Ingenia global

PROPUESTA DE SERVICIOS

Assessment en Ciberseguridad

Tercer Tribunal Ambiental de Chile

Enero de 2019

Ref.: POT1245

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Tercer Tribunal Ambiental - Assessment en Ciberseguridad	1.00	Primera versión.	24/01/2019

CONTROL DE DIFUSIÓN

AUTOR/ES: Ingenia Global Ltda.
DISTRIBUCIÓN: TERCER TRIBUNAL AMBIENTAL

INDICE

1 Características generales

1.1 Identificación de la oferta

Dar cumplimiento a los requerimientos solicitados por TERCER TRIBUNAL AMBIENTAL.

- **Objetivo general:** Realizar una evaluación de los procesos, plataformas de seguridad y sistemas críticos del Tercer Tribunal Ambiental, que se encuentra en las ciudades de Valdivia, contra la norma y buenas practicas de la ISO/IEC 27.001:2013, ISO/IEC 27032:2012 (Ciberseguridad), NIST (Ciberseguridad), SANS (Ciberseguridad), ISO 22301:2012, Cobit 5 y el Ciclo de Desarrollo de Software Seguros, que entregue visibilidad de todas las oportunidades de mejora de la Institución.

- **Objetivos específicos:**

    - Objetivo específico 1: Revisar, analizar y evaluar las plataformas de seguridad, sus sistemas críticos y planes de continuidad de negocio para los diversos procesos críticos que la Institución posee, en el contexto de los distintos escenarios de desastre identificados, con el objeto de asegurar la continuidad operacional ante un incidente de ciberseguridad.

    - Objetivo específico 2: Revisar, analizar y evaluar la cultura en la organización respecto a la concientización en ciberseguridad de sus empleados, gestión de incidentes de ciberseguridad, manejo de crisis, aplicabilidad de las contingencias y recuperación ante desastres operacionales y tecnológicos que permitan a TERCER TRIBUNAL AMBIENTAL, seguir brindando sus servicios.

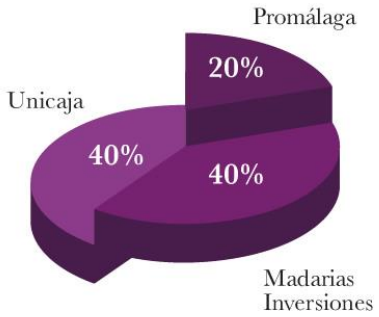
La finalidad de la presente propuesta de servicios desarrollada por INGENIA GLOBAL para TERCER TRIBUNAL AMBIENTAL, es mejorar y fortalecer las debilidades que puedan detectarse de la evaluación de ciberseguridad y recuperación ante desastres (DRP) que la Institución posee, a través de un proceso de levantamiento, evaluación y mejora en la estrategia de implementación de estos planes.

1.2 Breve presentación de Ingenia y sus referencias

En este apartado se aporta una visión general de la Institución. Puede consultarse toda la información pública disponible en el sitio web corporativo: www.ingeniaglobal.cl

Ingenia es una Institución internacional especializada en el sector de nuevas tecnologías, especialista en servicios de consultoría TI y seguridad estratégica, ciberseguridad, desarrollo de software y desarrollo web, infraestructura de comunicaciones y audiovisuales y servicios y soluciones e-learning.

Fundada en 1992, es decir, con más de 25 años de experiencia en el sector TIC, y localizada en el Parque Tecnológico de Andalucía, sus socios son Unicaja Banco, Madarias Inversiones y Promálaga.



- Misión:

Ser una Institución líder en tecnologías de la información, comunicaciones e Internet; motor de riqueza, innovación y desarrollo para nuestra sociedad.

- Visión:

Ingenia es una Institución de servicios integrados que transforma las posibilidades de la tecnología en valor para sus clientes, mediante soluciones innovadoras en sistemas de información, comunicaciones e Internet.

Vea a continuación un vídeo promocional del Grupo Ingenia

www.ingeniaglobal.cl

http://www.youtube.com/watch?v=l3aNkl23kHk

A continuación, se mencionan las principales líneas de negocio de Ingenia.

Ingenia actúa y ejecuta proyectos de toda índole distintas partes del mundo:

Ingenia, con **cerca de 350 empleados**, posee capacitación y acreditaciones suficientes para acometer con un nivel de calidad óptimo los trabajos de consultoría objeto de la propuesta, como lo demuestran las certificaciones/acreditaciones:

- Certificación de Sistema de Gestión de la Seguridad de la Información (ISO 27001:2013).
- Certificación Gestión de Servicio TI: UNE-ISO/IEC 20000-1:2011
- Certificación de Calidad (ISO 9001:2008)
- Certificación Medioambiente (ISO 14001:2004).
- Certificación de calidad en la Formación online (Norma UNE 66181:2008).
- Certificación en desarrollo software (CMMI nivel 3).

Adicionalmente, y como un indicador más de las capacidades de la Institución en el sector de la seguridad de la información, Ingenia está adherida a estándares y organizaciones relacionados con la seguridad informática, en concreto:

- **ISMS Forum**: Asociación Española para el Fomento de la Seguridad de la Información "https://www.ismsforum.es/miembros/miembros_panel.php".
- **E-sec**: Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza http://www.idi.aetic.es/esec/es/inicio/plataforma_esec/Presentacion/contenido.aspx.
- **ISACA**: Asociación de control y auditorías de sistemas de información (Information Systems Audit and Control Association)

  "http://www.isaca.org".

 **Chile**

Durante 2011 (Primer semestre), abrimos la sede de Santiago de Chile.

Adjudicatarios del Convenio Marco de Servicios de Comunicación Digital y Sitios Web no Transaccionales.

Algunos de nuestros **Clientes y Proyectos**:

- **Senado de la república de Chile**-Servicios de Asistencia Especializada de Seguridad (SOC, Auditorias de seguridad)
- **TRICOT**-Servicios de Asistencia Especializada de Seguridad (SOC, PCI-DSS compliant).
- Consultoría para la aplicación de un diagnóstico en base a la norma NCh 27001:Of. 2009, la elaboración de un plan general de seguridad trienal y la elaboración e implementación del programa de trabajo en el **Servicio del Registro Civil de Chile**.
- Consultoría de Implantación de la norma ISO 27001 en **Casa de Moneda de Chile**

- Plan de Sistemas y Plan de Seguridad basado en la norma ISO 27002 (basada en Anexo A de la norma NCh-ISO 27001) para los sistemas de información del **Gobierno Regional de Arica y Parinacota** (Chile).
- Consultoría experta en seguridad de la información para apoyar en la Implementación del Sistema de Gestión de la Seguridad de la Información (NCh-ISO 27001) en el **Gobierno Regional de Atacama** (Chile): Plan de Seguridad y desarrollo del marco normativo.
- Desarrollo del Plan Informático para la **Subsecretaría para las Fuerzas Armadas**, en el que se incluye definición de procesos TI en base a buenas prácticas, definición de roles y puestos, mejoras en seguridad de la información (NCh-ISO 27001 e ISO27002), mejoras en infraestructura y arquitectura TI.
- Consultoría de levantamiento y definición de aplicación y arquitectura del nuevo sistema informático para juzgados (**Corporación Administrativa del Poder Judicial**).
- **ONEMI** – Proyecto e-learning en el ámbito de formación y diseño instruccional. Portal web Corporativo + mantención. www.onemi.cl
- **Banco de Chile** – Desarrollo APP para tablets.
- **Clínica las Condes** – Desarrollo aplicaciones IOS y Android.

Perú

- Análisis de vulnerabilidades para el Ministerio de Educación del Perú
- Fase inicial para la implantación de un SGSI de acuerdo con la norma NTP-ISO/IEC 27001 en Ministerio de Educación del Perú
- Auditorías de certificación de la norma ISO 27001 para varios organismos públicos y privados en el Perú, en colaboración con una entidad certificadora de carácter internacional.

