PLAN DE PROYECTO

Servicio para la actualización y mantenimiento del software de escrutinios, que utiliza el Consejo Nacional Electoral, para los procesos electorales a llevarse a cabo en las vigencias 2025 y 2026

Diciembre 2025

INDRA COLOMBIA S.A.S.

Toda la información contenida en el presente documento y sus anexos tiene carácter confidencial, y sólo puede ser utilizada con el fin de ser evaluada por el destinatario (sea cliente, proveedor, colaborador, partners, etc.) de la misma y a los solos efectos de conducir los tratos comerciales, o de otra naturaleza, que motivan el envío del documento (en lo sucesivo, el "Propósito").

La información aquí presentada es propiedad de la Oferente que suscribe el presente documento, y es constitutiva de secreto empresarial (también denominado en determinadas jurisdicciones, secreto comercial), y además, puede estar protegida por derechos de autor, derechos afines, patente, modelo de utilidad y/o diseño industrial por lo que queda terminantemente prohibida su divulgación y/o transmisión a terceros sin el permiso previo, expreso y por escrito.

Se limitará al máximo el acceso a la información confidencial por parte del personal del destinatario de la misma, o del personal de aquellos terceros a los que se haya autorizado a acceder a la información confidencial, limitándose únicamente a aquellas personas cuyo acceso resulte estrictamente necesario, y debiendo el destinatario de la información confidencial garantizar que informa a dichas personas del carácter confidencial y propietario de la información así como del Propósito, asegurando que dicho personal trata la información confidencial única y exclusivamente para el Propósito, y absteniéndose de toda divulgación.

Una vez finalizado o concluido el Propósito, el cliente deberá restituir toda la información confidencial sin conservar ninguna copia de la misma, no pudiendo utilizarla de ninguna manera ni para ningún otro fin, salvo autorización previa, expresa y por escrito.

Copyright. Todos los derechos reservados. Colombia

Índice

1 Introducción 4

2 Planificación de Actividades 5

2.1 Elecciones de Congreso de la República 2026 5

2.2 Elecciones de Presidente y Vicepresidente de la República 2026 – primera vuelta 6

2.3 Elecciones de Presidente y Vicepresidente de la República 2026 – en caso de segunda vuelta 7

3 Metodología de Gestión de Riesgos 8

3.1 Alcance 8

3.2 Objetivos 8

3.3 Definiciones 8

3.4 Gestión de riesgos 9

3.5 Metodología ISO 31000:2018 10

3.5.1 Principios 10

3.5.2 Marco de referencia 11

3.5.3 Proceso 12

3.6 Criterios de evaluación activos 13

3.7 Amenazas 16

3.8 Consecuencias 17

3.9 Evaluación del riesgo inherente 18

3.10 Efectividad de controles y riesgo residual 19

3.11 Tratamiento del riesgo 21

3.12 Priorización de planes de remediación 21

1 Introducción

En este documento se describe el plan de proyecto inicial para la actualización y mantenimiento del software de escrutinio de la Comisión Escrutadora Nacional del CNE, así como del sistema de control y seguimiento al escrutinio nacional disponible en la web, durante 2026.

A continuación, se detallan las principales actividades a realizar antes de cada uno de los procesos electorales de 2026: Elecciones Legislativas (8 de marzo), Elecciones Presidenciales (31 de mayo) y eventual segunda vuelta (21 de junio).

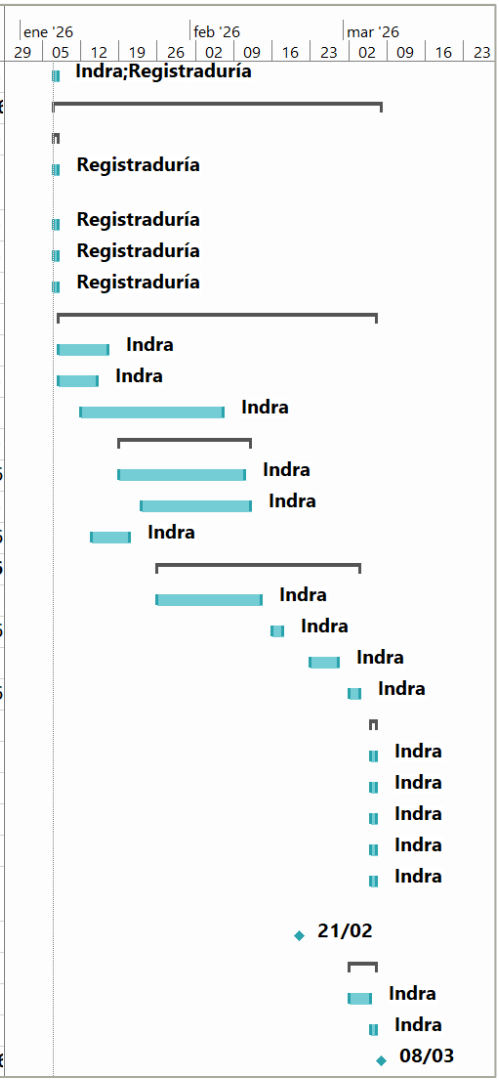
Esta planificación de actividades está basada en las fases establecidas en el plan de actualización y mantenimiento (revisión funcional, revisión de diseño gráfico, mantenimiento preventivo, auditoría, planes de pruebas, mantenimiento correctivo y entregas) y podrá ser actualizada a lo largo del proyecto.

