RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PERÚ Ministerio de Cultura

III SEMINARIO INTERNACIONAL DE GESTIÓN DOCUMENTAL Y ARCHIVOS 2018

"Innovación Tecnológica al Servicio de la Ciudadanía"

Gestión de riesgos informáticos en la gestión documental

Ing. Joan Palacios Ramírez
jpalacios@cultura.gob.pe

Con el apoyo de:

PERÚ Presidencia del Consejo de Ministros | Secretaría de Gobierno Digital

INSTITUTO NACIONAL DE RADIO Y TELEVISIÓN DEL PERÚ

Auspician:

IRON MOUNTAIN

UNIVERSIDAD esan

FIRMAUX DIGITAL

Image & Design

ASPARG
ASOCIACIÓN PERUANA DE ARCHIVEROS Y GESTORES DE LA INFORMACIÓN

TO.DIGITAL
TRANSFORMACIÓN DIGITAL EMPRESARIAL

GRAMD.COM
Identidad y Firma Digital con validez legal

indra

ACEPTA

Introducción

- El "Modelo de Gestión Documental"[1], indica que las entidades del Sector Público deben:
  1. Realizar un análisis de riesgos asociados a su gestión documental considerando:
     - ✓Riesgos de recursos humanos.
     - ✓Riesgos de proceso.
     - ✓Riesgos de Tecnología (Informáticos).
     - ✓ Otros.

[1] Aprobado con Resolución de Secretaria de Gobierno Digital N°001-2017-PCM/SEGDI.

Introducción

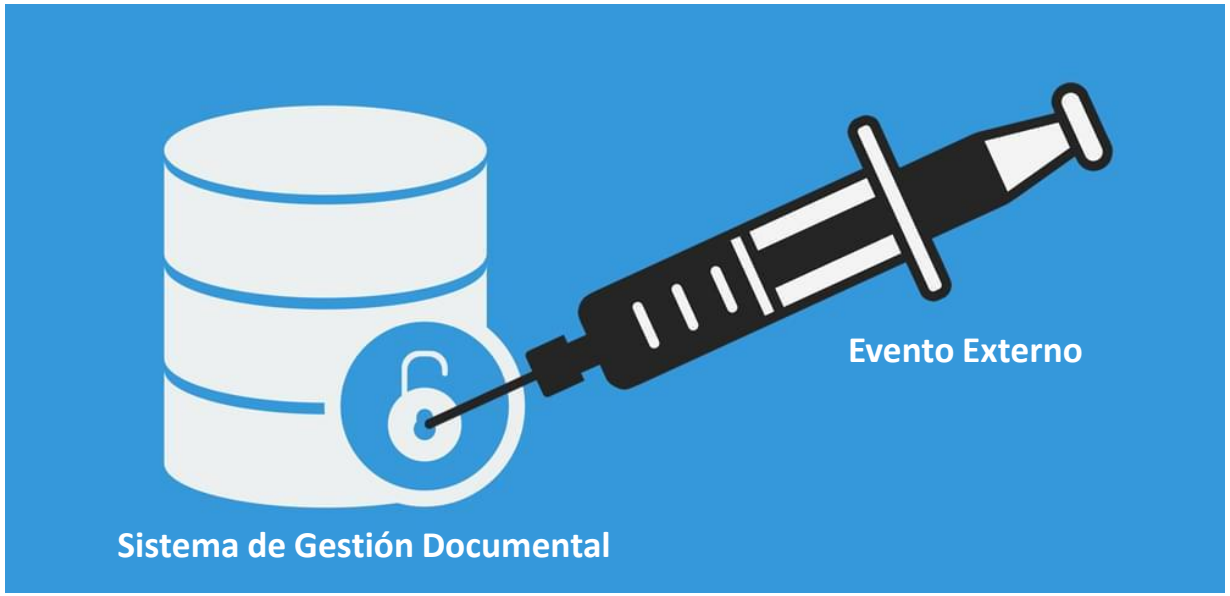
- El "Modelo de Gestión Documental"[1], indica que las entidades del Sector Público deben:
  2. Contar con un sistema de gestión documental que asegure la confidencialidad, disponibilidad[2] e integridad de los documentos.