En **Seguridad y Consultoría TI**, podemos cubrir de forma altamente especializada cualquier requisito de seguridad, ya sea asociado a la infraestructura TI, las aplicaciones software, a la sensibilización y capacitación del personal, a necesidades de índole legal, entre otros. Algunos de nuestros productos y servicios son:

- **Servicios de Consultoría:**
  - Auditoria & Compliance:
    - Auditorias de Sistemas y Procesos de Información.
    - Gobierno Corporativo y Gobierno TI.
    - Cumplimiento de Regulaciones.
    - Análisis GAP en los Procesos de Negocios.
    - Implementación de Modelos de Madurez & Gestión de Procesos.
  - Consultoría en:
    - Seguridad de la Información y Ciberseguridad.
    - **Auditoría de Riesgo TI y Operacionales.**
    - Gestión de Riesgo TI y de las Operaciones.
    - Continuidad Operativa del Negocio.
    - Planificación Estratégica y Balance Scorecard.
    - Ethical Hacking y Phising Ético.

- **Productos:**
  - **ePulpo:** es una plataforma web desarrollada por Ingenia diseñada para la gestión TI y la seguridad de la información en una organización. Permite mantener en una sola plataforma: Inventario y Gestión de Activos, Gestión de Tickets, Análisis y Gestión de Riesgos, Gestión de Planes de Acción, Gestión Documental, Generación de Informes y Generación de Cuadro de Mando.

2 Marco Metodológico

La consultoría contempla a lo menos la revisión de proyectos e iniciativas de Ciberseguridad, Riesgo Operacional y Tecnológico (estatus e impacto), revisión de la estructura de la gerencia (roles y perfiles adecuados), gaps encontrados, revisión de los procesos críticos y sus sistemas, proveedores críticos, lógica de externalización, y del apetito al riesgo, entre otros relevantes.

La Metodología que utilizará INGENIA GLOBAL se encuentra basada en la norma **ISO 31000:2018** el cual proporciona un marco de trabajo respecto a la Gestión de Riesgos. Por último, como complemente consideraremos incluir una mirada a **COSO ERM**, con el objeto de contar con un marco integrado de administración de riesgos en el entorno de Gobierno TI y su relación con el Gobierno Corporativo.

Para realizar nuestra **Consultoría**, lo primordial es comprender la situación de la Institución, como se involucra las Tecnologías de la Información en el quehacer de cada área de la Institución, y que tan importante son las TI para el desarrollo del Servicio. Esta mirada nos permitirá determinar aquellas desviaciones respecto a las normas y buenas prácticas existentes en el mercado, posibilitando además encontrar oportunidades de mejora de los procesos internos.

A continuación, presentamos un breve resumen de las normas, buenas prácticas y herramientas a consideradas en nuestra Auditoría de Sistemas:

- **COBIT 5**

  Este código de buenas prácticas proporciona un marco integral para las organizaciones con el objeto de que logren cumplir sus metas y que puedan entregar valor mediante un gobierno y una administración efectiva de las Tecnologías de la Información, manteniendo para esto un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

  Los 5 principios de COBIT 5 son:

1. Satisfacer las necesidades de las partes interesadas, para esto, las necesidades de las Partes Interesadas deben ser transformadas en una estrategia accionable para la Organización, a través de la definición de metas, cuyo principal beneficio es definir las prioridades para implementar, mejorar y asegurar el Gobierno TI.
2. Cubrir la Institución de forma integral, esto significa que integra el gobierno corporativo con el gobierno TI. Para esto trata las tecnologías de la información como activos que necesitan ser manejados como cualquier otro activo, por todos en la organización.
3. Aplicar un solo marco integrado, ya que se encuentra alineado con los últimos marcos de trabajo y normas existentes en el mercado tales como: COSO, COSO ERM, ISO 9001, ISO 27001, ISO 27032, ISO 31000, PMBOK, PRINCE2, CMMI, entre otros.
4. Habilitar un enfoque holístico, a través de habilitadores (por ejemplo: procesos, estructuras organizacionales, principios y políticas, infraestructura y aplicaciones, entre otros), que interconectadas entre si permiten conseguir los objetivos principales de la organización.
5. Separar el gobierno de la administración, tomando como criterio lo siguiente: El **Gobierno** asegura que se **evalúen** las necesidades de las partes interesadas, así como las condiciones y opciones, para determinar los objetivos corporativos balanceados acordados a lograr; fijando directivas al establecer prioridades y tomar decisiones; así como monitorear el desempeño, cumplimiento y progreso comparándolos contra las directivas y objetivos fijados; mientras **la Administración planifica, construye, ejecuta y monitorea** las actividades conforme a las directivas fijadas por el Gobierno para lograr los objetivos de la Institución.

- **ISO 22301:2012**

La norma **ISO 22301:2012** el cual especifica los requisitos para configurar y gestionar de forma eficaz un **Sistema de Gestión de la Continuidad de Negocio (BCMS)** al interior de las organizaciones.

La Gestión de la Continuidad del Negocio (BCMS) involucra a toda la organización en relación con la planificación y la gestión de recursos, así como la generación y tratamiento de procedimientos clave, permitiéndole garantizar la seguridad de su personal y salvaguardar los intereses de sus clientes y accionistas, su reputación y su situación financiera en caso de crisis.

El término "Crisis" es usado para todos los incidentes y eventos que amenazan con causar graves interrupciones de los procesos de negocio, lo que a su vez se refleja en un potencial impacto en los ámbitos financiero, normativo y/o reputacional. En el contexto de BCMS, se refiere a las crisis a aquellas que están relacionadas con las interrupciones de los procesos de negocio debido a la falta o a la indisponibilidad de los recursos humanos, sistemas de TI, servicios e instalaciones.

El conjunto completo de Planes de Continuidad de Negocio (BC) y acuerdos (por ejemplo, Análisis de Impacto en el Negocio (BIA), Plan de Gestión de Crisis, Planes de Recuperación ante Desastres (DRP), el Plan de Comunicación de Crisis) constituyen el marco de trabajo del **Plan de Continuidad de Negocio (BCP)**.

El Plan de Continuidad de Negocio (BCP) es un documento elaborado por las distintas entidades que componen la organización, en el cual se busca proporcionar procedimientos específicos para mantener las operaciones del negocio, mientras se realiza la recuperación. El BCP se orienta a cada uno de los procesos de negocio de la Institución, para lo cual cada unidad o área deberá determinar aquellos procesos considerados como críticos. Se considera involucrar a las Tecnologías de la Información en el caso que se requiera soporte de sistemas y comunicaciones para los procesos de negocio.

El **Plan de Recuperación de Desastres (DRP),** es un documento que posee diversos procedimientos detallados para la recuperación de los sistemas de información que afectan o están involucrados en los diversos procesos de negocio. Para elaborar este plan, se analizan los diversos riesgos y amenazas que pueden afectar a la plataforma que soporta los procesos de negocio, y se detalla en él, cada una de las acciones a realizar para mitigar los efectos de la contingencia y los procesos de regreso al estado

normal de funcionamiento. Como parte de los planes de recuperación de desastres, se pueden señalar:

- Cambio de sitio por contingencia.
- Uso de servidores de respaldo.
- Enlaces redundantes.
- Almacenaje de respaldos en sitios alternativos, etc.

- **ISO 27032:2012**

Esta norma, establece un nuevo estándar de ciberseguridad publicada en Julio de 2012 por La Organización Internacional de Normalización (ISO).

La Norma ISO/IEC 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" ofrece unas líneas generales de orientación para fortalecer el estado de la Ciberseguridad de la Institución, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con:

- La Seguridad en la Redes.
- Seguridad en Internet.
- Seguridad de la información.
- Y la Seguridad de las Aplicaciones.