Por último, se describe la metodología de gestión de riesgos que utilizará Indra en este proyecto.

2 Planificación de Actividades

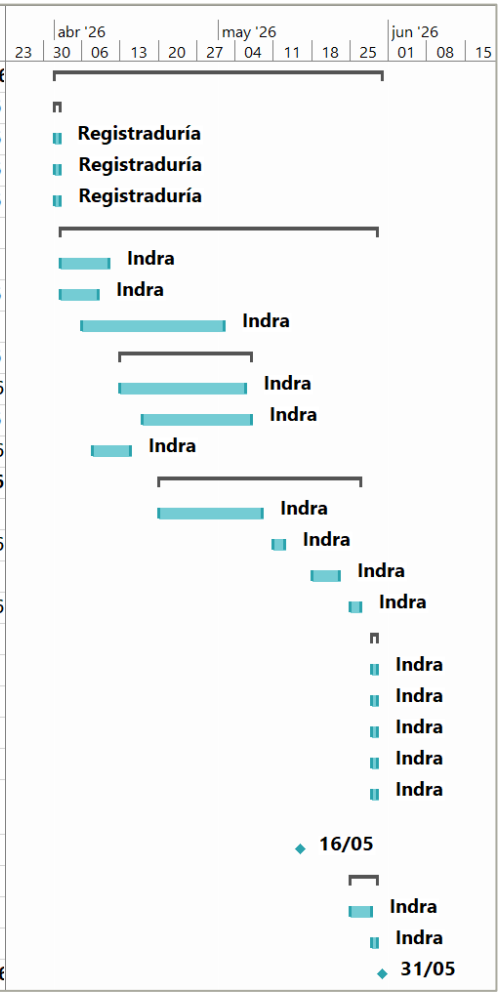
2.1 Elecciones de Congreso de la República 2026

Id	Nombre de tarea	Duración	Comienzo	Fin
1	Revisión de alcance del proyecto	1 día	mié 07/01/26	mié 07/01/26
2	**ELECCIONES LEGISLATIVAS**	**43 días**	**mié 07/01/26**	**dom 08/03/26**
3	**Información básica**	**1 día**	**mié 07/01/26**	**mié 07/01/26**
4	Software de escrutinio nacional (versión inicial)	1 día	mié 07/01/26	mié 07/01/26
5	DIVIPOLE	1 día	mié 07/01/26	mié 07/01/26
6	Listado de candidaturas y curules	1 día	mié 07/01/26	mié 07/01/26
7	Formatos E-14, E-24, E-26 y AGE Nacional	1 día	mié 07/01/26	mié 07/01/26
8	**Mantenimiento y actualización de software**	**42 días**	**jue 08/01/26**	**vie 06/03/26**
9	Revisión funcional	7 días	jue 08/01/26	vie 16/01/26
10	Revisión de diseño gráfico	5 días	jue 08/01/26	mié 14/01/26
11	Mantenimiento preventivo	20 días	lun 12/01/26	vie 06/02/26
12	**Auditoría**	**18 días**	**lun 19/01/26**	**mié 11/02/26**
13	Ejecución auditoría	17 días	lun 19/01/26	mar 10/02/26
14	Presentación informes auditoría	14 días	vie 23/01/26	mié 11/02/26
15	Planes de pruebas	5 días	mié 14/01/26	mar 20/01/26
16	**Mantenimiento correctivo**	**27 días**	**lun 26/01/26**	**mar 03/03/26**
17	Correcciones pruebas QA y auditoría	15 días	lun 26/01/26	vie 13/02/26
18	Test de release	2 días	lun 16/02/26	mar 17/02/26
19	Correcciones prueba general	5 días	lun 23/02/26	vie 27/02/26
20	Test de release final	2 días	lun 02/03/26	mar 03/03/26
21	**Entregas**	**1 día**	**vie 06/03/26**	**vie 06/03/26**
22	Software de escrutinio	1 día	vie 06/03/26	vie 06/03/26
23	Manuales	1 día	vie 06/03/26	vie 06/03/26
24	Documentación técnica	1 día	vie 06/03/26	vie 06/03/26
25	Protocolos de contingencia	1 día	vie 06/03/26	vie 06/03/26
26	Informes de auditoría y pruebas de aplicaciones	1 día	vie 06/03/26	vie 06/03/26
27	Prueba general	0 días	sáb 21/02/26	sáb 21/02/26
28	**Capacitación**	**5 días**	**lun 02/03/26**	**vie 06/03/26**
29	Funcional	4 días	lun 02/03/26	jue 05/03/26
30	Técnica	1 día	vie 06/03/26	vie 06/03/26
31	**DIA ELECTORAL**	**0 días**	**dom 08/03/26**	**dom 08/03/26**



