Metodología de Administración e Implementación de Repositorios Digitales para la Seguridad de la Información Clasificada del Sector Gubernamental

Nilda Mónica Cutili López
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
nilda_mcl@hotmail.com

***Resumen*—Los repositorios digitales, posibilitan una gestión automatizada de los procesos institucionales, facilitando de forma ordenada la difusión con el personal autorizado y accesibilidad de sus contenidos digitales, dichos contenidos en el presente se denotan como información clasificada. Es así que, para la implementación y administración de repositorios con información de alta sensibilidad, se plantea una metodología que guie estos procedimientos, el mismo está desarrollado en 5 fases fundamentales descritos en el desarrollo del presente.**

Palabras clave—Archivo digital, gestión documental digital, información clasificada, información sensible, repositorios digitales, sector gubernamental, estatal.

I. INTRODUCCIÓN

Los repositorios digitales, son una solución frente a requerimientos actuales del sector gubernamental, principalmente cuando la institución debe socializar su información con cierto grupo de funcionarios públicos (usuarios), para lo cual tiene implicancia una serie de procesos y procedimientos que influyen en la aplicación, funcionamiento, mantenimiento y administración, a objeto de permitir trabajar con una herramienta de gran aporte al desempeño institucional con las medidas de seguridad necesarias, basados en las dimensiones la confidencialidad, disponibilidad e integridad de la información, que a su vez se encuentre enmarcado en el cumplimiento de la normativa vigente del Estado Plurinacional de Bolivia, y por ende recoja las actividades, técnicas, resaltantes del ámbito internacional.

Es así, que el presente, muestra el desarrollo de una metodología de implementación y administración de repositorios digitales para la seguridad de la información clasificada del ámbito gubernamental y posterior presentación de resultados. La misma se encuentra basada en la siguiente interrogante, *¿Cuál es el tratamiento adecuado, de administración e implementación de repositorios digitales, para la seguridad de la información que es clasificada del sector gubernamental?*

La hipótesis se encuentra alineada a "*El desarrollo de una metodología de administración e implementación de repositorios digitales, brinda seguridad a la información clasificada del sector gubernamental*".

II. MÉTODOS

La presente metodología, parte de dos pilares fundamentales: La Normativa Legal Vigente y la Identificación de aspectos relacionados con el tratamiento de información clasificada en el ámbito internacional.

El ámbito legal, enmarcado Resolución Administrativa AGETIC/RA/0040/2018 [1], el Decreto Supremo 3525 sobre la Agencia de Gobierno Electrónico y Tecnologías de la Información [2], el Decreto Supremo Nº 28168 referido al Acceso a la Información [3], sobre todo la Ley Nº 164 Ley General de Telecomunicaciones Tecnologías de información y Comunicación [4] y los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la información de las entidades del Sector público [5].

Por otra parte, la identificación de aspectos relevantes del contexto internacional, con contextualización al ámbito nacional, tiene que ver con:

Las normas de seguridad de la información clasificada de España [6], el Libro Naranja del departamento de Defensa de EEUU [7], la Norma Internacional General de Descripción Archivista ISAD-G [8], las normas españolas para la seguridad de la información clasificada NS04, la NS05 [9], entre otros.

A. Propuesta Metodológica

La metodología consta de cinco 5 fases principales que son:

- FASE 1: Diagnóstico
- FASE 2: Análisis y diseño
- FASE 3: Implementación y Pruebas
- FASE 4: Capacitación
- FASE 5: Administración

Considérese que, en cada fase, se define tareas, roles y responsabilidades, etc. Así también, está orientada con un diseño detallado de cada etapa y actividad, que permita que la implementación sea llevada a cabo por medio de gestión autónoma de la institución interesada en contar con un repositorio digital, sin requerirse de la necesidad de contratación de equipos de trabajo externos que la ejecuten.

Para referenciar este artículo (IEEE):

[N] N. Cutili, «Metodología de Administración e Implementación de Repositorios Digitales para la Seguridad de la Información Clasificada del Sector Gubernamental», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 131-134, 2020.

1) PRIMERA FASE: Diagnóstico

Esta fase está dedicada, al inicio de la implementación de los repositorios digitales, es donde se determina las necesidades reales y la situación actual del tratamiento de la información clasificada.

Fase en concordancia a estándares internacionales de certificación de seguridad cibernética (GSEC) [10].