- **ISO 31010:2018**

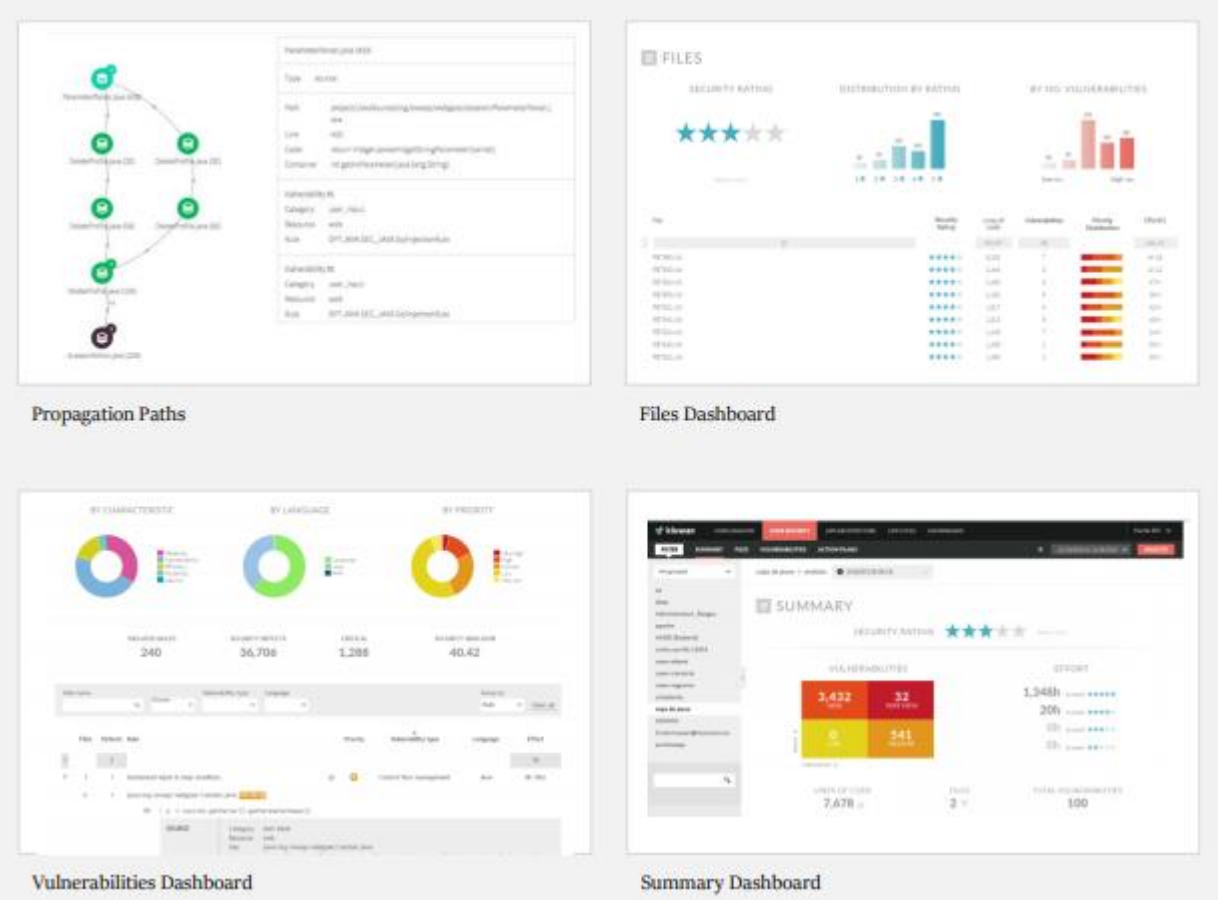
Esta norma, proporciona directrices sobre la selección y la aplicación de técnicas sistemáticas para la valorización del riesgo en una organización y es de apoyo a la norma ISO 31000:2018, que otorgar principios y directrices sobre la gestión de riesgos.

El propósito de la valorización del riesgo es suministrar información y análisis con base en evidencias para tomar decisiones informadas, sobre la manera de tratar los riesgos particulares y de seleccionar entre diversas opciones.

Algunos de los beneficios principales de llevar a cabo la valorización del riesgo incluyen:

- Entender el riesgo y su impacto potencial en los objetivos;
- Brindar información para aquellos que toman decisiones;
- Contribuir a la comprensión de los riesgos con el objeto de facilitar la selección de las opciones de tratamiento

- **Herramienta - Code Security (SAST)**



Propagation Paths | Files Dashboard

Vulnerabilities Dashboard | Summary Dashboard

- **COSO ERM (Marco Integrado de Administración de Riesgos Corporativos)**

Este marco de trabajo provee la definición, principios, criterios y componentes de un proceso de administración de riesgos corporativos. Es un proceso efectuado por el Directorio, Gerencia y otros miembros del personal, aplicado en el establecimiento de la estrategia y a lo largo de la organización, diseñado para identificar eventos potenciales que puedan afectarla y administrar riesgos de acuerdo con su apetito de riesgo, de modo de proveer seguridad razonable en cuanto al logro de los objetivos de la organización.

Al relacionar COSO ERM con los requerimientos a cumplir en el Gobierno TI, estos se alinean perfectamente, dado que, si la organización ya ha aplicado este marco de trabajo, desde la Alta Gerencia se habrá fijado los lineamientos respecto a las

definiciones del apetito de riesgo y la tolerancia que tendrá la Institución, por lo que estas mismas definiciones entonces serán aplicables al análisis de riesgos que realice el Gobierno TI respecto a los activos de información y procesos involucrados.

Definición de Función		Gobierno del Riesgo			Evaluación de Riesgo			Respuesta de riesgo		
Función	Definición Sugerida	Visión comun del riesgo	Integración con ERM	Decisiones concientes - riesgo	Recopilar datos	Analisis del riesgo	Mantener perfil del riesgo	Articular riesgo	Gestión de Riesgos	Acontecimientos de riesgo
Consejo	El grupo de los más altos ejecutivos y / o no-ejecutivos de la organización que son responsables de la gestión de la organización y tener el control total de sus recursos.									
(CEO) Director Ejecutivo	El más alto rango oficial que se encarga de la gestión total de la organización									
(CRO) Responsable de riesgos	Supervisa todos los aspectos de la gestión de riesgos en toda la organización. Un oficial de los riesgos, puede ser establecido para supervisar los riesgos relacionados con la TI									
(CIO) Responsable de TI	El más alto funcionario de la organización que es responsable de TI para la promoción; la alineación de TI y las estrategias organizacionales y la planificación, la asignación de recursos y la gestión de la prestación de los servicios de TI, la información y el despliegue de los recursos humanos asociados. El CIO normalmente preside el consejo de gobierno que maneja la cartera.									
(CFO) Responsable Financiero	El más alto funcionario de la organización que es responsable de la planificación financiera, el mantenimiento de registros, relaciones con los inversores y los riesgos financieros									
Comité de organización de riesgo	El grupo de ejecutivos de la organización que son responsables de la organización a nivel de la colaboración y el consenso necesario para apoyar las actividades de gestión de riesgos y decisiones. Un consejo de los riesgos puede ser establecido para examinar los riesgos con más detalle y asesorar al comité de organización de riesgo.									
Gestión de organizacion	Personas con funciones de negocio relacionadas con la gestión de (un) programa (s)									
Propietario de procesos de negocio	La persona responsable de la identificación de los requisitos del proceso, diseño y proceso de aprobación de la gestión de proceso de ejecución. En general, un proceso de negocio debe ser titular en un nivel suficientemente elevado en la organización y tener autoridad para comprometer recursos para el proceso específico de las actividades de gestión de riesgo.									
Funciones de control de riesgos	Las funciones en la organización responsable de la gestión de los dominios específicos de riesgo (por ejemplo, el jefe de seguridad de la información oficial, la continuidad del negocio-plan de recuperación de desastres, la cadena de suministro, gestión de proyectos de oficina)									
(RH) recursos humanos	El más alto funcionario de una organización que es responsable de la planificación y las políticas con respecto a todos los recursos humanos en esa organización.									
Cumplimiento y auditoría	La función (s) en la organización responsable del cumplimiento y de auditoría									

Leyenda de la tabla:
Celda Azul: El rol lleva la responsabilidad y/o la rendición de cuentas parcial para el proceso.
Celda Roja: El rol lleva la responsabilidad principal de este proceso. Solo un rol puede ser el principal responsable.