2.2 Elecciones de Presidente y Vicepresidente de la República 2026 – primera vuelta

Id	Nombre de tarea	Duración	Comienzo	Fin
32	**ELECCIONES PRESIDENCIALES**	**43 días**	**mié 01/04/26**	**dom 31/05/26**
33	**Información básica**	**1 día**	**mié 01/04/26**	**mié 01/04/26**
34	DIVIPOLE	1 día	mié 01/04/26	mié 01/04/26
35	Listado de candidaturas	1 día	mié 01/04/26	mié 01/04/26
36	Formatos E-14, E-24, E-26 y AGE Nacional	1 día	mié 01/04/26	mié 01/04/26
37	**Mantenimiento y actualización de software**	**42 días**	**jue 02/04/26**	**vie 29/05/26**
38	Revisión funcional	7 días	jue 02/04/26	vie 10/04/26
39	Revisión de diseño gráfico	5 días	jue 02/04/26	mié 08/04/26
40	Mantenimiento preventivo	20 días	lun 06/04/26	vie 01/05/26
41	**Auditoría**	**18 días**	**lun 13/04/26**	**mié 06/05/26**
42	Ejecución auditoría	17 días	lun 13/04/26	mar 05/05/26
43	Presentación informes auditoría	14 días	vie 17/04/26	mié 06/05/26
44	Planes de pruebas	5 días	mié 08/04/26	mar 14/04/26
45	**Mantenimiento correctivo**	**27 días**	**lun 20/04/26**	**mar 26/05/26**
46	Correcciones pruebas QA y auditoría	15 días	lun 20/04/26	vie 08/05/26
47	Test de release	2 días	lun 11/05/26	mar 12/05/26
48	Correcciones prueba general	5 días	lun 18/05/26	vie 22/05/26
49	Test de release final	2 días	lun 25/05/26	mar 26/05/26
50	**Entregas**	**1 día**	**vie 29/05/26**	**vie 29/05/26**
51	Software de escrutinio	1 día	vie 29/05/26	vie 29/05/26
52	Manuales	1 día	vie 29/05/26	vie 29/05/26
53	Documentación técnica	1 día	vie 29/05/26	vie 29/05/26
54	Protocolos de contingencia	1 día	vie 29/05/26	vie 29/05/26
55	Informes de auditoría y pruebas de aplicaciones	1 día	vie 29/05/26	vie 29/05/26
56	Prueba general	0 días	sáb 16/05/26	sáb 16/05/26
57	**Capacitación**	**5 días**	**lun 25/05/26**	**vie 29/05/26**
58	Funcional	4 días	lun 25/05/26	jue 28/05/26
59	Técnica	1 día	vie 29/05/26	vie 29/05/26
60	**DIA ELECTORAL**	**0 días**	**dom 31/05/26**	**dom 31/05/26**



2.3 Elecciones de Presidente y Vicepresidente de la República 2026 – en caso de segunda vuelta

Id	Nombre de tarea	Duración	Comienzo	Fin
61	**ELECCIONES PRESIDENCIALES (EVENTUAL 2ª VUELTA)**	**15 días**	**lun 01/06/26**	**dom 21/06/26**
62	**Mantenimiento y actualización de software**	**15 días**	**lun 01/06/26**	**vie 19/06/26**
63	Revisión funcional	3 días	lun 01/06/26	mié 03/06/26
64	Revisión de diseño gráfico	3 días	lun 01/06/26	mié 03/06/26
65	Mantenimiento preventivo	9 días	mar 02/06/26	vie 12/06/26
66	**Auditoría**	**4 días**	**jue 04/06/26**	**mar 09/06/26**
67	Ejecución auditoría	3 días	jue 04/06/26	lun 08/06/26
68	Presentación informes auditoría	2 días	lun 08/06/26	mar 09/06/26
69	Planes de pruebas	3 días	mar 02/06/26	jue 04/06/26
70	**Mantenimiento correctivo**	**6 días**	**mié 10/06/26**	**mié 17/06/26**
71	Correcciones pruebas QA y auditoría	2 días	mié 10/06/26	jue 11/06/26
72	Test de release	1 día	vie 12/06/26	vie 12/06/26
73	Correcciones prueba general	2 días	lun 15/06/26	mar 16/06/26
74	Test de release final	1 día	mié 17/06/26	mié 17/06/26
75	**Entregas**	**1 día**	**vie 19/06/26**	**vie 19/06/26**
76	Software de escrutinio	1 día	vie 19/06/26	vie 19/06/26
77	Manuales	1 día	vie 19/06/26	vie 19/06/26
78	Documentación técnica	1 día	vie 19/06/26	vie 19/06/26
79	Protocolos de contingencia	1 día	vie 19/06/26	vie 19/06/26
80	Informes de auditoría y pruebas de aplicaciones	1 día	vie 19/06/26	vie 19/06/26
81	Prueba general	0 días	sáb 13/06/26	sáb 13/06/26
82	**Capacitación**	**3 días**	**mié 17/06/26**	**vie 19/06/26**
83	Funcional	2 días	mié 17/06/26	jue 18/06/26
84	Técnica	1 día	vie 19/06/26	vie 19/06/26
85	**DIA ELECTORAL**	**0 días**	**dom 21/06/26**	**dom 21/06/26**



3 Metodología de Gestión de Riesgos

En este capítulo se describe la Metodología para la Identificación y Valoración de Riesgos, aplicando medidas preventivas para reducir cualquier riesgo que se evidencie. Para esto se utiliza la metodología establecida en el estándar ISO 31000:2018 para la gestión de riesgos de seguridad.