- Entrevistas al personal ejecutivo
- Entrevista al personal involucrada con la información clasificada
- Entrevista al personal de tecnologías de información
- Entrevista al personal responsable de seguridad de la información
- Documentación

2) SEGUNDA FASE: Análisis y Diseño

Siendo una de las más extensas, esta fase requiere de un trabajo minucioso y detallado sobre el análisis de las necesidades institucionales establecidas en la primera fase de diagnóstico, a fin de que permita la proyección de los beneficios y cobertura del servicio que se pretende implementar.

En esta fase se va a planificar todos los aspectos que se deben tomar en cuenta previa implementación y funcionamiento del repositorio digital que albergará la información clasificada, esta estará determinada de acuerdo a los siguientes puntos:

- ✓ Recursos
  - Recursos Humanos
    - Digitalizador
    - Catalogador
    - Supervisor
    - Administración del Repositorio Digital
    - Personal con acceso a la información clasificada
    - Personal de seguridad de la información
  - Infraestructura Tecnológica
    - Servidor
    - Conexión a un servidor SMTP
    - Red Local
    - Software Repositorio Digital
    - Acceso a internet
  - Recursos Económicos

- ✓ Responsabilidades
  - Personal involucrado con información clasificada
    - Categorización de la Información Clasificada
    - Control de Flujo de Trabajo
    - Catalogación de documentos
    - Tratamiento de metadatos
    - Digitalización y custodia
    - Soporte procedimental
    - Anulación de documentos
  - Personal de TI y responsable de SI
    - Capacitación y soporte
    - Actualización de BD
    - Mantenimiento
    - Disponibilidad
      - Copias de Seguridad
      - Conversión y migración
      - Seguridad Física
      - Gestión de Riesgos

- ✓ Normas de uso y de servicio
  - Misión y Visión
  - Clasificación de documentos digitales
  - Gestión de usuarios y grupos
  - Control de accesos
  - Permisos de los usuarios
  - Formato de los documentos digitales
  - Tipo de documentación
  - Conservación digital
  - Servicios
  - Anulación de documentación
  - Seguridad Física
  - Seguridad en las operaciones
  - Gestión de Riesgos

- ✓ Selección del Software
  - Características Principales
  - Base de Datos
  - Sistema de Archivos
  - Medidas de Seguridad
  - Tecnologías de Código Abierto
  - Repostes Estadísticos

- ✓ Documentación

3) TERCERA FASE: Implementación y Pruebas

Concluida con la segunda fase, corresponde proceder con el proceso de implementación del Repositorio Digital, por lo cual las actividades correspondientes a esta fase son:

4) CUARTA FASE: Capacitación

La capacitación al personal involucrado, es parte integral en la implementación del sistema, a fin de poder ponerlo en marcha, con la garantía de que los distintos responsables están en condiciones de utilizarlo de manera adecuada y así puedan asesorar a los potenciales usuarios sobre el manejo y bondades que ofrece el repositorio digital.

Para ello es preciso la coordinación del área de recursos humanos, con el responsable de seguridad de la información a objeto de fijar actividades relacionadas con la capacitación al personal involucrado con el sistema a fin de poner en conocimiento los manuales y normas de seguridad y de servicio de la información aplicados a este.

También se debe incluir un plan de sensibilización respecto al tratamiento de la información clasificada a fin de garantizar el éxito del uso del repositorio digital.

5) QUINTA FASE: Administración

Cuando se dé por concluido las anteriores fases, se dará inicio a la fase de administración y posterior mantenimiento; donde se debe considerar el óptimo funcionamiento del sistema y los servicios que conlleva, precautelando la seguridad de la información clasificada albergada en el repositorio digital. Esta fase está directamente relacionada a la Resolución Administrativa AGETIC/RA/0040/2018.

III. Resultados

A fin de dar marcha a la propuesta metodológica, se procedió a la implementación de un prototipo de repositorio.

Este se encuentra alojado en la siguiente dirección http://157.245.10.142:8080/ como se muestra en la figura. En cumplimiento a la propuesta metodológica en el punto Selección del Software, se realizó la evaluación de 4 herramientas candidatas, conforme a la siguiente valoración 1 (SI cumple) y 0 (NO cumple), dando como resultado DSpace con una puntuación aventajada de 26/34, en comparación a 20/34 (Lasefiche), 22/34 (Alfresco Comunity) y 18/34 (Alfresco con suscripción).