Figura N° 2: Responsabilidades y rendición de cuentas de los riesgos de TI, © ISACA®

Por lo anterior expuesto, una buena gestión de riesgos en las Institución adquiere bastante importancia y relevancia, de allí que se adopten los diferentes marcos de gobierno como COBIT 5, ISO 38500, ITIL, ISO 27001, ISO 27032, ISO 20000, entre otros, con el objeto de definir y trazar planes estratégicos que permitan la administración de éstas con el ánimo de aprovecharlas al máximo y alcanzar un excelente desarrollo de la organización.

La idea de integrar todos los marcos de referencia y normas aplicables, permitirán una mejor administración sobre los activos tecnológicos (ciberseguridad) y de información que se encuentran en las plataformas y sistemas de TERCER TRIBUNAL AMBIENTAL, analizar las amenazas y los riesgos sobre esos activos tecnológicos, elaborar planes de recuperación y de continuidad ante diversos escenarios de incidentes de ciberseguridad, crisis, cumplir con calidad de servicio los requerimientos efectuados por los clientes internos y/o externos y sobre todo, posibilitar tener una visión amplia de lo que sucede en el área, información fundamental para los procesos de planificación estratégica de la gerencia y que además alimenta a los objetivos fijados por la alta dirección de la Institución.

Por otra parte, se identificarán las brechas y se sugerirán planes de mejora, basados en los requerimientos de los diversos estándares considerados en la presente propuesta, por ejemplo:

	Problema	Plan de mejora	Referencias
Planeación Estratégica	No se lleva a cabo la actualizacion del Plan Estratégico de TI. No se desarrolla la estrategia de negocio.	- Cumplir y seguir un plan estratégico y táctico. - Mejorar la planeación estratégica de TI colaborando con la gerencia del negocio. - Actualización de planes de TI como respuesta a las solicitudes de la dirección. - La planeación estratégica de TI debe seguir un enfoque estructurado, que se deberá documentar y dar a conocer a todo el equipo.	ITILv3 - 3.3.1.PLANIFICACIÓN ITILv3 - 3.1.1.4.MEJORA ITILv3 - Estrategia de servicio
Estrategia de servicio	No crear y dar mantenimiento a un marco de trabajo de administracion de riesgos. No realizar evaluaciones a la organización.	- La planeación estratégica de TI es una función administrativa que debe definirse como responsabilidades de alto nivel. - Realizar evaluaciones por comparación contra normas industriales bien entendidas y confiables. - Definir políticas que determinen cómo y cuándo realizar la capacitación al personal de TI. - Preparado un plan para el entrenamiento del personal en las funciones de servicios de información.	ITILv3 - Estrategia de servicio ITILv3 - 2.10. COMUNICACIÓN, FORMACIÓN Y CAPACITACIÓN
Estrategia y organización	No existe conciencia por parte de la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio.	Concientizar a la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio. Concientizar a la gerencia de TI sobre las necesidades estratégicas de TI. La gerencia debe estar al tanto de las implicaciones del sistema. La gerencia debe identificar las [illegible] del negocio depende de forma crítica del sistema.	COBIT
Estrategia de táctica y operaciones	No se crean y mantiene un marco administrativo de riesgos. Los sistemas de información no se crean ni actualizan.	- Se debe discutir el monitoreo del plan estratégico de TI en reuniones de dirección del negocio. - Se deben obtener las aprobaciones por parte de la gerencia de la función de sistemas de información para cada fase de los proyectos de desarrollo. El programa de manejo de riesgos debe ser utilizado para identificar y eliminar o por lo menos minimizar los riesgos asociados con los proyectos. La gerencia autorizará la compra de software y de hardware, para que los técnicos monitoreen y reporten a la gerencia.	ITILv3 - 3.7.3.2. DESARROLLO DE LA DOCUMENTACIÓN COBIT COBIT
Tecnología y estrategia	No se monitorean y revisa el desempeño interno y externo contra los estandares y practicas de calidad.	- Comunicar la metodología de un plan estratégico de TI a todo el personal apropiado involucrado. - Se debe dar mantenimiento y soporte a los Sistemas de Información - Se deben controlar la calidad de los servicios para obtener los resultados necesarios. - Se debe discutir análisis preventivos de servicio y soporte.	ITILv3 - DOCUMENTACION COBIT COBIT COBIT

Figura N° 4: Tabla de ejemplo de identificación de mejoras

Además, se identificarán los porcentajes de cumplimiento respecto a las diferentes normas y buenas prácticas consideradas en la presente propuesta:

GRUPOS	ESTADO
A.5 Política de seguridad de la información	33%
A.6 Organización de la seguridad de la información	33%
A.7 Seguridad de los recursos humanos	56%
A.8 Gestión de activos	3%
A.9 Control de acceso	8%
A.10 Criptografía	61%
A.11 Seguridad física y ambiental	58%
A.12 seguridad de las operaciones	75%
A.13 seguridad de las comunicaciones	75%
A.14 Adquisición, desarrollo y mantenimiento de sistemas de información	51%
A.15 Relaciones con los proveedores	36%
A.16 Gestión de incidentes de seguridad de la información	74%
A.17 Aspectos de seguridad de la información en la gestión de continuidad del	12%
A.18 Conformidad	5%

Figura N° 5: Tabla de ejemplo de porcentaje de cumplimiento, basado en ISO 27001.

El resultado de este análisis establecerá la diferencia entre el desempeño actual y el esperado, con un informe que presente los hallazgos, indicaciones sobre dónde están las deficiencias y "qué" falta para cumplir con cada requisito de la norma.

Si aplicamos un modelo de madurez, tal como es CMMI, podremos obtener una escala de medición respecto a los requisitos de control de las normas aplicables dentro del GAP ANÁLISIS INTEGRAL.

0. No existente	0%
1. Inicial / Ad hoc	20%
2. Repetible pero intuitiva	40%
3. Proceso Definido	60%
4. Administrado y medible	80%
5. Optimizado	100%

Figura N° 6: Tabla de equivalencia respecto al porcentaje de cumplimiento v/s nivel.

Finalmente, en la revisión de los requisitos de control versus la tabla de equivalencia se podrá obtener los porcentajes reales de cumplimiento y el nivel en que la organización se encuentra, respecto a cada una de las normas, códigos de buenas prácticas, estándares locales y de TERCER TRIBUNAL AMBIENTAL considerados en la presente propuesta.

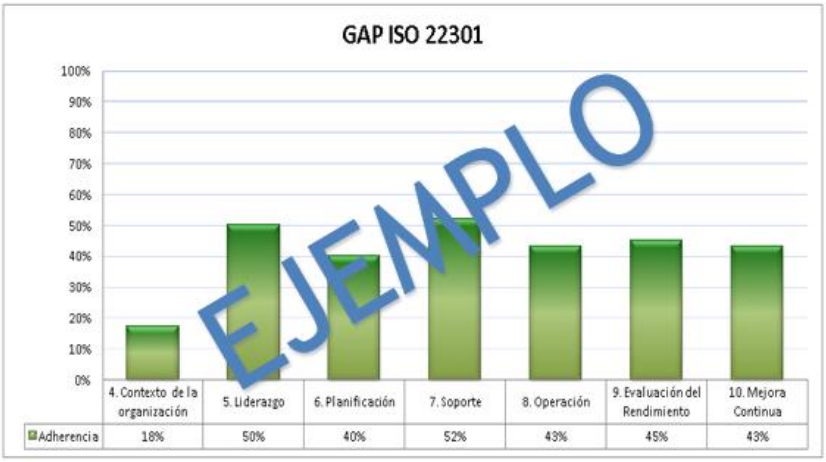


Figura N°7: Grafico (ejemplo) que muestra el cumplimiento de la norma ISO 22301.

3 Descripción de la solución propuesta

A continuación, se describen las actividades de consultoría para llevar a cabo el GAP Análisis.

- Arranque del proyecto.
- Levantamiento de Información.
- Identificación de brechas y recomendaciones.
- Presentación de resultados finales y roadmap.