3.1 Alcance

La metodología de Gestión de Riesgos desarrollada por Indra comprende un conjunto estructurado y detallado de procedimientos documentados, factores y/o técnicas que dirigen las actividades de Indra en relación con el servicio prestado y permiten:

- Identificación y valoración de activos.
- Establecimiento de amenazas, vulnerabilidades y ocurrencias.
- Determinar el riesgo Inherente (Probabilidad por Impacto).
- Establecimiento de controles para la mitigación del riesgo y su efectividad.
- Valoración del riesgo residual.
- Establecimiento de opciones de tratamiento (apetito de riesgo).
- Definición y priorización de planes de remediación.

3.2 Objetivos

Identificar los riesgos conocidos efectuando la valoración de la probabilidad de ocurrencia, el impacto y la creación de planes de acción para responder a los riesgos que lo requieran. Para el cumplimiento de este objetivo se deben llevar a cabo las siguientes actividades:

- Identificación de los Activos de Información.
- Identificar las consecuencias, amenazas y vulnerabilidades.
- Evaluar el riesgo inherente.
- Establecimiento de controles.
- Evaluar el riesgo residual resultante.
- Definición de planes de tratamiento de riesgos priorizados.

3.3 Definiciones

A continuación, se detallan algunos términos que se usarán con frecuencia.

- Activo(s): componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. Es todo aquel componente que tiene valor para la organización.
- Amenaza(s): circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).
- Confidencialidad: propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

- Control(es): mecanismo que permite reducir las vulnerabilidades de los sistemas.
- Disponibilidad: propiedad de la información, que garantiza el acceso a los datos en el momento, formato y tiempo que se requiera.
- Impacto: Es la consecuencia de que una amenaza se materialice sobre un activo.
- Integridad: propiedad de la información, que garantiza que los datos generados no sufren modificaciones por personal no autorizado.
- Plan de acción: documento que prioriza las iniciativas más importantes para cumplir con ciertos objetivos y metas.
- Riesgo: ponderación del valor del activo, la probabilidad de que suceda una amenaza y el impacto que tendría sobre el sistema.
- Riesgo inherente: Es aquel riesgo producto del análisis de riesgos sin tener en cuenta los controles correspondientes.
- Riesgo residual: Es aquel riesgo que queda después de aplicados los controles del riesgo inherente.
- Vulnerabilidad: Debilidad en activos que pueden ser aprovechadas por las amenazas para dañar a un activo.

3.4 Gestión de riesgos

La Gestión de Riesgos implica dos grandes tareas a realizar:

- Análisis de riesgos. Permite identificar qué es lo que se tiene y estimar lo que puede llegar a suceder.
- Tratamiento de los riesgos. Permite organizar la defensa frente a los riesgos, evitando o minimizando que nada malo suceda y preparándose para mitigar las amenazas, continuando con el negocio ante incidentes.

La gestión de seguridad se podría resumir en que es la gestión de los riesgos y que el análisis permite optimizar su gobierno.



Gestión de Riesgos

Enmarcando la gestión de riesgos dentro del estándar ISO 31000:2018, ésta cuenta con las siguientes características:

- Es iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas.
- Es parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión.
- Es parte de todas las actividades asociadas con la organización e incluye la interacción con las partes interesadas.

- Considera los contextos externo e interno de la organización, incluido el comportamiento humano y los factores culturales.
- Está basada en los principios, el marco de referencia y el proceso descritos en este documento. Estos componentes podrían existir previamente en toda o parte de la organización, sin embargo, podría ser necesario adaptarlos o mejorarlos para que la gestión del riesgo sea eficiente, eficaz y coherente.

3.5 Metodología ISO 31000:2018

Indra propone una metodología de identificación y evaluación del riesgo tecnológico para determinar el grado potencial de las amenazas que puedan materializarse, tomando en cuenta los activos de TI, las amenazas, las vulnerabilidades y los controles para determinar el riesgo y administrarlo adecuadamente.

Una de las mejores herramientas o guía establecida para gestionar el riesgo es la ISO 31000:2018, la cual establece una serie de principios, marco de referencia y Procesos que deben ser cumplidos para hacer una gestión eficaz del riesgo y también recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo (framework) o estructura de soporte, cuyo objetivo sea integrar el proceso de gestión de riesgos.

3.5.1 Principios

La gestión del riesgo eficaz requiere los elementos de la siguiente gráfica y puede explicarse de la siguiente manera:



Fuente: Estructura ISO/IEC 31000, tomado de la norma ISO/IEC 31000:2018

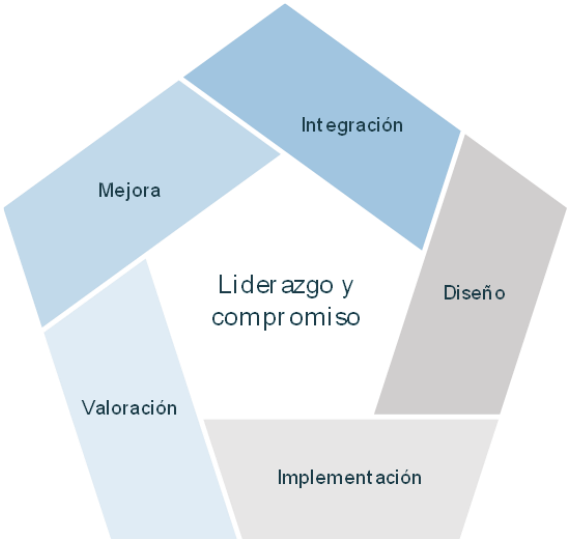
Principios de la metodología:

- Integrada: La gestión del riesgo es parte integral de todas las actividades de la organización.
- Estructurada y exhaustiva: Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.
- Adaptada: El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.
- Inclusiva: La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
- Dinámica: Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
- Mejor información disponible: Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
- Factores humanos y culturales: El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
- Mejora continua: La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

3.5.2 Marco de referencia

El propósito del marco de referencia de la gestión del riesgo es asistir a la organización en integrar la gestión del riesgo en todas sus actividades y funciones significativas. La eficacia de la gestión del riesgo dependerá de su integración en el gobierno de la organización, incluyendo la toma de decisiones. Esto requiere el apoyo de las partes interesadas, particularmente de la alta dirección.

El desarrollo del marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización. La siguiente gráfica ilustra los componentes del marco de referencia.



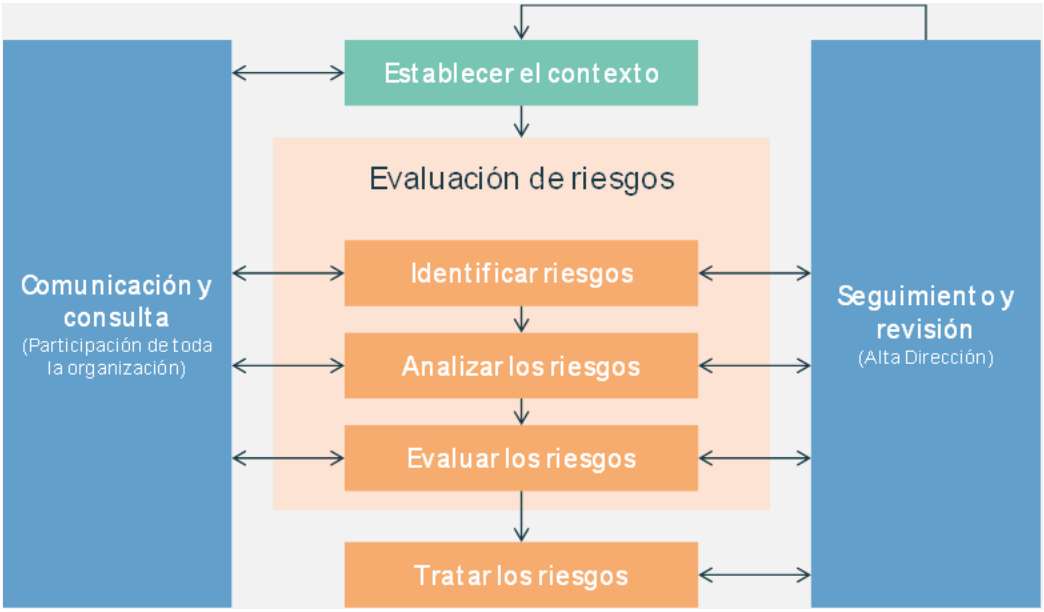
Fuente: Estructura ISO/IEC 31000, tomado de la norma ISO/IEC 31000:2018

Componentes del Marco de Referencia:

- Liderazgo y compromiso: La alta dirección y los órganos de supervisión, cuando sea aplicable, aseguran que la gestión del riesgo esté integrada en todas las actividades de la organización y deberían demostrar el liderazgo y compromiso.
- Integración: Integración de la gestión del riesgo en las estructuras y el contexto de la organización.
- Diseño: La organización analiza y comprender sus contextos externo e interno cuando diseñe el marco de referencia para gestionar el riesgo.
- Implementación: La organización implementa el marco de referencia de la gestión del riesgo.
- Valoración: Valorar la eficacia del marco de referencia para la gestión del riesgo.
- Mejora: Realizar el seguimiento continuo y adaptar el marco de referencia de la gestión del riesgo en función de los cambios externos e internos. Al hacer esto, la organización puede mejorar su valor.

3.5.3 Proceso

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. Este proceso se ilustra en la siguiente figura:



Fuente: Estructura ISO/IEC 31000, tomado de la norma ISO/IEC 31000:2018

Proceso de valoración de riesgos

A continuación, se describen las actividades a realizar:

- Establecer el contexto estratégico: consiste en la definición de parámetros básicos para la gestión del riesgo, así como el alcance y los criterios para el resto de los procesos. Algo que se debe hacer de manera ineludible desde el conocimiento de todos los aspectos que se engloban en la actividad llevada a cabo por la empresa.