IV. Discusión

A. *Demostración De La Hipótesis*

Para la demostración de la hipótesis, se citará la misma:

"El desarrollo de una metodología de administración e implementación de repositorios digitales, brinda seguridad a la información clasificada del sector gubernamental"

A objeto de demostrar la hipótesis, se planteó un estado previo y un estado posterior, dichos estados se realizaron en función a un análisis de riesgos, considerando la metodología MAGERIT y matrices de evaluación de riesgos. Basado en 10 indicadores.

Se realizó una encuesta aplicada a las instituciones que conforman la muestra, que por la sensibilidad de los datos serán referidas como Institución A, B, C, D, E, F y G, a tal efecto, la escala de valoración fue (1=inaceptable, 2=Deficiente, 3=Regular, 4=Bueno y 5=Excelente), dando como resultado previo al proceso de aplicación de la propuesta metodológica, la Figura 1. La ilustración refleja, una medición inicial de indicadores deficiente con tendencia a lo inaceptable. Como consecuencia nos lleva a comprender, que el actual tratamiento de la información clasificada del sector gubernamental no se encuentra entre los niveles aceptables.

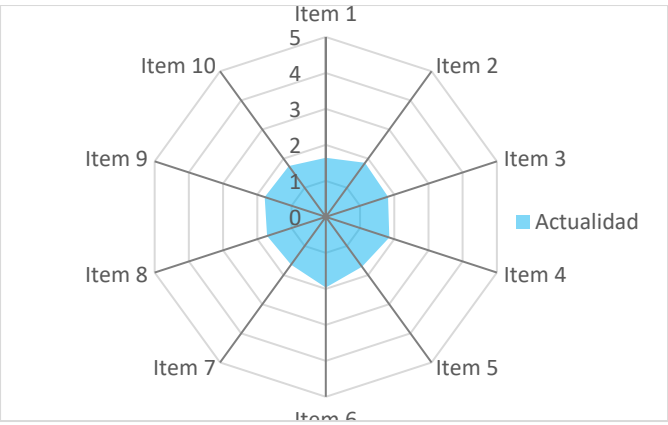

Fig. 1. Representación Gráfica de indicadores previo a la implementación de la propuesta metodológica.
Fuente: Elaboración propia, 2019

Así también, se identificó 28 riesgos asociados a la seguridad de la información clasificada, los mismos fueron representados en un mapa de calor de riesgos, evidenciado en la tabla 1.

TABLA I. Mapa de calor de riegos previo a la implementación de la propuesta metodológica

	IMPACTO				
PROBABILIDAD	1–Irrelevante	2–Menor	3–Moderado	4–Severo	5–Crítico
5- Cierta/Inminente			R2, R4, R8, R12	R5, R6, R7, R10, R11	R13
4- Muy probable			R1, R26	R3, R9, R21,R24	R14, R15, R16, R17, R27
3- Probable				R18, R19	R22, R23, R25, R28
2- Poco Probable					R20
1- Improbable					

Fuente: Elaboración propia, 2019

Actualmente los riesgos están en un nivel no aceptable y luego van subiendo. Es decir que los riesgos identificados requieren especial atención de manera prioritaria, a objeto de no comprometer la seguridad de la información clasificada del sector gubernamental.

En este entendido, a fin de la prueba de hipótesis, se han considerado como evidencias la elaboración de tres posibles escenarios identificados posterior a la implementación de la propuesta metodológica, estos escenarios son: Escenario Pesimista, Escenario Probable, Escenario Optimista, a ello se suma la situación actual, que dio como resultado lo siguiente:

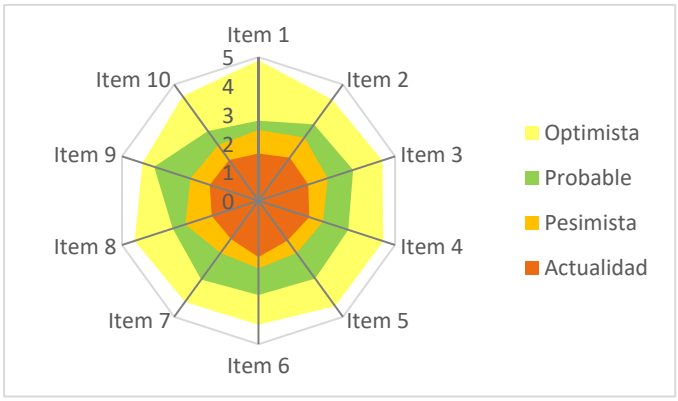

Fig. 2. Comparación de escenarios Probabilísticos.
Fuente: Elaboración propia, 2019

TABLA II. Mapa de calor de riegos Escenario Pesimista

	IMPACTO				
PROBABILIDAD	1–Irrelevante	2–Menor	3–Moderado	4–Severo	5–Crítico
5- Cierta/Inminente		R4, R16	R2, R10, R20, R25, R28	R11	
4- Muy probable			R1, R9, R14, R17, R19, R24		
3- Probable				R3, R5, R15, R18, R21, R26	R8, R22, R23, R27
2- Poco Probable				R7	R6, R12, R13
1- Improbable					

Fuente: Elaboración propia, 2019

En un escenario pesimista el riesgo de la seguridad es menor, con relación al estado previo a la implementación de la propuesta metodológica, es decir el riesgo ha disminuido.