[1] Aprobado con Resolución de Secretaria de Gobierno Digital N°001-2017-PCM/SEGDI.
[2] La Disponibilidad es la propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC 27000-2018).

¿Qué son los riesgos informáticos?

Riesgo Informático

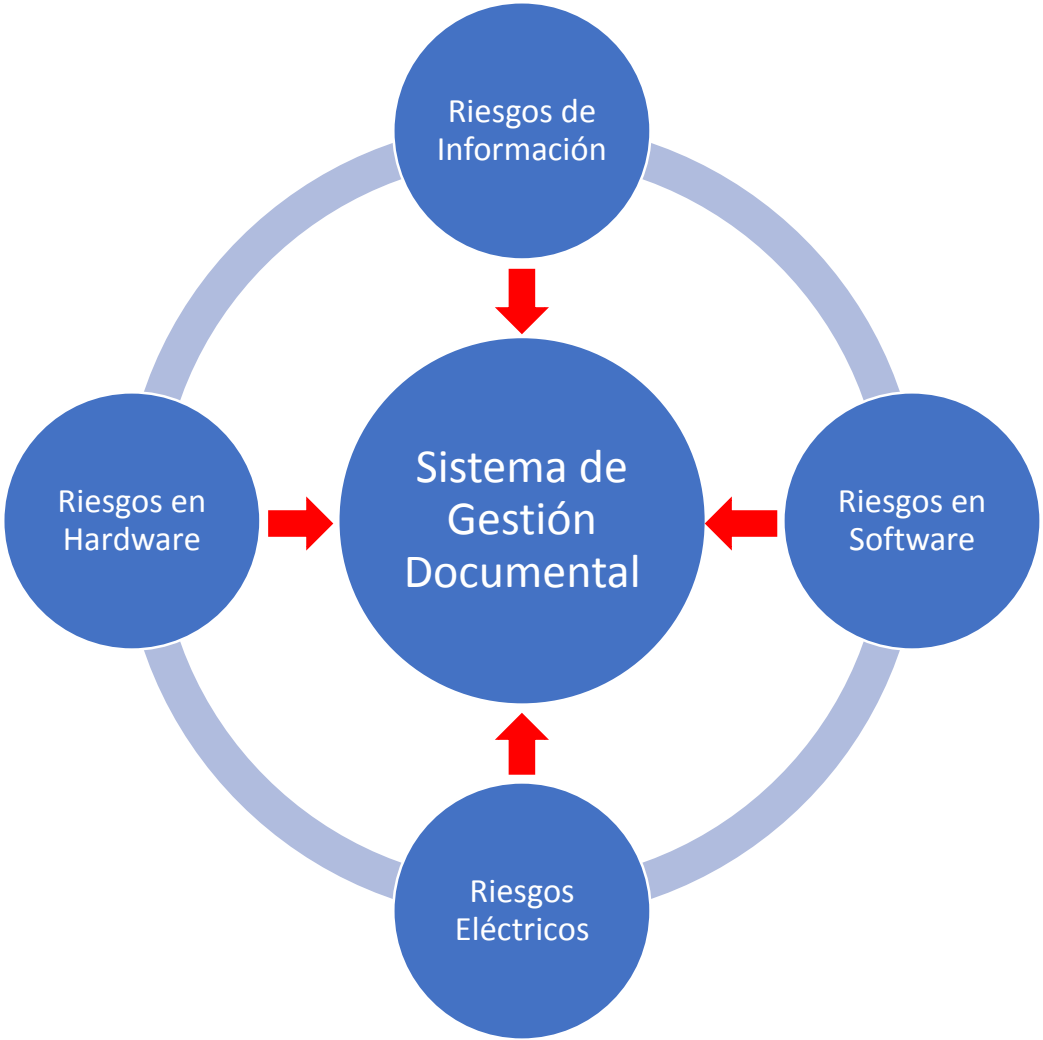
"Un riesgo informático o de tecnología es un evento o condición incierta que, si se produce, tiene un efecto negativo[1] en un sistema de gestión documental".



[1] Un riesgo también puede tener un efecto positivo.

¿Qué riesgos informáticos existen?

Riesgos Informáticos



¿Qué es la gestión de los riesgos informáticos?

