dedicado a identificar y responder a ataques en tiempo real?
❏ No utilizar Certificados SSL/TLS expirados
❏ No permitir acceso de equipos fuera de control administrativo, carentes de una configuración segura (security baseline).
❏ Uso de NETFLOW
❏ Network segmentation & micro-segmentation
❏ Política estricta de acceso remoto privilegiado
    ❏ Uso de VPN
    ❏ Uso de MFA / STRONG AUTHENTICATION
    ❏ Restringir por usuario
    ❏ Uso de SESSION TIMEOUT
❏ Antes de otorgar acceso a la red, uso de herramientas NAC (network access control) para
    ❏ verificar configuración
    ❏ verificar que los equipos están actualizados
❏ FIREWALLS
    ❏ Hardware
    ❏ Software - endpoint
    ❏ NGFW (next generation firewall), actualizada
    ❏ Firewall, actualizada

- ❏ WAF - web application firewall

❏ Antispoofing
❏ Ingress / egress packet filtering
❏ Malware defense
❏ Protección de ataques DDoS (distributed denial of service)
❏ Proxy Servers
❏ DNS FILTERING y Whitelisting
❏ IDS (intrusion detection) / IPS (intrusion prevention)
❏ Uso de VPNs
❏ DMZ con Firewall interno y Firewall externo, de distintos fabricantes

9.2.3. Wi-Fi

❏ Política de acceso inalámbrico
❏ Con seguridad WPA3-enterprise, WPA3-personal, o WPA2-AES con KRACK patch

9.2.4. Endpoint

❏ Política de seguridad incluye
- ❏ Uso de flash drives
- ❏ Screensavers con protección de PASSWORD, activado máximo 10 minutos

❏ Actualización automática de navegador y correo electrónico
❏ Uso de herramientas DLP (DATA LOSS PREVENTION)

9.2.5. Arquitectura tecnológica para interoperabilidad

❏ El portal de acceso a usuarios (el servidor de aplicación) se conecta con la aplicación web-service en otro servidor.
❏ La aplicación web-service es quien se conecta con el servidor DB.

9.3. LOGS. Política y Procedimientos.

9.3.1. ¿Cuál es la seguridad de los LOGs? Utilizar firma electrónica para salvaguardar la integridad y seguridad de los LOGs.
9.3.2. ¿Cuál es el tiempo de retención
9.3.3. Activarlos en todos los sistemas y en todos los equipos de redes
9.3.4. CONTROL CENTRAL - los LOGs deben ser agregados a un administrador central de LOGs para su análisis y revisión. Deben existir herramientas que transforman o convierten los distintos formatos a uno único para así generar un análisis centralizado.
9.3.5. ESPACIO DISPONIBLE. Verificar que todos los equipos tienen suficiente espacio para almacenar sus LOGs.

9.3.6. DETALLE - los LOGs del sistema deben incluir información detallada incluyendo fecha y hora, usuario, dirección de origen (source address), dirección de destino (destination address), causa del log, ..

9.3.7. DHCP LOG para actualizar el inventario de hardware.

9.3.8. TIPOS DE LOGS.

❑ Seguridad
❑ Cambio en configuraciones BASELINE
❑ Sistema Operacional
❑ Eventos del Sistema Operacional
❑ LOGs de auditoria
❑ Software (aplicaciones)
❑ DATA

9.3.9. EVENTOS - generación de LOGs

a. Cuando se modifican las CONFIGURACIONES DE SEGURIDAD
b. PASSWORD. LOG al uso exitoso, ALERTA cuando intentos fallidos.
c. USUARIO PRIVILEGIADO. LOG cuando se crea, modifica, o remueve una cuenta, ALERTA si la cuenta es privilegiada.
d. MALWARE, LOG y ALERTA.
e. URL, por cada URL accesado
f. SHELLS (ms powershell, linux bash, ..)
g. DATA. Los requeridos para cumplir con el audito de DATA.
h. Al utilizarse llaves de criptografía
i. Eventos de seguridad
j. Excepciones
k. Fallas