Es importante poner de manifiesto que los trabajos aquí descritos son un GAP Análisis no incluyendo en ningún momento la implementación que solvente las brechas detectadas como resultado de este.

3.1 Arranque del proyecto

El objetivo de esta etapa es presentar al equipo de personas que participarán en el proyecto y definir el programa de trabajo.

Para ello se llevarán a cabo las siguientes actividades

- **Reunión de lanzamiento del Proyecto**. En esta reunión se presentarán los miembros del equipo consultor a la contraparte del cliente, se definirán los mecanismos de intercambio de información y los formatos de la documentación a elaborar como resultado del análisis. Asimismo, el Cliente indicará de cual de la siguiente información dispone (alguna de la cual sólo podrá ser suministrada en terreno):
    - Información de procesos.
        - Gestión de Compras.
        - Gestión de Recursos Humanos.
        - Seguridad Patrimonial.
        - Sistemas Críticos, mapas de red, códigos fuentes, contratos, entre otros.
    - Posibles informes de GAP análisis previos, si los hubiese.

- Políticas, normativas, procedimientos, instrucciones de trabajo, declaraciones de aplicabilidad, planes, documentación de arquitectura de sistemas, redes y seguridad, inventarios, entre otros.
- Información sobre el personal a entrevistar en la contraparte.

- **Elaboración y aprobación del programa de trabajo**. Una vez que se disponga de la información, se estimará las necesidades de entrevistas y se elaborará un programa de trabajo, que incluirá tanto los trabajos de terreno, **para el levantamiento de la información, reuniones de trabajo adicionales y presentación de trabajo** como los de gabinete (para el análisis de la información y la redacción de los informes de conclusiones, presentaciones y otros trabajos de gestión). Este programa de trabajo será revisado por el cliente y, una vez aprobado, será la Hoja de Ruta que definirá las actuaciones hasta el final del proyecto.

Resultado:

Presentaciones de las reuniones previas al lanzamiento del proyecto.

Programa de Trabajo. Como resultado de estas actividades se generará un Programa de Trabajo, que recogerá la siguiente información: aspectos a analizar, perfiles a entrevistar, fechas, horas y duración de entrevistas, tipo de entrevista (revisión de sistema, presencial, responder en remoto a algún cuestionario), consultor a cargo de la entrevista.

3.2 Levantamiento de Información

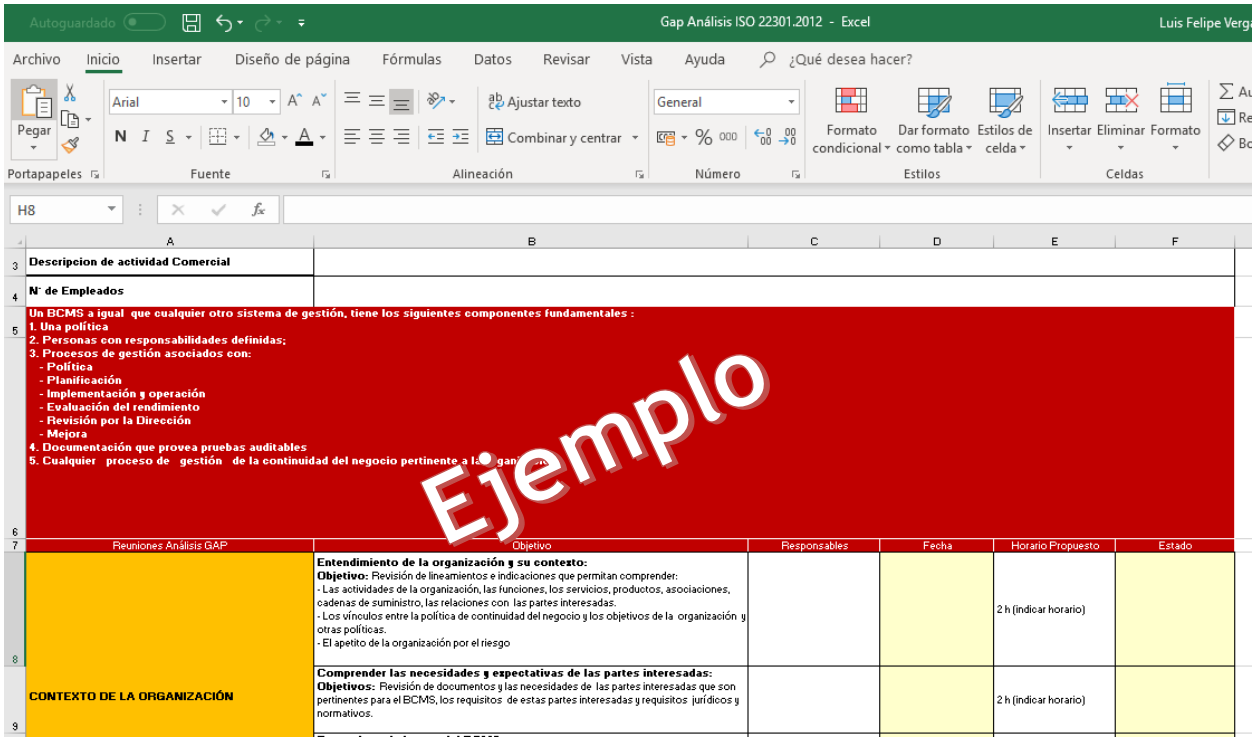
Una vez aprobado el marco de trabajo en la fase anterior, en esta fase se llevarán a cabo las actividades de recogida de información tanto de las reuniones y de los sistemas críticos.

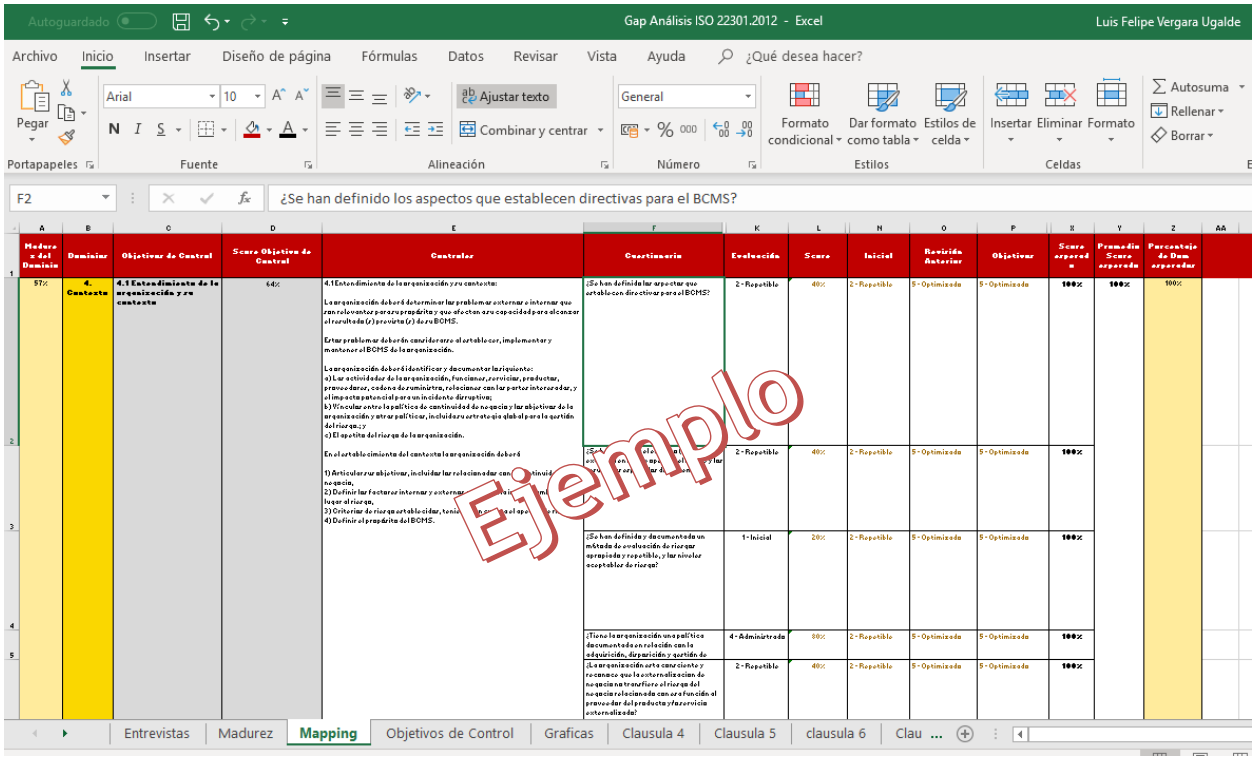
Estas actividades serán llevadas a cabo dentro **3 semanas cada una (algunas en paralelo)** y consistirán en:

- **Adecuación de cuestionarios de análisis.** En esta fase se revisitarán los cuestionarios tipo de análisis ISO 27001, 27032 y 22301 de los que ya se dispone, para depurarlos y

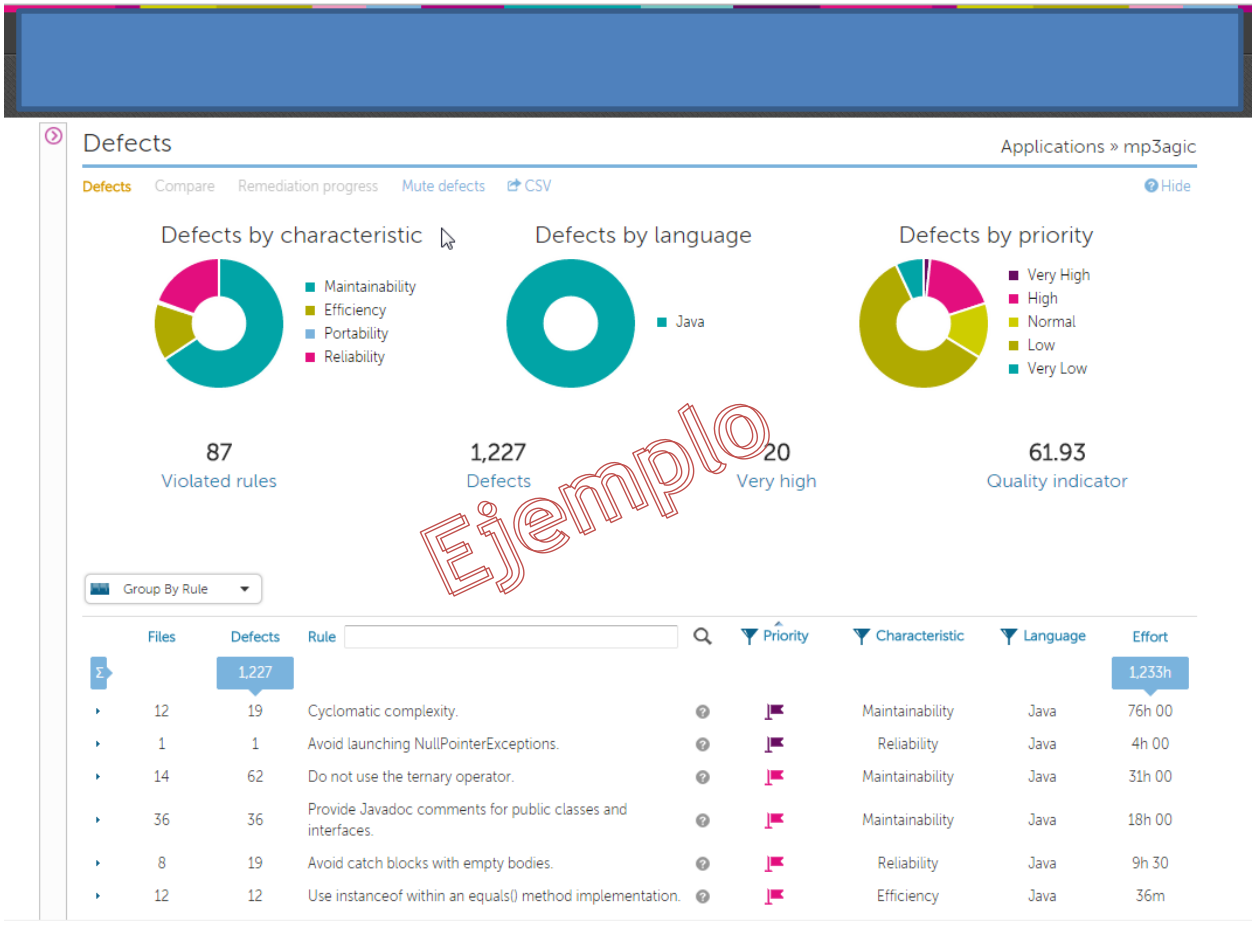
rellenarlos parcialmente (con la información que proporcione Tercer Tribunal Ambiental mencionada en el apartado anterior) antes de usarlos en las entrevistas.

- **Realización de entrevistas.** Se llevarán a cabo las entrevistas con la contraparte, conforme al Programa de Trabajo definido de la etapa anterior y se irán completando todos los cuestionarios conforme el personal entrevistado vaya suministrando la información requerida.




Gap Análisis ISO 22301.2012 - Excel
Luis Felipe Vergara Ugalde
Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Ayuda ¿Qué desea hacer?
F2
¿Se han definido los aspectos que establecen directivas para el BCMS?
Ejemplo
Entrevistas Madurez Mapping Objetivos de Control Graficas Clausula 4 Clausula 5 clausula 6 Clau ...

- **Revisión de código de sistemas críticos.** Se llevarán a cabo la revisión de código fuente de un programa informático crítico para la Institución. Con el objetivo de mejorar la calidad del código que se genera en el proceso de desarrollo del software, mediante la detección temprana de errores en el código de los programas o alternativas más eficientes a la implementación inicial. También se utiliza como técnica para mejorar las cualidades de los desarrolladores involucrados en la práctica, mediante la discusión abierta de posibles mejoras en el programa.



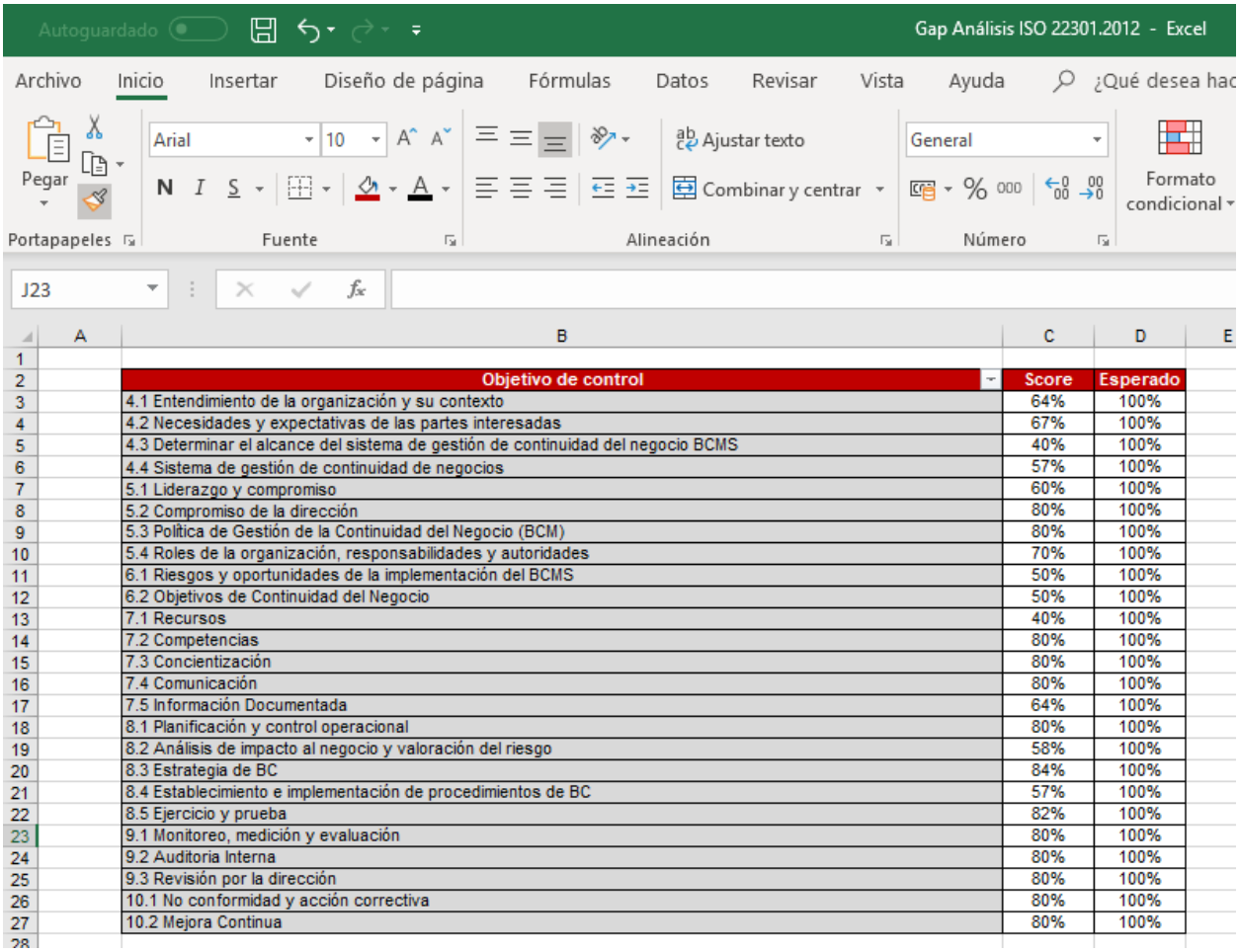
Resultado: **Información de levantamiento.** Información recogida, preparada para su procesamiento y análisis.