Gestión de Riesgos

1. **IDENTIFICAR Riesgos.**

2. **CALIFICAR Riesgos**

3. **ESTRATEGIA para el Riesgo.**

4. **ACCIÓN para el Riesgo.**

Anexo 3 MGD: Evaluación de Riesgos

Nº	Riesgo	Categoría (1)	Probabilidad (2)	Impacto (3)	Calificación (4)	Estrategia (5)	Acción (6)
1							
2							
3							
...							
....							

Calificación del riesgo: Tomar como base la matriz de Probabilidad e Impacto.

Alto	A
Medio	M
Bajo	B

Matriz de Probabilidad e Impacto:

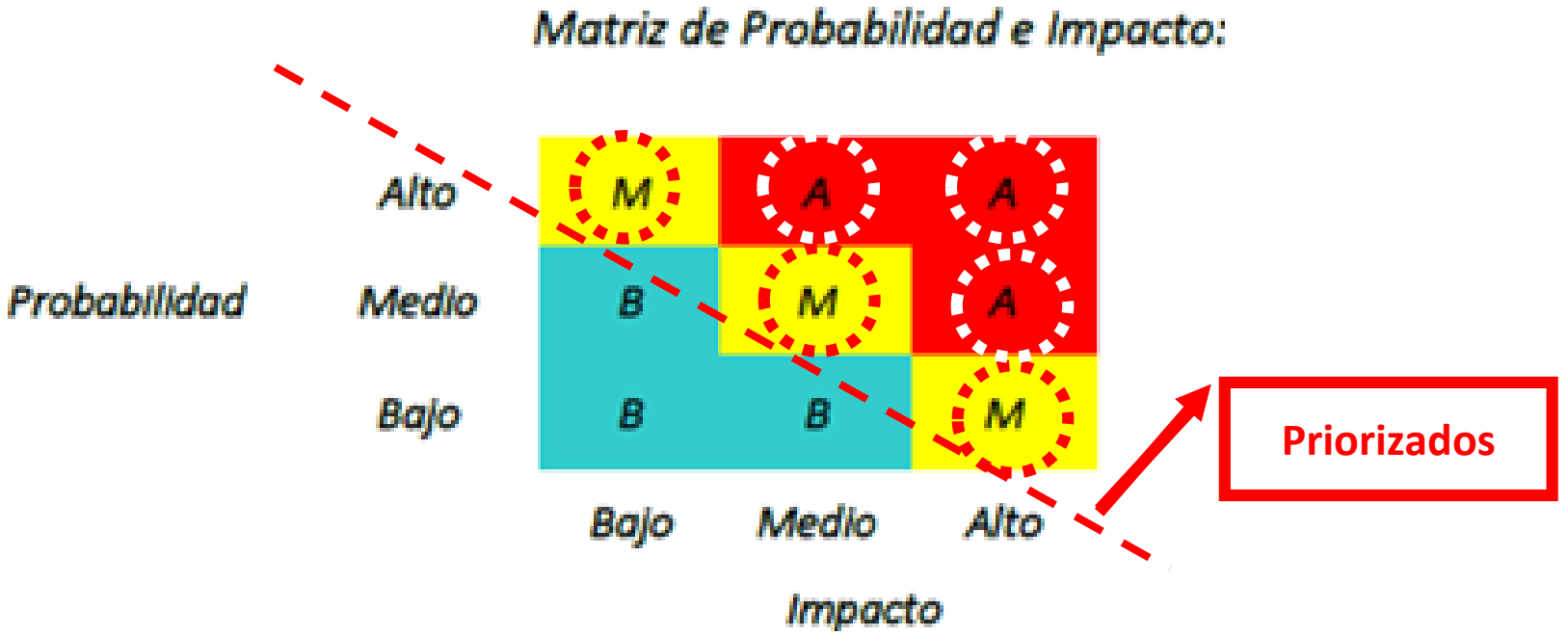
Probabilidad \ Impacto	Bajo	Medio	Alto
Alto	M	A	A
Medio	B	M	A
Bajo	B	B	M

Estrategia:

- **Aceptar:** Se acepta el riesgo y se deja que ocurra.
- **Evitar:** No se quiere que el riesgo suceda, por lo tanto se elimina; implica cambiar el plan, la actividad, el proceso. Se puede llegar a invertir recursos para evitarlo o incluso perder los beneficios u oportunidades asociados al riesgo.
- **Mitigar:** Busca bajar la probabilidad de que el riesgo ocurra y/o bajar su impacto.
- **Transferir:** Trasladar el riesgo a un tercero, solo será exitoso si el tercero a quien se le transfiere está en condiciones de manejarlo.
- **Compartir:** De manera coordinada, se asocian con otra área, entidad, proceso para enfrentar el riesgo.