9.4. Tolerancia a Fallas (FAULT TOLERANCE)

Como es la arquitectura de **redundancia**, identificar SINGLE POINT OF FAILURE

❑ Conexiones WAN / INTERNET
❑ Servidores
❑ Almacenaje
❑ DBs
❑ Web services
❑ Enterprise software que brinda algún servicio
❑ Personal técnico en cada una de las áreas requeridas para resolver incidente

9.5. Vulnerabilidades - Incidentes

9.5.1. Estrategia / Procedimiento de resolución de Incidentes

Se debe crear un procedimiento anticipando las vulnerabilidades más probables, de alto o mediano impacto. La organización debe utilizar con regularidad herramientas activas y herramientas pasivas para identificar vulnerabilidades y luego de su identificación, prontamente eliminarla.

9.5.2. Medidas de Prevención

a. Hacer pruebas de seguridad durante el desarrollo de SOFTWARE.
b. Verificar la configuración de todos los equipos, especialmente el hardware y software de seguridad.
c. Utilizar MICRO SEGMENTATION de redes.
d. El personal informático, incluyendo contratistas, deben ser motivados a advertir y reportar vulnerabilidades.
e. Procedimiento rápido para dar de baja a un usuario.
f. Los reportes de vulnerabilidad deben ser generados, evaluados, y sus hallazgos deben ser resueltos con prontitud.
g. Frecuente revisión de las reglas del SIEM
h. Procedimiento a utilizar que garantiza la recuperación de CUALQUIER llave de encriptar perdida.
i. Los servidores deben eliminar o monitorear activamente la utilización de Java, ActiveX, JavaScript, y VBScript.
j. Deshabilitar la ejecución automática de binarios o scripts, incluyendo AutoRun (ambiente windows)
k. Cambiar DEFAULT passwords de usuarios o remover DEFAULT usuarios todos los hardware incluyendo servidores y equipos de seguridad de redes.
l. Deshabilitar o remover funcionalidades o servicios no utilizados, habilitar el mínimo de servicios requeridos.
m. En caso de Incidente, debe existir un listado de responsabilidades y funciones, incluyendo cómo contactar a todos los proveedores de servicio.

9.5.3. Monitoreo

a. Vulnerabilidades originadas por decisiones técnicas contrarias a buenas prácticas o contrarias a las recomendaciones de personal técnico especialista en la materia.
b. Monitoreo de vulnerabilidades identificadas en cve.mitre.org, o similar
c. Tiempo de respuesta y de resolución a una detección debe ser rápida
d. Scan cada equipo que entra en la red, clasificando resultados de acuerdo a severidad. Luego de cada scan, utilizar el previo scan como baseline para identificar la presencia de cambios en la configuración.
e. Uso de herramientas SCAP
f. Utilización de SIEM u otra herramienta analítica centralizada. Referirse a Gartner, MAGIC Quadrant for SIEM
g. Personal dedicado al monitoreo del SIEM, ALERTAS y LOGs
h. Monitorear abuso de privilegio de los usuarios

i. Promover con los usuarios y crear un ágil y rápido procedimiento para que los usuarios reporten fallas de seguridad.

9.5.4. Análisis
a. El auditor debe hacer un análisis del SIEM y comprender su historial de reportes y su historial de revisión de reglas del SIEM
b. Personal dedicado al análisis del SIEM, ALERTAS y LOGs
c. Frecuencia de revisión y análisis del SIEM, ALERTAS y LOGs
d. Clasificar vulnerabilidad de acuerdo a su impacto o importancia
e. El LOG de Seguridad debe ser monitoreado y evaluado, detectando incidentes y ejecutando correctivos.

9.5.5. Resolución de Incidentes
a. La resolución de los Incidentes debe seguir los procedimientos documentados.
b. Debe existir una bitácora describiendo el problema, su resolución, las medidas preventivas tomadas para evitar que se repita, y la probabilidad que se repita, creando o actualizando el procedimiento de resolución.