- Identificar los riesgos: la empresa tiene que identificar de forma sistémica los riesgos a los que se encuentra sometida, las causas de los mismos y los posibles efectos que tendría su materialización. Se encuentran recogidas las acciones que se relacionan con la clasificación del riesgo, dependiendo de su tipología.
- Analizar el riesgo: en esta fase se establece la probabilidad de que suceda un riesgo y el impacto que generan sus consecuencias, mediante su calificación y su evaluación, con el fin de que se establezca, de la manera más eficiente posible, el nivel de riesgo y por lo tanto las acciones correctivas que se deben llevar a cabo. El éxito de este proceso depende en gran medida de la calidad de la información que se haya obtenido en la fase de identificación y el tipo de método que se haya escogido para realizar el análisis.
- Evaluar los riesgos: se deberán confrontar los resultados obtenidos a raíz del análisis del riesgo, con las medidas de control que han sido identificadas, para establecer prioridades en el tratamiento de los riesgos y poder fijar las políticas de gestión que sean más adecuadas.
- Tratamiento de riesgos: constituye la fase final. Una vez identificados, clasificados y valorados los riesgos, es el momento de establecer las opciones de gestión de riesgo que se desean implementar. Estas se encuentran articuladas en cuatro ejes diferentes: transferencia del riesgo, retención del riesgo, reducción del riesgo o evitar dicho riesgo.
- Monitorización y revisión: teniendo en cuanta de que es muy difícil que los riesgos detectados dejen de suponer una amenaza para la empresa, es imprescindible establecer los indicadores de seguimiento sobre las medidas que se establecen para la gestión de riesgos.

3.6 Criterios de evaluación activos

Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas. Pueden hacerse análisis de riesgos centrados en una única faceta, independientemente de lo que ocurra con otros aspectos. Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

En las tablas siguientes se definen los tipos de activos, los códigos correspondientes a los grados de confidencialidad, integridad y disponibilidad y el código del valor de los activos.

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Ficheros, copias de respaldo, datos de configuración, registro de actividad, código fuente, código ejecutable, datos de prueba, etc.
[S] Servicios	Función que satisface una necesidad de los usuarios.
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos, etc.
[HW] Hardware / Equipos informáticos	Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
[M] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o temporal.
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.

TIPO DE ACTIVO	DESCRIPCIÓN
[P] Personal	Personal relacionado con los sistemas de información.
[SI] Sistema de Información	Conjunto de elementos interrelacionados que permiten la obtención, procesamiento, almacenamiento y distribución de la información, para apoyar la toma de decisiones y el control en una organización.

Tipos de activos

Integridad: Para calificar los requerimientos de integridad (exactitud de la información) se definió la siguiente escala:

CÓDIGO	INTEGRIDAD	DESCRIPCIÓN
S	Sensible	Información que requiere controles estrictos para su protección
N	Normal	Información que requiere controles habituales para su protección
B	Baja	Información que requiere controles mínimos para su protección

Niveles valoración Integridad

Confidencialidad: Para calificar los requerimientos de confidencialidad (garantizar que la información solo es conocida por quien está autorizado para conocerla) se definió la siguiente escala:

CÓDIGO	CONFIDENCIALIDAD	DESCRIPCIÓN
C	Confidencial	Restringida a un conjunto de personas de la organización
I	Uso Interno	Sólo personal de la organización o terceros autorizados
P	Uso Público	Información dispuesta al público en general

Niveles valoración Confidencialidad

Disponibilidad: Para calificar los requerimientos de disponibilidad (garantía que la información puede ser accedida por quien la requiere y cuando lo requiere.) se definió la siguiente escala:

CÓDIGO	DISPONIBILIDAD	DESCRIPCIÓN
A	Alta	Tiempo tolerable de interrupción menor a 2 horas
M	Media	Tiempo tolerable mayor a 2 horas y menor a 8 horas
B	Baja	Tiempo tolerable mayor a 8 horas y menor a 5 días

Niveles valoración Disponibilidad.

Criticidad del Activo: Cuando los criterios de confidencialidad, integridad y disponibilidad se encuentren valorados en “Alto” la criticidad del activo se considerará “Critico”. En caso de tener unas valoraciones diferentes a Altos en cualquiera de los 3 criterios (Confidencialidad, integridad y disponibilidad) el activo se valorará como “No Critico”.

CONFIDENCIAL	INTEGRIDAD	DISPONIBILIDAD	VALORACIÓN ACTIVOS
Confidencial	Sensible	Alta	Alta
Confidencial	Sensible	Media	Alta
Confidencial	Sensible	Baja	Media

CONFIDENCIAL	INTEGRIDAD	DISPONIBILIDAD	VALORACIÓN ACTIVOS
Confidencial	Normal	Alta	Alta
Confidencial	Normal	Media	Media
Confidencial	Normal	Baja	Media
Confidencial	Baja	Alta	Alta
Confidencial	Baja	Media	Media
Confidencial	Baja	Baja	Media
Uso Interno	Sensible	Alta	Alta
Uso Interno	Sensible	Media	Media
Uso Interno	Sensible	Baja	Media
Uso Interno	Normal	Alta	Media
Uso Interno	Normal	Media	Media
Uso Interno	Normal	Baja	Baja
Uso Interno	Baja	Alta	Media
Uso Interno	Baja	Media	Baja
Uso Interno	Baja	Baja	Baja
Uso Público	Sensible	Alta	Media
Uso Público	Sensible	Media	Media
Uso Público	Sensible	Baja	Baja
Uso Público	Normal	Alta	Media
Uso Público	Normal	Media	Baja
Uso Público	Normal	Baja	Baja
Uso Público	Baja	Alta	Media
Uso Público	Baja	Media	Baja
Uso Público	Baja	Baja	Baja

VALORACIÓN ACTIVO	DESCRIPCIÓN
ALTA	Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Niveles clasificación activos

3.7 Amenazas

Se presenta a continuación un catálogo de amenazas posibles sobre los activos de un sistema de información.