Acción: Iniciativa, actividad o proyecto a realizar en base a la Estrategia definida.

Gestión de Riesgos

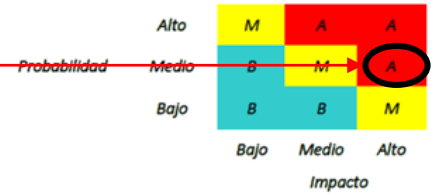


5 Casos Prácticos
Problemas y Soluciones

Caso 1

"(…) Un día el sistema dejó de funcionar y no tuvimos backups, ahora usamos el sistema de trámite desde cero (…)"

1. *Identificar Riesgo: No contar con copias de seguridad (Riesgo de información).*
2. *Calificar Riesgo: Probabilidad MEDIO / Impacto ALTO*



3. *Estrategia para el Riesgo: **MITIGAR**, bajar su impacto.*
4. *Acción para el Riesgo:*
   - ✓ *Contar con una persona en la Oficina de Informática, formalmente designada, para realizar el resguardo de la información (Backups).*
   - ✓ *Contar con un servicio de respaldo de la información (Almacenamiento en Bóveda) **MUY IMPORTANTE**.*
   - ✓ *Pueden optarse por lugares alternos distintos al institucional. **ATENCIÓN.***

Caso 1

"(…) Un día el sistema dejó de funcionar y no tuvimos backups, ahora usamos el sistema de trámite desde cero (…)"

HERMES
LA SOLUCION SEGURA

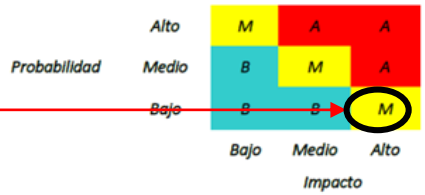
IRON MOUNTAIN®

PROSEGUR
Seguridad de confianza

Caso 2

"(…) Cuando necesitábamos el backup de documentos, lo probamos y no funcionó, perdimos la información (…)"

1. *Identificar Riesgo: Las copias de seguridad no funcionan (Riesgo de información).*
2. *Calificar Riesgo: Probabilidad BAJA / Impacto ALTO*



3. *Estrategia para el Riesgo: **EVITAR**, eliminar el riesgo.*
4. *Acción para el Riesgo:*
   - ✓ *Contar con el procedimiento formalmente aprobado de "Realizar copias de seguridad".*
   - ✓ *Probar las copias de seguridad de manera permanente. **MUY IMPORTANTE.***

Caso 2

"(…) Cuando necesitábamos el backup de documentos, lo probamos y no funcionó, perdimos la información (…)"

PERÚ Ministerio de Cultura	CONTROL DE PRUEBAS DE RESTAURACIÓN DE LA INFORMACIÓN	CODIGO: SGSI-F-013
Fecha de vigencia: 26/01/2018	USO INTERNO	FORMATO VERSIÓN: V.01

RESPONSABLE:	Patricia Valdivia Heredia	FECHA:	09/11/2018	FIRMA:

Sistema/Base de Datos/Equipo	Información restaurada	Resultado	Observaciones
Base de datos INCPROD del servidor 192.25.0.110	Copia de seguridad de fecha 04.11.2018	Integridad de la base datos exitosa	La restauración de la copia de seguridad de fecha 04.11.2018 respecto a su integridad, fue exitosa. El proceso de restauración de cinta a servidor lo realizó el Sr. Hatemm Palacios Saman y la restauración de la base de datos lo realizó la Sra. Elizabeth Mayta Nieto. Las pruebas incluyeron la validación de la información restaurada realizado por el Sr. Willy Yucra Limahuay de la Oficina de Desarrollo Tecnológico, los mismos que según lo informado no presentaron inconsistencias:

Sistemas validados	STATUS
Sistema de Boletería	OK
Sistema de Trámite Documentario	OK
SINAR	OK
CIRA	OK
PMA	OK
POSTULACIONES CAS	OK
Sistemas de Gestión de Concursos	OK
Quipu	OK

Resumen:

ASPECTOS RELEVANTES	TIPO DE INFORMACIÓN RESTAURADA Base de Datos INCPROD
Tiempo de atención de HERMES (atención por emergencia)	Inicio de restauración: 09:29 am del 09.11.2018 Contacto inicial: 10:15 del 09.11.2018 Llegada de las cintas: 12:12 del 09.11.2018 Tiempo total: 01:57 horas

PERÚ Ministerio de Cultura	CONTROL DE PRUEBAS DE RESTAURACIÓN DE LA INFORMACIÓN	CODIGO: SGSI-F-013
Fecha de vigencia: 26/01/2018	USO INTERNO	FORMATO VERSIÓN: V.01

ASPECTOS RELEVANTES	TIPO DE INFORMACIÓN RESTAURADA Base de Datos INCPROD
Tiempo de restauración de las cintas al servidor (Horas)	Escaneo en la Librería de Cinta:12:34 Termino de restauración en Librería HPE: 14:20 Tiempo total: 1:46 horas
Tiempo de Restauración de la base de datos	Nota: Considerando el empleo del ambiente del restore (192.25.0.130) para la capacitación del CIRA informado por la ODT; se solicitó que la restauración de la BD inicie en la noche. Tareas previas de restauración: 12:50 am Inicio de la restauración de la BD: 01:00 am BD restaurada 02:31 am Tiempo total de restauración: 1:31 horas
Tiempo Total de restauración (Horas)	06:32 horas
Resultado de la restauración	Exitosa
Validación de la información en los sistemas	SITD, Sistema de Boletería, SINAR, CIRA, PMA, Postulaciones CAS, Sistema de Gestión de Concursos, QUIPU Pruebas de validación conforme.
Integridad de la copia de seguridad	SI

Hatemm Palacios Saman
Analista de redes

Elizabeth Mayta Nieto
Administradora de Base de Datos

Robert Ramos Vargas
Coordinador de redes y telecomunicaciones

Willy Yucra Limahuay
Oficina de Desarrollo Tecnológico

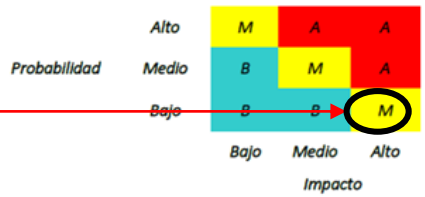
Jairo W Pinedo Pinas
Responsable de la Oficina de Informática y Telecomunicaciones

Caso 3

"(…) Cuando se va el fluido eléctrico, nunca tenemos sistema de trámite (…)"

1. Identificar Riesgo: No contar con contingencia eléctrica (Riesgo eléctrico).

2. Calificar Riesgo: Probabilidad BAJA / Impacto ALTO



*3. Estrategia para el Riesgo: **EVITAR**, eliminar el riesgo.*

4. Acción para el Riesgo:

- ✓ *Contar con un grupo electrógeno **OPERATIVO.***
- ✓ *Probar el grupo electrógeno de manera permanente. **MUY IMPORTANTE.***

Caso 3

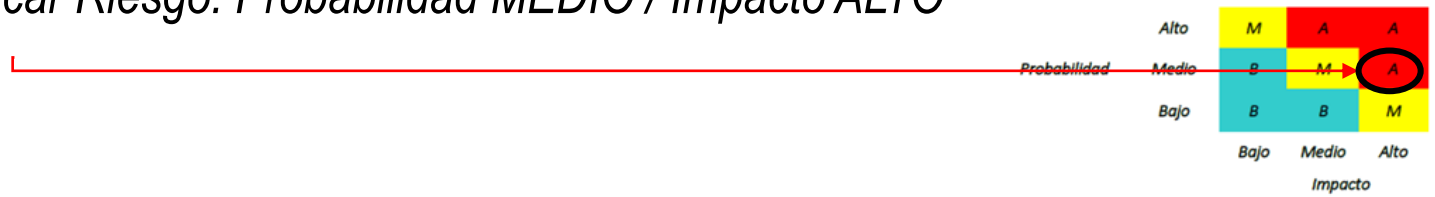
"(…) Cuando se va el fluido eléctrico, nunca tenemos sistema de trámite (…)"

Caso 4

"(…) Últimamente los servidores del sistema de trámite están fallando constantemente (…)"

1. Identificar Riesgo: Falla del sistema informático (Riesgo en Hardware).

2. Calificar Riesgo: Probabilidad MEDIO / Impacto ALTO



3. Estrategia para el Riesgo: ***COMPARTIR****, bajar su impacto.*

4. Acción para el Riesgo:

- ✓ *Contar con un servicio de soporte, garantía y mantenimiento vigente y de la marca.* ***MUY IMPORTANTE.***
- ✓ *Considerar anualmente los costos de mantenimientos a los equipos informáticos como ineludibles (Plan Anual de Contrataciones).*

Caso 4

"(…) Últimamente los servidores del sistema de trámite están fallando constantemente (…)"

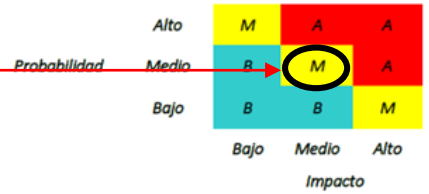
GARANTIAS EJECUTADAS 2018	
Equipo Averiado	**Costo**
Fuente de energía	S/2,000.00
Disco de Almacenamiento	S/2,000.00
Disco de Almacenamiento	S/2,000.00
Servidor de Procesamiento	S/10,000.00
Servidor de Procesamiento	S/10,000.00
Base de Servidores	S/20,000.00
Procesador	S/20,000.00
Fuente de energía	S/2,000.00
Fuente de energía	S/2,000.00
Disco de Almacenamiento	S/2,000.00
	S/72,000.00

Caso 5

"(…) Los reportes que muestra el sistema de trámite no son correctos y últimamente salen muchos errores (…)"

1. Identificar Riesgo: Falla del sistema informático (Riesgo en Software).

2. Calificar Riesgo: Probabilidad MEDIO / Impacto MEDIO



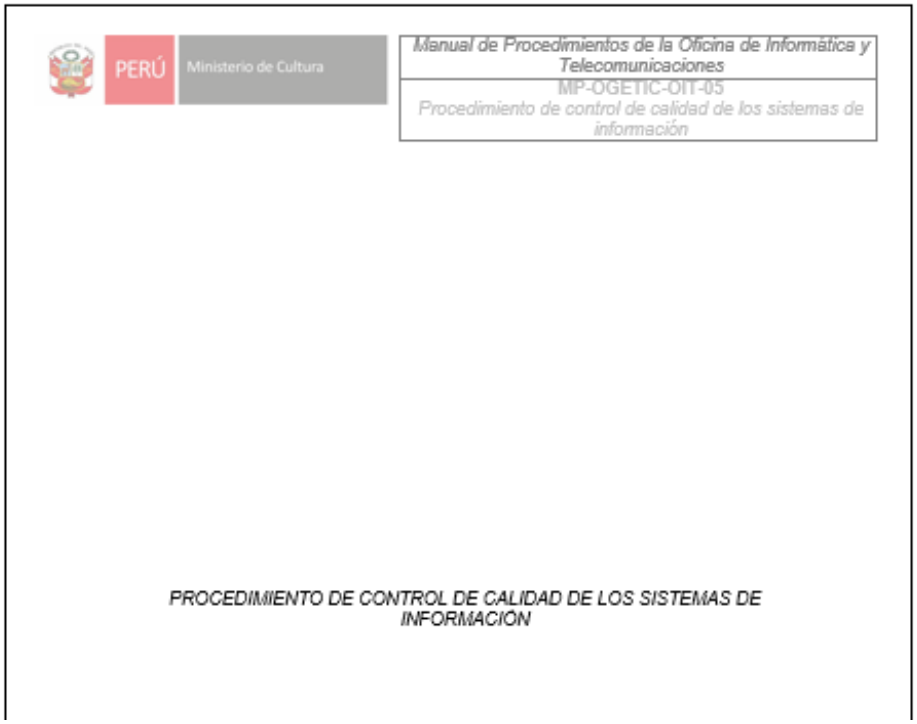
*3. Estrategia para el Riesgo: **MITIGAR**, eliminar el riesgo.*

4. Acción para el Riesgo:

- ✓ *Contar con una persona en la Oficina de Informática, formalmente designada, para realizar pruebas de sistemas(Testing).*
- ✓ *Contar con el procedimiento formalmente aprobado de "Control de calidad de sistemas de información".*

Caso 5

"(…) Los reportes que muestra el sistema de trámite no son correctos y últimamente salen muchos errores (…)"

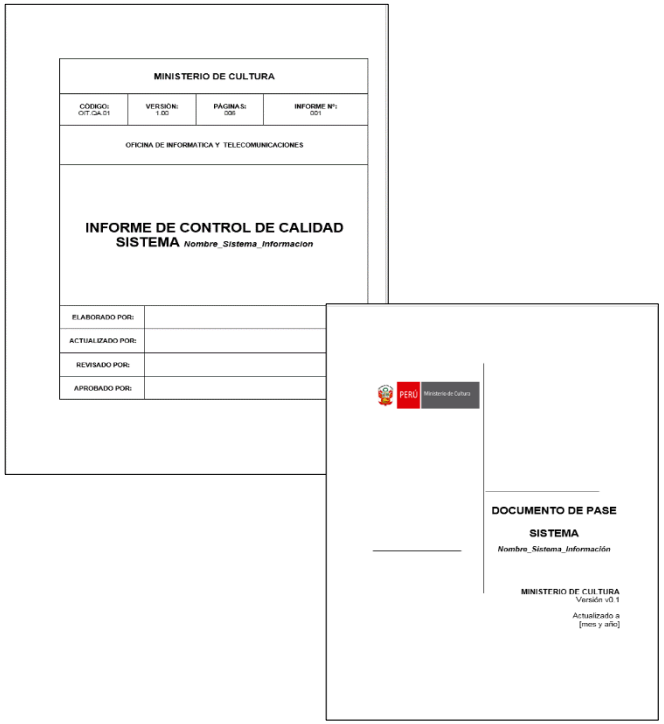

PERÚ Ministerio de Cultura

Manual de Procedimientos de la Oficina de Informática y Telecomunicaciones

MP-OGETIC-OIT-05

Procedimiento de control de calidad de los sistemas de información

PROCEDIMIENTO DE CONTROL DE CALIDAD DE LOS SISTEMAS DE INFORMACION


MINISTERIO DE CULTURA

CÓDIGO: OIT.QA.01	VERSIÓN: 1.00	PAGINA S: 006	INFORME Nº: 001

OFICINA DE INFORMATICA Y TELECOMUNICACIONES

INFORME DE CONTROL DE CALIDAD
SISTEMA *Nombre_Sistema_Informacion*

ELABORADO POR:	
ACTUALIZADO POR:	
REVISADO POR:	
APROBADO POR:	

PERÚ Ministerio de Cultura

DOCUMENTO DE PASE
SISTEMA
Nombre_Sistema_Información

MINISTERIO DE CULTURA
Versión v0.1
Actualizado a
[mes y año]

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

PERÚ Ministerio de Cultura

III SEMINARIO INTERNACIONAL DE GESTIÓN DOCUMENTAL Y ARCHIVOS 2018

"Innovación Tecnológica al Servicio de la Ciudadanía"

Gestión de riesgos informáticos en la gestión documental

Ing. Joan Palacios Ramírez
jpalacios@cultura.gob.pe

Con el apoyo de:

PERÚ Presidencia del Consejo de Ministros | Secretaría de Gobierno Digital

INSTITUTO NACIONAL DE RADIO Y TELEVISIÓN DEL PERÚ

Auspician:

IRON MOUNTAIN

UNIVERSIDAD esan

FIRMAUX DIGITAL

Image & Design

ASPARG
ASOCIACIÓN PERUANA DE ARCHIVEROS Y GESTORES DE LA INFORMACIÓN

TO.DIGITAL
TRANSFORMACIÓN DIGITAL EMPRESARIAL

GRAMD.COM
Identidad y Firma Digital con validez legal

indra

ACEPTA