3.3 Identificación de brechas y recomendaciones

Una vez recogida toda la información, en esta etapa se llevará a cabo el análisis de esta para identificar las brechas.

Estas actividades serán llevadas a cabo en **7 semanas repartidas tanto en oficinas de Ingenia Global como en dependencias de Tercer Tribunal Ambiental** y también como parte de los trabajos de gabinete. Consistirán en realizar un detallado análisis de cumplimiento de los siguientes aspectos:

- Como por Ejemplo Cláusulas de la norma ISO 27001:2013, ISO 27032:2012, ISO 22301:2012, Cobit 5 y desarrollo de software seguros.



	Objetivo de control	Score	Esperado
3	4.1 Entendimiento de la organización y su contexto	64%	100%
4	4.2 Necesidades y expectativas de las partes interesadas	67%	100%
5	4.3 Determinar el alcance del sistema de gestión de continuidad del negocio BCMS	40%	100%
6	4.4 Sistema de gestión de continuidad de negocios	57%	100%
7	5.1 Liderazgo y compromiso	60%	100%
8	5.2 Compromiso de la dirección	80%	100%
9	5.3 Política de Gestión de la Continuidad del Negocio (BCM)	80%	100%
10	5.4 Roles de la organización, responsabilidades y autoridades	70%	100%
11	6.1 Riesgos y oportunidades de la implementación del BCMS	50%	100%
12	6.2 Objetivos de Continuidad del Negocio	50%	100%
13	7.1 Recursos	40%	100%
14	7.2 Competencias	80%	100%
15	7.3 Concientización	80%	100%
16	7.4 Comunicación	80%	100%
17	7.5 Información Documentada	64%	100%
18	8.1 Planificación y control operacional	80%	100%
19	8.2 Análisis de impacto al negocio y valoración del riesgo	58%	100%
20	8.3 Estrategia de BC	84%	100%
21	8.4 Establecimiento e implementación de procedimientos de BC	57%	100%
22	8.5 Ejercicio y prueba	82%	100%
23	9.1 Monitoreo, medición y evaluación	80%	100%
24	9.2 Auditoria Interna	80%	100%
25	9.3 Revisión por la dirección	80%	100%
26	10.1 No conformidad y acción correctiva	80%	100%
27	10.2 Mejora Continua	80%	100%

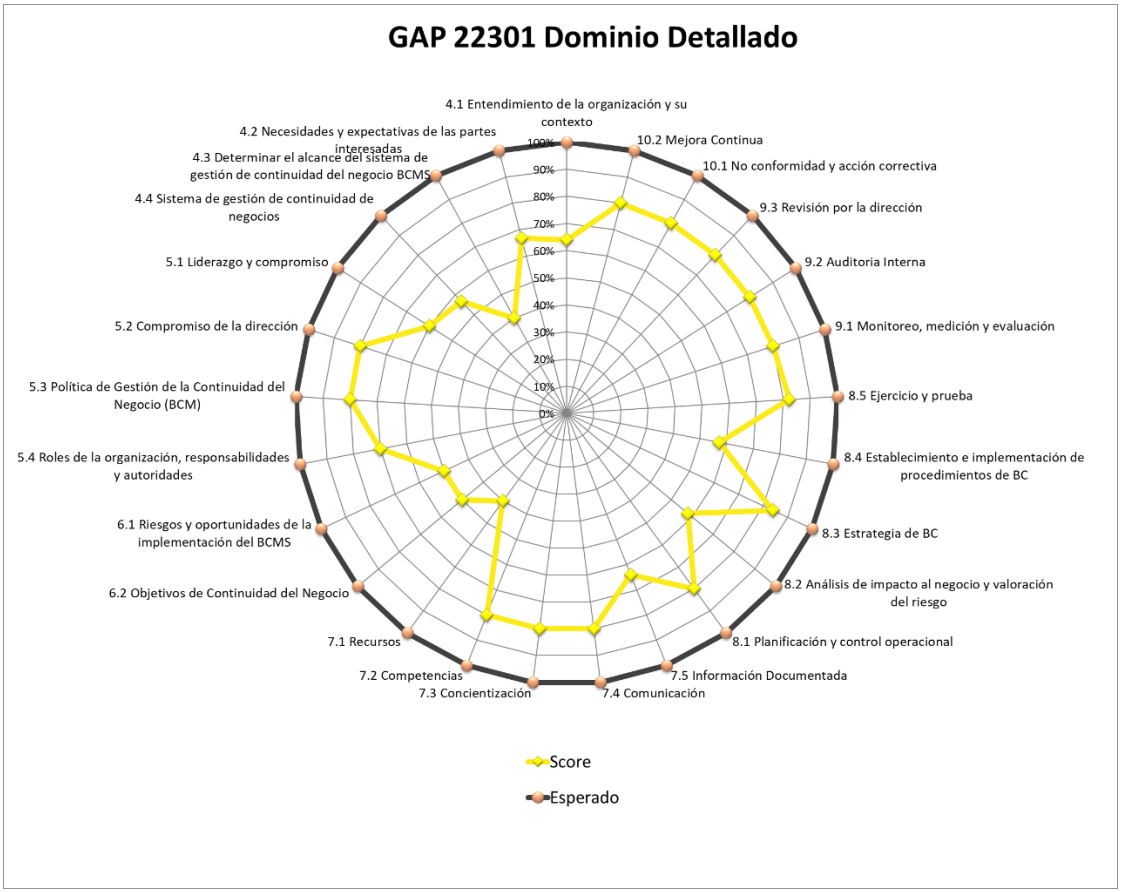


Ilustración 1. Ejemplos de resultado del GAP análisis

Resultado: **Informe de brechas (avance de resultado)**. Como resultado de esta fase se dispondrá de un informe de brechas por cada uno de los aspectos analizados, a modo de borrador diagnóstico de situación respecto al cumplimiento normativo.

Este informe deberá ser aprobado por el cliente. Ingenia realizará todos los cambios que serán precisos para dar respuesta a los comentarios emitidos por el cliente hasta llegar a una versión definitiva, que será el que se entregue en la etapa siguiente.

Nota: en caso de que, pasados 15 días desde la emisión del informe de brechas, no se reciban comentarios, este se dará por aprobado a todos sus efectos. Asimismo, cualquier información que, siendo requerida al cliente final, no fuese proporcionada, implicará que el diagnóstico será realizado prescindiendo de la misma.