TIPO	AMENAZA
Daño físico	Fuego
	Agua
	Contaminación
	Accidente Importante
	Destrucción del equipo o medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado
	Perdida de suministro de energía
	Falla en equipo de telecomunicaciones
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia comprometida
	Espionaje remoto
	Escucha encubierta
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información.
Acciones no autorizadas	Uso no autorizado del equipo

TIPO	AMENAZA
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Tipos de amenaza

3.8 Consecuencias

Las consecuencias son el impacto negativo derivado de la explotación de una vulnerabilidad por una amenaza. Para el presente análisis se tendrán como referencia el siguiente listado, sin limitarse a otras que puedan identificarse durante la valoración:

CONSECUENCIAS
Fraude y malversación de fondos
Toma de decisiones erradas
Sanciones
Pérdidas Financieras
Deterioro de la imagen pública.
Incumplimiento de tipo legal o contractual
Indisponibilidad de servicios, Aplicaciones y/o Base de Datos
Modificaciones no Autorizadas
Pérdida en la efectividad
Retraso en la toma de decisiones
Perjuicio a las relaciones de la Entidad con otros organismos
Pérdida de productividad de los empleados
Interrupción del servicio o del negocio
Fuga de información
Robo
Vandalismo
Pérdida de la confianza del cliente

Tipos consecuencias (Riesgos)

Para determinar la importancia de los riesgos o impactos es necesario establecer la probabilidad (frecuencia de ocurrencia) y el nivel de impacto (daño) de cada ocurrencia de amenaza. A continuación, se presentan las escalas utilizadas para calificar probabilidades y niveles de impacto.

3.9 Evaluación del riesgo inherente

La evaluación del riesgo inherente se basa en la medición del impacto y la frecuencia, es decir clasificar el riesgo según su grado de afectación y estimación de la periodicidad de ocurrencia. A continuación, se presentan las tablas para determinar la frecuencia, el impacto y el mapa de riesgos tecnológicos:

CLASIFICACIÓN	IMPACTO	DESCRIPCIÓN
5	Alto	Altas pérdidas presupuestales, pone en alto riesgo la imagen de la entidad.
4	Mayor	Pérdida significativa presupuestal, amenaza la imagen de la entidad.
3	Moderado	No amenaza la imagen de la entidad.
2	Menor	Afecta el presupuesto.
1	Bajo	Bajo.

Escalas impacto

CLASIFICACIÓN	PROBABILIDAD	DESCRIPCIÓN
100%	Alto	Certera.
75%	Mayor	Probable, se espera que ocurra.
50%	Moderado	Posible, se espera que no ocurra regularmente.
25%	Menor	No esperado, pero podría ocurrir algunas veces.
10%	Bajo	Remoto, puede ocurrir en circunstancias excepcionales.

Escalas probabilidad

De acuerdo con la categorización del riesgo por su impacto y frecuencia, se pueden usar la siguiente escala para identificar los riesgos inherentes al usar la tecnología.

			PROBABILIDAD				
			Bajo	Menor	Moderado	Mayor	Alto
			10%	25%	50%	75%	100%
IMPACTO	Bajo	1	Bajo	Bajo	Bajo	Bajo	Moderado
	Menor	2	Bajo	Bajo	Menor	Menor	Moderado
	Moderado	3	Menor	Menor	Moderado	Moderado	Mayor
	Mayor	4	Moderado	Moderado	Mayor	Mayor	Alto
	Alto	5	Moderado	Mayor	Mayor	Alto	Alto

Riesgo Inherente

El riesgo de acuerdo con su probabilidad e impacto se clasifica en el mapa de riegos como:

RIESGO INHERENTE			
RANGO	**VALOR**	**DESCRIPCIÓN**	**PRIORIDAD ATENCIÓN**
76% - 100%	Alto	Indica que el riesgo tiene una gran probabilidad de ocurrencia y un impacto crítico.	Situación crítica, posible corrección urgente.
51% - 75%	Mayor	Indica que el riesgo tiene una probabilidad de ocurrencia mayor y un impacto importante.	Implementar medidas de contingencia.
26% - 50%	Moderado	Indica que el riesgo tiene una probabilidad de ocurrencia moderada e impacto significativo.	Asegurar las medidas de control.
11% - 25%	Menor	Indica que el riesgo tiene una probabilidad de ocurrencia Menor e impacto bajo.	Monitorear constantemente el riesgo detectado para ver su comportamiento.
0% – 10%	Bajo	Indica que el riesgo tiene una mínima probabilidad de ocurrencia e impacto menor.	No intervenir a menos que un análisis preciso lo justifique.

Niveles riesgo Inherente

Dentro de las opciones de tratamientos de riesgos se evaluarán las opciones de tratarlos, transferirlos y/o aceptarlos. Los riesgos que se identifiquen como ALTOS serán tratados y se definirán los controles necesarios para mitigarlos e identificar el riesgo residual.