9.6. Pruebas de Penetración (PENTEST)
9.6.1. Las pruebas deben ser ejecutadas por un ente independiente.
9.6.2. Presentar Certificación y Experiencia
9.6.3. Penetración Externa e Interna
9.6.4. Penetración de Micro-Segmentación
9.6.5. Sistemas Críticos
9.6.6. En CAPA de Aplicación (capa 7) y Capa de Red (capa 3)
- ❏ Prueba de Autenticación de CUSTOM SOFTWARE
- ❏ Aplicaciones Web

9.6.7. Ingeniería Social

10. Rendimiento y Elasticidad (Performance and Elasticity)

El establecimiento de baselines, el monitoreo del rendimiento y la generación de alertas de rendimiento son elementos necesarios para proveer un buen nivel de servicio. El análisis de rendimiento permite identificar debilidades, cuellos de botella, para así ajustar los recursos y configuraciones y brindar un óptimo nivel de servicio.

Es necesario conocer los recursos disponibles, proyectar los requerimientos de crecimiento, y planear futuras compras.

10.1. Análisis del último reporte de rendimiento.
10.2. Utilización de herramientas para el análisis de rendimiento (server performance analysis tool).

10.3. Para cada servidor/enterprise software, cuál es su performance baseline (normal workload) y como se comporta el servicio en día y horas pico. Generación de alertas de rendimiento (PERFORMANCE ALERT LOG).
10.4. Elasticidad -¿Cuál es la disponibilidad de recursos en día y hora pico?
10.5. Utilización de discos SSD para almacenar data de alto acceso.
10.6. ¿Cuál es el espacio disponible en cada Enterprise Filesystem?
10.7. ACCOUNT PROVISIONING: cual es la capacidad de crear y administrar usuarios

10.8. Monitorear cada servidor correlacionando el enterprise software

10.8.1. CPU

- ❑ Load
- ❑ Speed
- ❑ Idle time
- ❑ User time
- ❑ Capacidad de mensaje de los procesadores (PROCESSOR MESSAGING CAPACITY)

10.8.2. RAM y PAGINACIÓN

- ❑ Considerar el uso de SSDs
- ❑ Monitorear nivel de paginación (hard faults) y tamaño de working-set

10.8.3. NETWORK & INTERNET

- ❑ LOAD BALANCE
- ❑ LATENCY (ping)
    - ❑ 100 ms es razonable
    - ❑ 50 ms es bueno
    - ❑ 30 ms es muy bueno
- ❑ THROUGHPUT
- ❑ BANDWIDTH saturation: velocidad de subida y de bajada
- ❑ Identificar BOTTLENECKS

10.8.4. ALMACENAJE

- ❑ LOAD BALANCE
- ❑ read / write THROUGHPUT
- ❑ Identificar BOTTLENECKS

11. Políticas de Uso

El *Centro de Almacenamiento* debe establecer y hacer saber sus políticas de uso para:

❏ el personal que utiliza el sistema de almacenamiento y

❏ el personal que administra el sistema de almacenamiento y sus consecuencias en caso de falta.

Algunos temas para considerar:

11.1. La protección física y uso exclusivo del *Dispositivo Seguro para la Creación de Firma Electrónica.* Incluye informar de inmediato en caso de ser extraviado o robo.

11.2. Prácticas de seguridad física

11.3. Seguridad para visitantes contractuales

11.4. A quien acudir dependiendo del tipo de problema

11.5. Cuando ocurre un LOCKOUT

11.6. Wi-Fi: WPA2-AES como mínimo

11.7. Actualizar endpoint: automática diaria del sistema operacional, email, navegador, y software de seguridad

11.8. Email: contenido que atenta contra la moral, propiedad intelectual, uso de SPAM, enviar y recibir archivos, como defenderse de PHISHING, no es para uso personal, ..

11.9. Navegación WEB: contenido que atenta contra la moral, visitar sitios no corporativos, considerar uso de whitelist, o de por lo menos uso de blacklist, buenas prácticas de navegación, ..

11.10. Uso de flash drives

11.11. Manejo de passwords: no escribirlo, no guardarlo en computador, ..

11.12. Acceso remoto,

11.13. Confidencialidad de DATOS

11.14. Uso restrictivo de cuenta privilegiada

12. Digitalización con Firma Electrónica

Es la responsabilidad del *Centro de Almacenamiento* educar, hacer cumplir los procedimiento y velar por la validez del proceso de Digitalización con Firma Electrónica.

❏ Procedimiento, pasos a seguir

❏ Adiestramiento y capacitación del personal

❏ Monitoreo proactivo, seguimiento

❏ Monitoreo proactivo de la seguridad del *Dispositivo Seguro para la Creación de Firma Electrónica*

❏ Al utilizar un scanner, considerar la resolución de digitalización (dpi) de acuerdo al tipo o propósito del documento. En caso de que el objeto escaneado sea texto, debe ser claramente legible, en caso que el objeto escaneado no sea texto, la resolución debe ser suficientemente nítida para apreciar detalles de importancia.

13. Almacenaje en la Nube (Cloud Storage)

13.1. Método de cómo se clasificó la información y las diversas protecciones adicionales implementadas dependiendo de su valor.

13.2. Relacionar como los DATOS transitan de un sistema, equipo, aplicación, API (application programming interface) a otro.

13.3. Contrato con proveedor y sus adendas deben incluir descripción clara y detallada de las responsabilidades del proveedor

a. Lenguaje indicando cumplimiento con legislación panameña

b. Como el proveedor comunicará cambios al Contrato, habrá negociación

c. Elasticidad y Rendimiento,

d. Privacidad,

e. Protección de Confidencialidad (Datos Personales)

f. Política de Retención de datos, utilizando su clasificación

g. Como es el manejo de los históricos de cambio (REVISION HISTORY)

h. Mecanismo de Respaldo y Recobro (BACKUP and RECOVERY)

i. Instructivo y capacitación para los Controles Administrativos Centralizados de accesos y almacenamiento (Centralized Cloud Storage Controls for managing users and DATOS)

j. Descripción técnica clara de cómo está implementada la seguridad, ¿cuáles son las protecciones que utiliza?

1. Geovalla (GEO-FENCE)
2. Identificar todos los equipos y software que se conectan a la NUBE. Identificar quien, y como se usan, manejo de ROGUE DEVICES
3. RBAC (role based access control): autorizaciones y privilegios de acceso
4. Uso de MFA (MULTI FACTOR AUTHENTICATION)
5. Uso de SECURE FILE STORAGE
6. Criptografía
    - ❑ data-in-motion, mínimo IPsec con criptografía AES-GCM
    - ❑ data-at-rest y data-in-use, mínimo AES-128
    - ❑ Quién controla las llaves de criptografía y cómo se utilizan
7. Monitoreo del LOG buscando riesgos de vulnerabilidad, uso de herramientas SIEM
8. Procedimiento a seguir en caso de un daño o una penetración
9. Pago de Compensación (REDRESSING)
10. DDOS - DISTRIBUTED DENIAL OF SERVICE attack
11. Ataque Brute force
12. Infección de Malware
13. Utilización de Filtros DATA AWARE, inteligencia en contenido, usuarios y actividad
14. ¿Cuáles son las protecciones para problemas de seguridad en software?

14. Datos, Records y Metadatos

Cuando el Prestador de Servicios de Almacenamiento no es el Prestador de Servicios de Procesamiento, el Prestador de Servicios de Almacenamiento exigirá contractualmente al Prestador de Servicios de Procesamiento que cumpla con las disposiciones aquí presentes que le competan.