3.4 Entrega de resultados finales y roadmap.

Una vez resueltos los comentarios del cliente en la actividad anterior, en esta fase se desarrollarán **los informes finales de diagnóstico**, incluyendo presentaciones ejecutivas que serán realizadas de forma presencial a la dirección o a quién el cliente determine que es relevante que conozca los resultados (porque tenga poder de decisión).

De esta forma, si la dirección (o quien tenga poder de decisión en inversiones dentro de la Institución) es consciente de la situación actual, dotará a la Organización de los apoyos y recursos necesarios para llevar a cabo los proyectos que surjan del GAP Análisis.

Resultado: **Informe final de brechas.** Como resultado de esta fase se dispondrá de un informe final con el compendio de todas las brechas. Se acompañarán de resúmenes ejecutivos y roadmap para presentarlos a la dirección.

4 Planificación de los trabajos

Los trabajos aquí descritos se realizarán en un **plazo de 2 meses**, desde la realización de la reunión de lanzamiento (el plazo final dependerá del calendario de entrevistas que finalmente se acuerde con el Cliente).

Tercer Tribunal Ambiental de Chile — Assesment Ciberseguridad	Mes 1				Mes 2			
	1	2	3	4	1	2	3	4
Administración de Proyecto								
Planificación y movilización del proyecto	■							
Reuniones de seguimiento e Informe Semanal	■	■	■	■	■	■	■	■
Ejecución del Proyecto								
Fase de Planificación	■							
Arranque del proyecto		■						
Levantamiento de Información Procesos			■	■	■			
Levantamiento de Información Sistemas				■	■	■		
Identificación de brechas y recomendaciones	■	■	■	■	■	■	■	
Entrega de resultados finales (Informe) y roadmap								■
Presentación gerencial								■
Fin del Proyecto								
Cierre del proyecto								■

4.1 Equipo de Trabajo

ROL	NOMBRE	EXPERIENCIA
Consultor Senior / Líder del Proyecto	Luis Vergara Ugalde	**Grados Académicos** • Ingeniero en Informática de la Universidad de Viña del Mar **Diplomado** • Diplomado de Postítulo en Gestión de Empresas de la Universidad de Chile. **Certificaciones** • **Implementador Líder ISO/IEC 27.001:2013 - BSI** • **ITIL Foundation V3 - Pearson VUE** **Experiencia** +10 años de experiencia en educación, proyectos de implantación y auditorías de Sistemas de Gestión, Seguridad de la Información, Ciberseguridad, Continuidad de Negocio y DRP.
Consultor Senior de Assessment en Ciberseguridad	David Navarro Cerda	**Grados Académicos** - Contador Público y Auditor en la Universidad de Santiago de Chile. **Diplomados** - Diplomado de Especialización en Auditoría en la Universidad de Chile, obteniendo la Máxima Distinción. Auditorías: Operativa, Financiera, Tributaria y Computacional.

		- Diplomado en Normas Internacionales de Información Financiera IFRS en la Universidad de Santiago de Chile. **Certificación** - **CISSP (Certified Information Systems Security Professional)** **Conferencias y Cursos** - Asistencia a la conferencia Latinoamericana de Fraudes y Riesgos en Cancún, México. - Dominio Seguridad de Datos de la industria de pagos PCI DSS. - Curso CCNA. - Cursos: Revenue Recognition, Protecting Trade Secrets, FCPA, DPSS. - **CEH v8 Ethical Hacking.** - Seminario Preparación para el examen CISA. - Curso de Microsoft Access, SQL, ACL. - Curso Fast Track de Ingles. **Experiencia** - +20 años de experiencia en proyectos de implantación y auditorías de Sistemas de Gestión de Seguridad de la Información y Ciberseguridad.

4.2 Certificación Implementador Líder ISO/IEC 27.001:2013

bsi.

Certificado

Este documento es para certificar que:

Luis Felipe Vergara Ugalde

Ha completado:

Implementador Líder ISO/IEC 27001:2013

A nombre de BSI:

Reg Blake, Vice Presidente, Asuntos regulatorios, BSI Group America Inc.

Fecha del curso: 04/06/2018 - 08/06/2018

Número de certificado: 8960807-192592

Fecha de emisión: 03/08/2018

UEAs otorgadas: 4.0

...making excellence a habit.

Este certificado es propiedad de BSI y está sujeto a las condiciones de contrato.
The British Standards Institution is incorporated by Royal Charter.
BSI Group Mexico, Paseo de la Reforma 505, Edificio Torre Mayor, Piso 50, Colonia Cuauhtémoc, 06500 México
BSI Group America Inc., 12110 Sunset Hills Road, Suite 200, Reston, VA 20190, USA

4.3 Certificación ITIL

EXIN

AXELOS GLOBAL BEST PRACTICE

This is to certify that

Luis Felipe Vergara Ugalde

Has achieved the

ITIL® Foundation Certificate in IT Service Management

Effective from
20 September 2017

Certificate number
6089396.20695799

Candidate Number
6089396

Peter Hepworth, CEO, AXELOS

drs. Bernd W.E. Taselaar, CEO, EXIN

This certificate remains the property of the issuing Examination Institute and shall be returned immediately upon request.

ITIL RESILIA PRINCE2 PRINCE2 AGILE MSP M_o_R P3M3 P3O MoP MoV

AXELOS, the AXELOS logo, the AXELOS swirl logo, ITIL, PRINCE2, PRINCE2 AGILE, MSP, M_o_R, P3M3, P3O, MoP and MoV are registered trade marks of AXELOS Limited. RESILIA is a trade mark of AXELOS Limited.

4.4 Certificación CISSP

International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

David Alejandro Navarro Cerda

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Wim Remes - Chairperson

Kevin Charest - Secretary

ID# 105224

Certification Number

December 31, 2020

Expiration Date

Certified Since 2008

CISSP®

ANSI ACCREDITED ISO/IEC 17024 Personnel Certification #0068

0139

(ISC)²

5 Valoración económica

El precio del servicio asociado a la presente propuesta se indica a continuación:

Descripción	Precio UF
ASSESSMENT EN CIBERSEGURIDAD	**1.342,2 UF**

Este precio no incluye IVA, ni ningún otro impuesto que pudiera recaer sobre ellos.

La compra de los servicios podrá ser realizada a través del Convenio Marco de Perfiles para el Desarrollo y Mantención de Sistemas Informáticos, con los siguientes perfiles e ID's:

Código ID	PERFIL	Valor Hora UF	HH Estimadas	Total, UF
1155014	JEFE DE PROYECTO - SENIOR VALOR HORA HABIL **(CONSULTOR ESPECIALISTA EN SEGURIDAD)**	1,46	310	452,6
1155002	CONSULTOR - SENIOR VALOR HORA HABIL **(INGENIERO ESPECIALISTA EN SEGURIDAD)**	1,39	640	889,6
				1.342,2

5.1 Validez de la propuesta

La validez de esta propuesta es la siguiente:

- **Personal propuesto y fechas de incorporación** (o cualquier otro hito referenciado en la oferta como plazo de ejecución, fecha de comienzo, entre otros.): **hasta 28.02.2019**. Pasada esa fecha, deberá revisarse la disponibilidad de los técnicos propuestos y sus posibles fechas de incorporación.
- **Plazo de arranque**: los servicios comienzan a disfrutarse con la aceptación de la propuesta.

Condiciones generales y económicas: **hasta 28.02.2019.**

5.2 Aceptación de la oferta

Y para que aquí conste, y en prueba de conformidad y aceptación del contenido de este documento, de referencia POT1245, ambas partes lo firman por duplicado y a un solo efecto en la fecha y lugar indicados:

Por Ingenia Global, (Fecha, firma y sello)	Por TERCER TRIBUNAL AMBIENTAL, (Fecha, firma y sello)
	
Fdo: Luis Felipe Vergara Ugalde Fecha: 24-01-2019	Fdo: Fecha: