CONTRALORÍA GENERAL DE LA REPÚBLICA

NIVELES DE RIESGO EN EL AMBIENTE DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

2023

SECTOR PUBLICO

INFORME

INDICE

INFORME SOBRE LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC) DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO

MUNICIPALIDAD DE KARAPAI

1. Antecedentes

Origen del informe

La Contraloría General de la República, conforme a lo que la Ley Nº 276/94 "Orgánica y Funcional de la Contraloría General de la República", formula el presente Informe.

2. Objetivos

Objetivo general

Verificar los mecanismos de control y seguridad aplicados para la protección sobre el software, hardware y la infraestructura que administra la información, de manera a definir los niveles de riesgo tecnológico existentes en los Organismos y Entidades del Estado (OEE).

Objetivos específicos

- Relevar datos sobre la situación de la gestión de las Tecnología de la Información y Comunicación (TIC) de las Instituciones del Estado, a enero de 2023.
- Identificar los niveles de riesgo tecnológico al que están expuestos los Organismos y Entidades del Estado, basados en los indicadores presentados en cada uno de los cuestionarios de control.
- Brindar conclusiones y recomendaciones a cada una de las Instituciones.

3. Alcance

Relevamiento general de datos sobre mecanismos básicos de control tecnológicos de los Organismos de la Administración Central, Descentralizada y Municipalidades, a enero de 2023.

Determinación de los niveles de riesgo tecnológico en base a los datos relevados, utilizando formulario elaborado para el efecto.

El trabajo constituyó exclusivamente un relevamiento de datos a efectos de brindar un informe referencial, no representó una auditoría, no se revisaron documentos de respaldo de las respuestas brindadas ni realizaron verificaciones in situ, sin embargo, en base a las respuestas se realizaron recomendaciones a los OEE tendientes a lograr una seguridad razonable y mantener la integridad, confiabilidad, confidencialidad y disponibilidad de la información administrada por las instituciones.

4. Limitaciones

Las limitaciones al alcance de trabajo, fueron las que surgieron como consecuencia de la falta de respuesta de modo a contar con la información completa del 100% de las Instituciones. Así mismo, las respuestas inconsistentes brindadas por algunas instituciones, o que impidieron llegar a una aproximación exacta de los riesgos existentes.

5. Base Legal

El presente Informe de la Contraloría General de la República, se elaboró sobre la base de las siguientes normativas:

1. Constitución Nacional.
2. Ley N° 276/94 "*Orgánica y funcional de la Contraloría General de la República".*
3. Decreto N° 6234 del 8/11/16 *"Por el cual se declara de interés nacional la aplicación y el uso de las Tecnologías de la Información y Comunicación (TIC) en la gestión pública, se define la estructura mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento".*
4. Resolución MITIC N° 733 del 26/12/19, *Modelo de Gobernanza de Seguridad de la Información.*
5. Resolución MITIC N° 277 del 23/06/23, *Controles sobre Ciberseguridad*
6. ISSAI 5310, Seguridad de los Sistemas de Información.
7. COBIT 5- Objetivos de control para Tecnologías de Información y Tecnologías Relacionadas.
8. ISO 27000, Marco de gestión para la seguridad de la información.
9. ISO 31000, Gestión de riesgos.

6. Proceso de Elaboración del Informe

La elaboración y aprobación del Informe comprendió las siguientes fases:

a. Recopilación de información para elaborar el Informe

Se remitió un cuestionario de control a los OEE que forman parte del Presupuesto General de la Nación, relevando datos sobre la gestión de las Tecnologías de Información y Comunicación.

b. Análisis de la información

Se realizó el análisis basado en la información recibida en los cuestionarios, asignando valor a cada una de las respuestas brindadas para lograr definir el nivel de riesgo tecnológico por área.

c. Elaboración y presentación del Informe

Posterior a la realización del análisis de la información, se ejecutaron las conclusiones por cada área y las recomendaciones correspondientes.

7. Indicadores de riesgo

En el ambiente tecnológico existen circunstancias internas y externas que amenazan a la infraestructura, los recursos, y ponen en riesgo la confidencialidad, disponibilidad e integridad de la información.

La evaluación de riesgos realizada a través de este trabajo, estableció la aplicación de indicadores en diferentes aspectos del entorno tecnológico el cual comprendió las siguientes áreas:

Evaluar, orientar, supervisar

Mediante el cual se evidenció el compromiso de la máxima autoridad con el mejoramiento del ambiente tecnológico, implementando procedimientos para que los objetivos de la Institución sean logrados, Analizadas a las necesidades de los interesados, el apoyo al establecimiento de políticas y lineamientos generales de Tecnología de la Información y Comunicación (TIC). Para este aspecto, se cuenta con 12 indicadores.

Alineación, planificación y organización

Por el que se proporciona un enfoque de gestión consistente para el cumplimiento de la misión y visión de la Institución, cubriendo las estrategias y las tácticas. Tiene que ver con identificar la manera en que TIC puede contribuir mejor con los objetivos de la Institución. Para este aspecto, se cuenta con 21 indicadores.

Entrega, servicio y soporte

Involucra la entrega en sí de los servicios requeridos, incluyendo la prestación del servicio, la administración de la seguridad y de la continuidad. Para este aspecto, se cuenta con 5 indicadores.

Supervisar, evaluar y valorar

Proporciona transparencia en el rendimiento, conformidad y conducción del ambiente de TIC hacia el logro de los objetivos del área mediante la evaluación regular de la totalidad de los procesos; para este aspecto, se cuenta con 8 indicadores.

Para todos los indicadores, el sistema de calificación del formulario está compuesto de los siguientes rangos:

RIESGO BAJO	**menor a 0,5**
RIESGO MEDIO	**de 0,50 a 1.49**
RIESGO POTENCIALMENTE ALTO	**de 1,50 a 2.49**
RIESGO ALTO	**mayor o igual a 2,50**
No aplica	

Observación: para fines de este sondeo, la calificación de las Instituciones que no presentaron las respuestas se consideró como riesgo ALTO, ya que los controles mencionados constituyen puntos básicos en ambiente de TIC.

Para obtener la calificación final del riesgo de cada Institución, se aplicó un porcentaje de ponderación teniendo en cuenta las siguientes áreas:

- Área Evaluar, Orientar, Supervisar, el porcentaje de ponderación asignado fue de 30%, por considerarse que el apoyo a nivel estratégico se constituye en un elemento fundamental para el crecimiento del entorno tecnológico.
- Área Alineación, Planificación y Organización, el porcentaje de ponderación asignado fue del 30%, por considerarse los elementos que sirven de base para la organización e implementación de controles generales en ambiente de Tecnologías de la Información y Comunicaciones, sin los cuales los controles posteriores no serían eficaces.
- Área Entrega, Servicio, Soporte, se asignó como porcentaje de ponderación el 15%, teniendo en cuenta los objetivos de control establecidos.
- Área Supervisar, Evaluar, Valorar, se asignó como porcentaje de ponderación el 20%, teniendo en cuenta los objetivos de control establecidos.

8. Cuestionamientos básicos del ambiente de TIC

Teniendo en cuenta la importancia de las TIC para cada una de las actividades, se vieron aspectos claves del cuestionario que hacen referencia a esa área, con el fin de verificar el nivel de riesgo asignado en cada uno de los casos expuestos por las Instituciones.

En la tabla siguiente se resaltan las consultas, que son básicas para los entornos de TIC en cada área analizada, las respuestas, determinaron los niveles de riesgo correspondientes.

Evaluar, Orientar, Supervisar

Ítem	Preguntas
1	¿La Institución cuenta con una unidad específica que administre el entorno tecnológico?
2	En caso que la respuesta del punto 1 sea afirmativa, ¿Depende directamente de la máxima autoridad de la Institución?
3	¿Se cumple con lo establecido en los artículos del Decreto de la Presidencia de la República-Ministerio del Interior N° 6234 del 08/11/16, "Por el cual se declara de interés nacional la aplicación y uso de las Tecnologías de la Información y Comunicación (TIC) en la Gestión Pública, ¿se define la estructura mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento"?
4	¿La Institución cumple con lo establecido en el Modelo de Gobernanza de Seguridad de la Información, de acuerdo a lo establecido en la Resolución MITIC N° 733 del 26/12/19?
5	¿La Institución tiene en cuenta la Resolución MITIC N° 277 del 23/06/2020 para establecer los controles sobre la ciberseguridad?
6	¿Se encuentra la administración de TIC alineada a los objetivos de generales de la organización?
7	¿La máxima autoridad apoya el cumplimiento de los planes estratégicos de TI?
8	¿La máxima autoridad conoce la importancia de TIC y su papel con las actividades de la Institución?
9	¿La unidad de TIC comunica sus planes a las partes interesadas de la Institución y dueños de procesos?
10	¿La unidad de TIC comunica sus actividades, retos y riesgos regularmente a la máxima autoridad?
11	¿Se realiza el monitoreo de los avances del plan estratégico y reacciona en consecuencia para cumplir con los objetivos establecidos?
12	¿Se evalúan periódicamente las estructuras, normas y procesos de TIC? Se encuentran operando efectivamente.

Alineación, Planificación y Organización

Ítem	Preguntas
1	¿Se encuentra establecida la estructura de la unidad de TIC acorde a las necesidades de la Institución?
2	¿Están las funciones y responsabilidades de las unidades de TIC definidas, documentadas y entendidas?
3	¿Los encargados de la administración de TIC hacen el seguimiento del cumplimiento de las políticas y procedimientos?
4	¿Los encargados de la administración de TIC tienen conocimientos y experiencia para cumplir con sus responsabilidades?
5	¿El área de TI cuenta con recursos humanos suficientes para apoyar de manera apropiada a las metas, objetivos de la Institución y los procesos de TIC?
6	¿Se encuentran definidos los propietarios de datos y sistemas?
7	¿La propiedad y responsabilidad de los datos fue comunicada a interesados y estos las han aceptado?
8	¿Para la gestión de TIC se ha implementado una adecuada división de roles y responsabilidades para controlar que un mismo individuo no tenga dominio de más de un proceso crítico?
9	¿La Institución ha adoptado y promovido la cultura de gestión de TIC, incluyendo el código de ética y las evaluaciones de los recursos humanos de TIC?
10	¿Se realizan socializaciones y programas de formación continua en TIC que incluyan la conducta ética, las prácticas de seguridad del sistema, las normas de confidencialidad, las normas de integridad y de las responsabilidades de seguridad de todo el personal?
11	¿Se realizó la evaluación de los riesgos referidos a los procesos informáticos y el impacto para el logro de los objetivos institucionales?
12	¿Para la evaluación de riesgos se tuvo comunicación directa y realizaron consultas a las áreas funcionales de la Institución?
13	¿Para la evaluación de riesgos se tuvo en cuenta los factores internos y externos que pueden afectar el logro de los objetivos?
14	¿Para la evaluación de riesgos, se tuvieron en cuenta los contextos: de la organización, de los departamentos, proyectos, ¿las actividades individuales y los riesgos específicos?
+15	¿Se identificaron los principales factores que contribuyen con los riesgos definidos?, por ejemplo: los puntos débiles en los sistemas y en la organización; uso masivo de tecnología; conexión a internet; usuarios poco conscientes de los riesgos etc.

Ítem	Preguntas
16	¿Los riesgos identificados proporcionan información para la toma de decisiones?
17	¿Se evaluó la probabilidad de ocurrencia de eventos y los mecanismos de acción para mitigarlos?
18	¿Se realiza una revisión y monitoreo regular del área de TIC, a fin de evidenciar que los riesgos y los mecanismos de acción siguen siendo útiles y valederos?
19	¿Se conocen las consecuencias de que las informaciones almacenadas en los sistemas sean accidental o deliberadamente modificadas, destruidas o divulgadas?
20	¿Se incluye a la unidad de TIC en todos los proyectos relacionados con sistemas, software y equipos informáticos?
21	¿Se tienen identificados los activos informáticos críticos para la provisión de servicios y resguardo de la información?

Entrega, servicio y soporte

Ítem	Preguntas
1	¿Se establece y mantiene un plan que permita a TIC responder a incidentes e interrupciones de servicio y la operación continua de los procesos críticos, para mantener la disponibilidad de la información a un nivel aceptable por la Institución?
2	¿Todos los usuarios de sistemas están identificados de manera única y tienen derecho de acceso de acuerdo con sus roles en la Institución?
3	¿Se implementaron medidas lógicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida? Ejemplo: Firewall, Antivirus, actualización de parches de seguridad, otros.
4	¿Se implementaron medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida? Ejemplo: Acceso físico, refrigeración, sistema de extinción, detector de humo, otros.
5	¿Se cuenta con plan de continuidad y contingencias?

Supervisar, Evaluar y Valorar

Ítem	Preguntas
1	¿Se realiza de forma continua evaluación y supervisión, de control interno al área de TIC?
2	¿La gestión de TIC ha establecido métricas apropiadas para gestionar con eficacia las actividades del día a día del departamento de TIC?
3	¿Los responsables de la administración de TIC, monitorean la prestación de servicios para identificar deficiencias y establecen planes de acción concretos de mejoramiento? Ejemplos: rendimiento de la red; estado físico de los equipos; detección de incidentes; calidad de los servicios; definir, documentar, acordar, monitorear, y revisar el desempeño de los servicios prestados.
4	¿Los responsables de la administración de TIC realizan revisiones independientes de sus operaciones? Ejemplos: controles de cambio a sistemas; cumplimiento de objetivos; habilitación de usuarios etc.
5	¿Existe un mecanismo de control interno para permitir el monitoreo de los proveedores de servicios tercerizados?
6	¿Se realizan copias de respaldo de los datos contenidos en las bases de datos?
7	¿Se cuenta con sitio alterno de resguardo de las copias?
8	¿Se realizan pruebas de restauración de las copias?

9. Resumen General de la Institución

Institución	Evaluar, Orientar, Supervisar	Alineación, Planificación y Organización	Entrega, Servicio, Soporte	Supervisar, Evaluar, Valorar	Riesgo por Entidad	Riesgo
MUNICIPALIDAD DE KARAPAI	3	3	3	3	3	ALTO

El riesgo ALTO implica que existe una alta probabilidad de que un evento negativo ocurra en relación con el uso de la tecnología, lo que puede resultar en consecuencias graves para una organización y la información administrada.

10. Equipo Técnico

Lic. Yassir Admen
Director General de TIC

Ing. Mabel Arriola
Jefa de Dpto. Control de TIC

MABEL ELIZABETH ARRIOLA PEREIRA
Firmado digitalmente por MABEL ELIZABETH ARRIOLA PEREIRA
Fecha: 2023.08.04 10:43:33 -04'00'

YASSIR ADMEN RAMIREZ
Firmado digitalmente por YASSIR ADMEN RAMIREZ
Fecha: 2023.08.03 11:18:43 -04'00'