Se debe conocer donde se almacena la información y las características de almacenamiento. Por ejemplo, se debe conocer si es un NTFS filesystem, la disponibilidad de espacio libre en el filesystem, si se utiliza RAID 6, si esta encriptado, si se utiliza EFS, el uso de load balance, el tipo de uso, como para DB, DATOS críticos, imágenes, videos, uso general, ...

14.1. Http Cookie

❏ política de uso

❏ ¿qué DATOS se guardan y su propósito. ¿Algún dato confidencial?

❏ ¿Cuál criptografía se utiliza?

❏ La información a guardar deber ser mínima, no se puede almacenar información confidencial

14.2. Framework de Gobernanza de Datos

El Prestador de Servicios de Procesamiento definirá las pautas y reglas (GUIDELINES AND RULES) para la creación, manipulación, y acceso a DATOS.

14.3. Control de Acceso

❏ Se protege la privacidad de la información y se limitan accesos a información clasificada. ¿Cuáles son los mecanismos que autorizan acceso a la información?

❏ Analizar el correcto funcionamiento de las aplicaciones y DBs que accesan DATA clasificada para ser protegida a ser modificada, o clasificada para monitoreo de acceso. ¿Se generan LOGs de audito?

❏ Se protege la integridad de la información creando una nueva versión de un archivo, manteniendo el original, cuando el usuario modifica DATA. Cómo funciona el mecanismo de protección a la información cuando se modifica información presente en una DB. Cómo funciona el mecanismo de protección a la información cuando se modifica información a través de una aplicación.

14.4. Confidencialidad

❏ La utilización de mecanismos de privacidad como tokenización, seudonimización, anonimización, o REDACTION (tachar datos del documento imposibilitando su comprensión).

❏ En el caso de Datos Personales protegidos por legislación, definir y hacer público en la web los requisitos para el trámite de solicitud de datos, incluyendo tiempos de respuesta.

❏ Utilizar criptografía, como mínimo AES-128 para data-in-use, data-at-rest

❏ Utilizar criptografía, como mínimo AES-GCM capa-3 (IPsec) para datos-en-tránsito

14.5. Integridad

❏ Para datos que deben tener validez legal, el Prestador de Servicios de Almacenamiento requerirá sustentar el procedimiento utilizado para probar que cada archivo fue recibido fidedignamente y que

corresponde al actual archivado. El Prestador de Servicios de Procesamiento deberá probar que cada archivo fue generado cumpliendo con el Marco Legal.

❏ El Jefe de Archivos, cargo definido por legislación, mantendrá expediente con el sustento técnico de toda autenticación.

❏ LOGS. Política e implementación para la generación de LOGs requeridos para un audito.

❏ RESILIENCIA (DATA RESILIENCE). ¿Cuáles son los mecanismos utilizados para cada tipo de DATA? Uso de replicación de datos (DATA REPLICATION) sincrónico o asincrónico, RAID, ...

14.6. Criterios de Clasificación

Los DATOS tienen variada importancia y tolerancia a riesgo, pueden ser clasificados de acuerdo a una extensa variedad de criterios:

❏ VALOR: esencial, estratégica, alto, mediano, bajo

❏ SEGURIDAD: nivel de seguridad

❏ RIESGO: crítica, no-critica

❏ LEGISLACIÓN: aquellos legalmente custodiadas

❏ CONFIDENCIALIDAD: alta/secreta, mediana/protegida, uso-interno, publica

❏ ESTRUCTURA: documento tipo office, pdf, html, DB-DATOS, código fuente de software, ejecutables de software, emails, imágenes, videos, audio, ..

14.7. Clasificación

Políticas y procedimientos de acuerdo a su clasificación, incluyendo

❏ acceso desde dentro y fuera del país,

❏ Seguridad

❏ Seguridad de datos-en-tránsito cifrada,

❏ control de cambios (versiones),

❏ almacenaje,

❏ retención,

❏ descarte / disposición,

❏ respaldo,

❏ recuperación (RESTORE de un BACKUP)

14.8. Metadatos / Interoperabilidad

Para poder utilizar DATA requerimos saber de su existencia. Los METADATOS son el mecanismo de localización. Una organización con carencias en la creación de METADATOS limita o impide la utilidad de la información. Es clave que un conjunto apropiado de procedimientos para el etiquetado de la información sea desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización facultando los estándares internacional ISO y/o de protocolo OAI-PMH (XML

over HTTP) y de vocabulario DUBLIN CORE METADATA SCHEME. Analizar la optimización de capacidad, utilización de herramientas analíticas, y la efectividad de búsquedas.

14.9. Metadatos / Generación
Procedimientos y políticas de aprobación y validación

❑ Automatizada por Software
❑ Manual
❑ Personal interno
❑ Personal contratista

15. Póliza de Responsabilidad Civil

❑ La Póliza debe cumplir con todos los requerimientos legales
❑ Presentar copia vigente
❑ Presentar carta de empresa aseguradora afirmando que la póliza presentada el año anterior nunca perdió vigencia por falta de pago o cualquiera otro motivo.

16. Acuerdo de Nivel de Servicio (Sla - Service Level Agreements)

Las partes deben claramente definir las responsabilidades penales originadas por faltas del contratista y mantener póliza según mandato legislativo.

El anexo técnico al contrato debe definir clara y formalmente las responsabilidades de

❑ actualizaciones,
❑ mantenimiento,
❑ servicios definiendo las políticas, procedimientos y mecanismos de monitoreo
❑ de acceso,
❑ de seguridad,
❑ de respuesta a incidentes
❑ de continuidad del negocio con específicos que pueden ser medidos y/o verificados definiendo un nivel de servicio.

Los contratistas, externos o visitantes a las instalaciones, deben ser evaluados en su saber de las políticas y prácticas relacionadas a

❑ CONFIDENCIALIDAD
❑ SEGURIDAD
❑ MARCO LEGAL

17. Recursos y Referencias

Recomendamos el uso de herramientas enterprise

❏ GOBERNANZA DE DATOS
http://www.datagovernance.com/

❏ CPU BENCHMARK
Recomendamos medir el poder computacional de un CPU utilizando el THREAD MARK de
https://www.cpubenchmark.net/CPU_mega_page.html

❏ ASSET MANAGEMENT - gratuito, portatil {WIN}
Free PC Audit : https://www.misutilities.com/free-pc-audit/

❏ SYSTEM INFORMATION TOOL - gratuito {WIN}
Speccy: https://download.ccleaner.com/spsetup132.ex_e

❏ S.M.A.R.T. tool - gratuito {WIN}
HDDScan : https://hddscan.com/

❏ S.M.A.R.T. tool kit - smartmontools { LINUX }

❏ HDD / SSD - SURFACE SCAN - gratuito, portatil {WIN} Disk Scanner : https://www.ariolic.com/disk-scanner/

❏ HDD / SSD - SURFACE SCAN - badblock {LINUX}

❏ HDD / SDD benchmark- gratuito, portatil { WIN } Crystal Disk Mark:
https://crystalmark.info/en/software/crystaldiskmark/

❏ NETWORK INFORMATION TOOL - gratuito {WIN} Network Software Scanner
https://emcosoftware.com/network-software-scanner

❏ NETWORK SCANNER - gratuito, portatil
Angry ip scanner : https://sourceforge.net/projects/ipscan/

❏ NETWORK PROTOCOL ANALYZER - gratuito, portatil
Wireshark : https://www.wireshark.org/download.htm_l

❏ IP SCANNER y PORT SCANNER - gratuito { WIN } Free IP Scanner 3.2 :
https://www.eusing.com/ipscan/free_ip_scanner.htm

❏ PORT SCANNER TOOL - gratuito, portatil { WIN }
Free port scanner : https://www.advanced-port-scanner.com/

❏ VULNERABILITY SCANNER AND NETWORK DISCOVERY - gratuita
Zenmap / NMAP : https://nmap.org/zenmap/