TABLA III. MAPA DE CALOR DE RIEGOS ESCENARIO PROBABLE

	IMPACTO				
PROBABILIDAD	1–Irrelevante	2–Menor	3–Moderado	4–Severo	5–Crítico
5- Cierta/Inminente	R25, R28	R7, R10, R16, R20			
4- Muy probable			R1, R2, R8, R12, R19		
3- Probable		R5, R13		R4, R11	
2- Poco Probable		R21		R3, R9, R14, R18, R24, R27	R6, R17
1- Improbable				R26	R15,

Fuente: Elaboración propia, 2019

En un escenario probable, el riesgo de la seguridad de la información clasificada es también menor, con relación al estado actual, es decir el riesgo ha disminuido

Finalmente, en un escenario optimista, los riesgos de la seguridad de la información clasificada son muchísimo menor, con relación al estado actual, es decir el riesgo ha disminuido considerablemente.

Por lo tanto, de los 3 casos de análisis de riesgos correspondientes a los diferentes escenarios probabilísticos, el riesgo de la seguridad de la información clasificada disminuye considerablemente. Así también, de acuerdo a la comparación de los ítems (Indicadores), en ningún caso el escenario actual es mayor a los otros escenarios.

Con base esta demostración se afirma que la hipótesis está comprobada.

V. CONCLUSIONES

El desarrollo de una "metodología de administración e implementación de repositorios digitales para la seguridad de la información clasificada del sector gubernamental", contribuye a la gestión institucional, de una manera eficiente, considerando que brinda seguridad a la información clasificada, que cuya divulgación no autorizada, puede desencadenar en riesgos de gran impacto como es la seguridad interna y externa del Estado Plurinacional de Bolivia.

Sobre la formulación de la hipótesis de investigación, la misma ha sido comprobado mediante la técnica de creación de escenarios, que permitió combinar distintas variables para prever situaciones posibles. En proyectos muy complejos suelen plantearse numerosos escenarios, pero para el desarrollo del presente, bastó con el planteamiento de tres situaciones: escenario pesimista, escenario probable, escenario optimista. Teniendo como resultado, la efectividad de la propuesta metodológica, para la seguridad de la información clasificada del sector gubernamental.

REFERENCIAS

[1] Resolución Administrativa AGETIC/RA/0040/2018. (01 de 06 de 2018). AGETIC. La Paz, Bolivia: Agencia de Gobierno electrónico y Tecnologías de Información y Comunicación.

[2] Decreto Supremo 3525. (4 de 04 de 2018). Agencia de Gobierno Electrónico y Tecnologías de la Información. La Paz, Bolivia.

[3] Decreto Supremo Nº 28168 Acceso a la Información. (16 de 05 de 2005). Gaceta Oficial del Estado Plurinacional de Bolivia. Bolivia, Bolivia.

[4] Ley Nº 164 Ley General de Telecomunicaciones Tecnologías de información y Comunicación. (8 de 08 de 2011). Gaceta Oficial de Bolivia. Bolivia, Bolivia.

[5] Consejo para las Tecnologías de Información y Comunicación. (2017). Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la información de las entidades del Sector público. La Paz, Bolivia.

[6] Autoridad Delegada para la seguridad de Información Clasificada. (2018). Normas de la Autoridad Nacional. Madrid: Ministerio de defensa.

[7] Department of Defense Standard. (1985). Orange Book Department of Defense Trusted Computer System Evaluation Critical. EEUU.

[8] Comité de normas de descripción. (septiembre de 1999). Norma Internacional General de Descripción Archivística - ISAD (G). Estocolmo, Suecia: Ministerio de Educación Cultura y Deporte.

[9] Autoridad Delegada para la seguridad de Información Clasificada. (2018). Normas de la Autoridad Nacional. Madrid: Ministerio de defensa.

[10] GIAC Security Essentials (GSEC)