3.10 Efectividad de controles y riesgo residual

Los controles son las medidas utilizadas para prevenir o reducir el impacto de eventos no deseados. Por tal motivo, es necesario establecer el nivel de efectividad de los controles implementados. Para ello, cada control se debe ponderar de acuerdo con el tipo de control (Preventivo, Detectivo y/o Correctivo), y la forma en que se implementó (Automático o Manual).

A continuación, se describe cada uno de estos criterios y el peso que debe usarse para evaluar la efectividad del control:

TIPO CONTROL	DESCRIPCIÓN	RELEVANCIA
Correctivo	Permiten el restablecimiento de la actividad después de ser detectado el evento no deseable y la modificación de las acciones que propiciaron su ocurrencia.	1
Detectivo	Descubre un evento, de irregularidad o resultado no previsto, alertan sobre la presencia de riesgos y permiten tomar medidas inmediatas.	3
Preventivo	Actúa sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia.	5

ESQUEMA IMPLEMENTACIÓN	DESCRIPCIÓN	RELEVANCIA
Manual	El control necesita 100% de la intervención de las personas.	1
Semi automático	El control es automático, pero requiere de la intervención de una persona.	3

ESQUEMA IMPLEMENTACIÓN	DESCRIPCIÓN	RELEVANCIA
Automático	El control no requiere de la intervención 100% de una persona. El objetivo es que la mayoría de los controles que se implementen tengan esta característica.	5

Contexto controles

La escala de efectividad de los controles se debe entender de la siguiente manera:

EFECTIVIDAD CONTROL	DESCRIPCIÓN
1%-10%	Los controles existentes pueden contrarrestar situaciones particulares, pero son insuficientes. Se requieren medidas de control adicionales en el corto plazo.
11%- 25%	Los controles existentes pueden contrarrestar situaciones especiales, pero son insuficientes. Se requieren medidas de control adicionales en el mediano plazo.
26% -50%	Los controles existentes brindan un nivel de protección medio. Son insuficientes. Se requieren controles adicionales en el mediano plazo para elevar los niveles de protección.
51% - 75%	Los controles existentes brindan un nivel de protección alto. Son insuficientes. Se requieren controles adicionales en el largo plazo para elevar los niveles de protección de los activos.
76% - 100%	Los controles existentes son altamente efectivos. Las buenas prácticas indican que su aplicación previene o detecta y corrige la mayoría de las ocurrencias de la amenaza analizada.

Efectividad controles

Para el cálculo del riesgo residual se procede a analizar el riesgo inherente y la efectividad de los controles implementados. En la siguiente grafica se muestra la escala para determinar el nivel de riesgo residual:

			PROBABILIDAD				
			Bajo	Menor	Moderado	Mayor	Alto
			1 - 10%	11 - 25%	26 - 50%	51 - 75%	76 - 100%
RIESGO INHERENTE	Alto	1	Alto	Alto	Mayor	Mayor	Moderado
	Mayor	2	Mayor	Mayor	Moderado	Moderado	Menor
	Moderado	3	Moderado	Moderado	Menor	Menor	Bajo
	Menor	4	Menor	Menor	Menor	Bajo	Bajo
	Bajo	5	Bajo	Bajo	Bajo	Bajo	Bajo

Efectividad controles

3.11 Tratamiento del riesgo

Una vez identificados los riesgos y los controles a implementar se procederá a determinar las opciones de tratamiento de riesgo teniendo en cuenta las opciones de tratamiento que se pueden implementar:

OPCIONES	DESCRIPCIÓN
Mitigación	Implementar los controles de seguridad identificados.
Transferir	Adquisición de una póliza de seguro y transferimos el riesgo a la compañía de seguros que nos la ha vendido.
Evitar	Paralizando aquella actividad que supone demasiado nivel de riesgo o haciéndola de una manera diferente.
Aceptación	Esta opción sería para aquellos casos en lo que el coste de eliminar el riesgo es mayor que el daño que causará.

Opciones de tratamiento de riesgo

Para cada riesgo identificado se debe establecer la opción de tratamiento, la cual debe quedar completamente documentada y justificada por parte de Indra con aprobación de la Registraduría.

3.12 Priorización de planes de remediación

Teniendo en cuenta el nivel de riesgo identificado, se prioriza la implementación de los planes de remediación de la siguiente forma:

PRIORIDAD	DESCRIPCIÓN
Alta	Se priorizarán los planes de remediación para reducción el nivel de riesgo actual.
Moderada	Informe con los resultados de valorar los riesgos de los activos de información. Se identificarán las vulnerabilidades, consecuencias, amenazas, nivel de riesgo inherente, controles a implementar y el nivel de riesgo residual.
Baja	Se les hará únicamente seguimientos periódicos. Esto no los excluye de futuras evaluaciones en las que pueda cambiar sus valores de impacto y probabilidad de ocurrencia y sea necesario identificar e implementar las acciones de mitigación y tratamiento necesarias para llevarlos nuevamente a valores aceptables.

Priorización planes de tratamiento

Los planes de tratamiento de riesgos deberán indicar los controles a implementar, los responsables de la implementación, fechas de implementación, nivel de avance de las actividades, entre otros.

REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

INDRA COLOMBIA S.A.S.