PLAN DE IMPLEMENTACIÓN DE UN SGSI BASADO EN LA NORMA ISO 27001:2013 EN EL ÁMBITO DE LA ADMINISTRACIÓN PUBLICA ARGENTINA

Nombre Estudiante: Bruno Alejandro Roberti Ferri

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia Henares
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: 28/12/2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Plan de implementación de un SGSI basado en la norma ISO 27001:2013 en el ámbito de la Administración Pública Argentina.*
Nombre del autor:	*Bruno Roberti Ferri*
Nombre del consultor/a:	Antonio Segovia Henares
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	12/2020
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	*Sistema Gestión Seguridad*

Índice

Lista de figuras

No se encuentran elementos de tabla de ilustraciones.

1. CONTEXTO Y ESTADO ACTUAL

1.1 Introducción

El organismo ha sido pionero en la implementación de sistemas de información en la administración pública nacional (APN) de Argentina, contando con soporte informático para un alto porcentaje de sus procesos. Acorde con el impacto de los sistemas de información en el mismo, en el año 2003 se implementó el "Manual de normas y procedimientos de Seguridad Informática" siguiendo los lineamientos de ISO/IRAM 17799:2002, el cual por diversos motivos no fue actualizado hasta el año 2014. En ese año se inició la actualización de la política de seguridad que se encuentra vigente en el organismo de acuerdo a lo expresado por la Decisión Administrativa N° 669/2004 [1] de la Jefatura de Gabinete de Ministros que estableció la obligatoriedad para los organismos del Sector Público Nacional de dictar o bien adecuar sus políticas de seguridad de la información conforme a la "Política de Seguridad de la Información Modelo" dictada por la Oficina Nacional de Tecnologías de la Información (ONTI). La versión implementada en la actualidad en el organismo se corresponde con la aprobada mediante Disposición 3/2013 de ONTI.

En el año 2015 y en el transcurso del trabajo de actualización y adaptación de a la política modelo por parte del organismo, la ONTI dictó la Disposición 1/2015 [2] aprobando la nueva versión de la política modelo basada en la norma ISO/IEC 27002:2013. El organismo aún no implementa esta versión, lo cual es uno de los objetivos del presente trabajo.

Debe tenerse en cuenta que si bien el organismo cuenta desde hace varios años con una política de seguridad, nunca ha implementado un Sistema de Gestión de la Seguridad de la Información en toda su extensión, por lo tanto a través de este trabajo se propone la elaboración del Plan Director de Seguridad que permita la implantación de un SGSI, lo cual canalizará de forma efectiva los esfuerzos del organismo en esa materia.

1.2 Conociendo la Disposición 1/2015 ONTI

Como se ha indicado en la introducción debido a la normativa de la república Argentina para el presente trabajo se utilizarán los controles implementados en la "Política de Seguridad de la Información Modelo" dictada por la Oficina Nacional de Tecnologías de la Información (ONTI) en lugar de los especificados en norma ISO/IEC 27002. A continuación se brinda un resumen de la historia de esta normativa y su comparación con la norma ISO/IEC 27002.

En diciembre de 2004, la DA N° 669/2004 de la Jefatura de Gabinete de Ministros estableció la obligatoriedad para los organismos del Sector Público Nacional de dictar o bien adecuar sus políticas de seguridad de la información conforme a una política modelo, la cual en realidad es un conjunto de mejores prácticas que ha dictado la ONTI, basándose en la normativa ISO/IRAM 17999. Citando la introducción de la primera versión de la norma:

"En septiembre de 2003, la Oficina Nacional de Tecnologías de Información (ONTI) convocó a especialistas en seguridad informática de diversos Organismos públicos, con el fin de conocer sus opiniones respecto a una estrategia de seguridad informática para el Sector Público Nacional. De estas reuniones surgió la necesidad de que todos los Organismos del Sector

Público Nacional cuenten con una Política de Seguridad de la Información, implementada y documentada.

En consecuencia, se conformó un grupo de trabajo con el objeto de formular un modelo de Política de Seguridad de la Información que sirviera de punto de partida para la elaboración de las políticas correspondientes en cada Organismo. Dicho grupo de trabajo decidió basar el modelo en la norma ISO/IRAM 17799, como un marco de referencia para la gestión de la seguridad de la información en una entidad. El modelo fue sometido a la consideración de los Organismos de la Administración Pública y de las Autoridades Nacionales para su aprobación."

En el año 2005 mediante la Disposición N° 6/2005 de la Oficina Nacional de Tecnologías de Información se aprueba la primera "Política de Seguridad de la Información Modelo" y en septiembre del 2011 se procedió a realizar la actualización de aquel Modelo, en base a las actualizaciones sufridas por la norma ISO/IEC 27002. (EN el año 2007 la norma ISO/IEC 17799:2005 pasa a denominarse ISO 27002:2005).

En mayo del 2014 se procedió a realizar la actualización de Modelo, en base a las actualizaciones sufridas por la norma ISO/IEC 27002 versión 2013 y la incorporación de temas que esa versión incluyó. La norma fue publicada mediante la Disposición 1/2015 aprobando la nueva versión de la política modelo.

En una comparación entre ambas guías de buenas prácticas podemos decir que ambas normas poseen la misma cantidad de capítulos (clausulas en ONTI). Son 14 capítulos destinados a detallar los controles y describir su implementación.

Sin embargo, debido a que están destinadas a organismos públicos las políticas de la ONTI han variado la cantidad de controles y el agrupamiento en categorías dentro de esta clausulas. A nivel general la primera diferencia es el número de controles: ISO/IEC tiene definidos 114 controles mientras que la "Política Modelo de Seguridad" Disp. 1/2015 ONTI define 137 controles. En cuanto al agrupamiento dentro de cada capítulo, ISO/IEC posee 35 categorías mientas que la norma de ONTI agrupa en 40 categorías.

No obstante lo expuesto no es tan grande la diferencia entre ambas normas, y si bien no es el objetivo de este estudio identificar cada una de estas diferencias podemos identificar las más importantes:

- Categoría 9.4: No están definidos los controles de ISO, en su lugar la norma de ONTI define controles que entiendo están más orientados a las redes. Se va a proponer incluir estos controles dentro de los que utilizará el organismo.

- Categorías 14.4 y 14.5: Nuevamente la norma de ONTI desplazó algunos controles definidos por ISO, en este caso para estándares de desarrollo por otros que consideró oportunos. Se va a proponer incluir los controles de ISO dentro de los que utilizará el organismo.

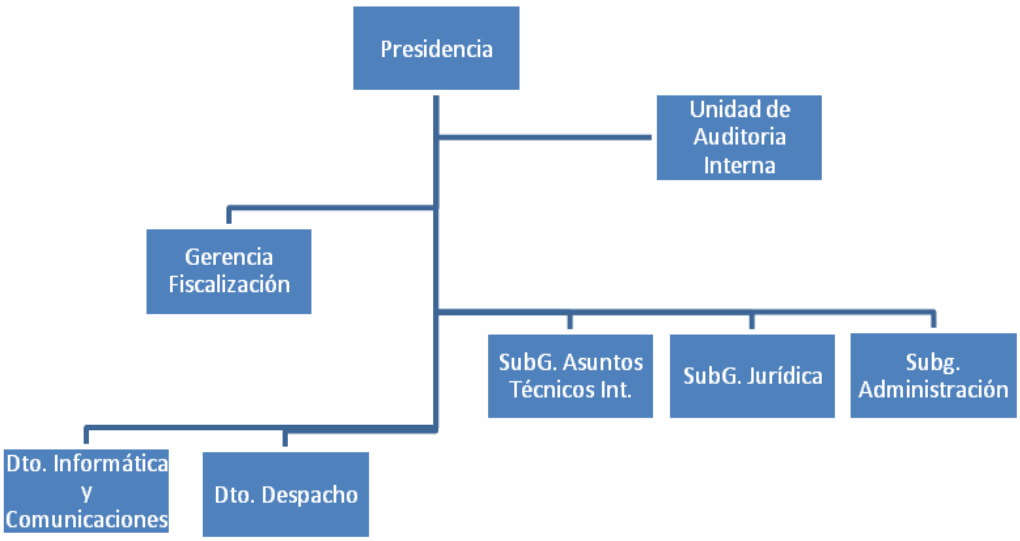
- Categoría 16.1: La versión de ONTI de gestión de incidentes omite varios aspectos importantes que si considera ISO. Para esta categoría también se va a proponer sumar los controles ausentes

1.3 Contextualización

El organismo es un ente descentralizado perteneciente al Poder Ejecutivo de la república Argentina, fue creado por ley hace más de 60 años y tiene por función resguardar a la comunidad respecto de la genuinidad y aptitud para el consumo productos de origen vegetal. También tiene a su cargo en forma permanente el contralor técnico de la producción, circulación, fraccionamiento y comercialización de los productos bajo su órbita.

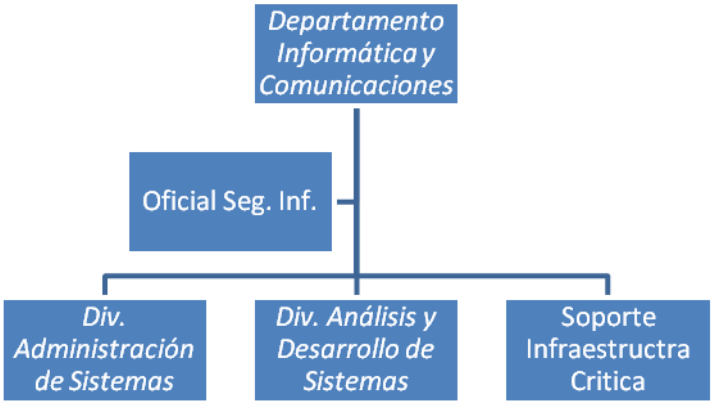
Dentro de otras funciones el organismo interviene en las Negociaciones Internacionales, articulando con Cancillería y la Secretaria de Gobierno de Agroindustria dependiente del Ministerio de Producción y Trabajo, canales que faciliten las transacciones comerciales del sector. Elabora las estadísticas nacionales del sector y es responsable de aportarlas a los diferentes ámbitos Nacionales y Provinciales. Publica información estadística para todos los interesados del país y del mundo.

El organismo cuenta con competencia jurisdiccional en todo el territorio de la República Argentina, implementando su presencia a través de delegaciones jurisdiccionales, 17 en total y una sede central. Actualmente posee unas 600 personas trabajando bajo su ámbito entre todas sus sedes, y la última versión de su estructura orgánica funcional se instrumentó mediante decreto Decisión Administrativa en el año 2018, donde se aprobó la nueva estructura organizativa de primer y segundo nivel.



"Figura 1: Organigrama primer nivel"

La unidad que tiene la responsabilidad sobre las funciones asociadas con las Tecnologías de Información y Comunicaciones es el del "Departamento Informática y Comunicaciones" el cual posee dependencia jerárquica con la Presidencia del organismo. El departamento cuenta 25 personas en su totalidad, agrupados en las siguientes unidades



"Figura 2: Organigrama DIC"

Si bien hay un oficial de seguridad de la Información, las funciones de Responsable de Seguridad de la Información emanadas de la DA ° 669/2004 de la Jefatura de Gabinete de Ministros están asignadas al Jefe del departamento DIC.

1.3.1 Breve descripción de los Sistemas informáticos Existentes.

El cumplimiento de las actividades del Organismo, se realiza con el soporte de tres grandes categorías de sistemas informáticos:

- Sistemas de Fiscalización.
- Sistemas de Conducción.
- Sistemas de Apoyo.

A continuación se presenta un breve detalle de los sistemas informáticos existentes en el organismo, basado en el listado de activos informáticos y agrupados por el tipo de proceso al que brindan soporte.

Sistemas de FISCALIZACIÓN: Son los sistemas informáticos desarrollados para la Gerencia de Fiscalización y sus áreas comprendidas.

- *Sistemas para Control de Volumen.*
- *Sistemas de Legajo Electrónico.*
- *Sistemas de Laboratorio.*
- *Sistemas de DDJJ.*
- *Sistema de Notificaciones Electrónicas.*
- *Sistema de Productos Observados.*
- *Sistema de Estimación de Cosecha.*
- *Extranet.*
- *VUCEA.*

Sistemas de CONDUCCIÓN: Comprenden sistemas informáticos que prestan apoyo a las actividades de las conducción del organismo, los principales destinatarios son la Presidencias y unidades dependientes de la misma.

- *Tablero de Comandos.*
- *Sistema de Auditoria, Gestión y Procesos.*

- *COMDOC III.*
- *Sistema Digesto Administrativo.*
- *Correo Electrónico.*
- *GDE: Gestión Documental Electrónica.*

Sistemas de APOYO: Comprenden sistemas informáticos que prestan soporte a las Subgerencias de Administración, Asuntos Jurídicos, Despacho de Presidencia, Departamento de Informática y Comunicaciones. Se dividen en 2 tipos, sistemas administrados desde el organismo y sistemas administrados por terceros donde sólo realizan operaciones las áreas usuarias.
Dentro de la primera categoría encontramos los siguientes sistemas:

- *Sistema de Gestión Personal.*
- *Marcación Horaria.*
- *Sistema Integral de Recaudaciones:*
- *Sistema de Almacén.*
- *Sistema de Automotores.*
- *Sistemas de Gestión de Convenios*
- *Sistema de Control de Exportaciones y Emisión de Certificados.*
- *Sistema de Administración de Usuarios General.*
- *Sistema de Cámaras de Vigilancia*
- *Sitio Web Institucional.*
- *SIU MAPUCHE.*
- *Sistema de Mesa de Ayuda.*

Dentro de los sistemas administrados por otros organismos y utilizados en este se encuentran:

- *COMPR.AR Sistema de Contrataciones de bienes y servicios.*
- *CONSOL Resolución 42/2006.*
- *SLU: SIDIF Local Unificado.*
- *e-SIDIF: Sistema Integrado de Información Financiera Internet.*
- *e-PROA: Sistema de Formulación del Pres. de Gastos en Personal.*
- *BAPIN: Banco de Proyectos de Inversión.*
- *EVALFIS: Sistema de Evaluación Física del Pres.*
- *SIREPEVA: Sistema Registro de Personal y Evaluaciones.*
- *MCC: Módulo de Compras y Contrataciones.*
- *SIBIS: Sistema de Bienes y Servicios.*
- *SIPRO: Sistema de Información de Proveedores.*
- *RCPD: Registro Central de Personas Discapacitadas.*
- *RCPC: Registro Central de Personal Contratado.*
- *SINEP: Sistema de Nacional de Empleo Público.*
- *SISAC: Sistema de Seguimiento de Acciones Correctivas.*
- *SIGEJ: Sistema Único Informático de Gestión Judicial.*

1.4 Alcance

La implementación del SCGI dentro del organismo abarcará a todos los sistemas de información, procedimientos y personal que soportan los procesos de Fiscalización, en cuanto a los sistemas de Apoyo abarcará a los sistemas administrados desde el organismo. Por

administrados se entiende que se tiene control del código fuente y están alojados en los servidores del organismo.

La política / lineamientos de seguridad física sólo se aplicaran a los equipos alojados en sede central.

La política de desarrollo de software no afectará a los sistemas con licencias del tipo free software/código abierto que son modificados en el organismo.

1.5 Objetivos del Plan Director

1. Mejorar la seguridad en los servicios de información brindados por el organismo eliminado la brecha entre implementación y política. Implementar controles faltantes.

2. Actualizar los estándares de desarrollo para incluir metodología que contemple la seguridad en todo el proceso de desarrollo de aplicaciones.

3. Generar las normas y procedimientos faltantes en las clausulas de Desarrollo, Comunicaciones y Operaciones.

4. Generar un Plan de Continuidad de Negocios.

5. Cumplir con el marco legal de la ONTI el cual indica que se debe actualizar la política de seguridad acorde con la versión de la Disp. 1/2015.

6. Generar una cultura en Seguridad de la Información, mejorando la formación y concientización del personal del organismo en temas relativos a la misma.

7. Mejorar la eficiencia de procesos y sistemas para el tratamiento de la información comprendida en la Ley 25.326 del año 2000 (Ley de Datos Personales) y sus normas complementarias.

1.6 Análisis Diferencial

La realización de un Análisis Diferencial nos permite determinar el estado actual de la seguridad de la información en el organismo desde el punto de vista del cumplimiento de los requisitos de la norma ISO/IEC 27001 y de sus controles contenidos en el Anexo A de la misma. Debido a la normativa que regula a los organismo de la APN en Argentina, hemos adaptado el presente el análisis para utilizar los controles aprobados en la Disposición 1/2015 ONTI (“Política de Seguridad de la Información Modelo” 2015).

En este análisis se evaluó el nivel de cumplimiento para los requerimientos de la norma ISO 27001 comprendidos en los apartados 4 al 10 y para los 140 controles de la Disp. 1/2015 ONTI comprendidos en las clausulas 5 a 18. Esto nos permite establecer el punto de partida para implementar la norma y evaluar el esfuerzo necesario así como tener una herramienta fiable para elaborar el plan Director de Seguridad.

Como método de evaluación del cumplimiento se utilizó un modelo de madurez, específicamente se utilizó el modelo de madurez definido por COBIT (Control Objectives for

Information and related Technology) y basado en el CMM (Capability Marurity Model) desarrollado por la Carnegie Mellon School. Que se detalla a continuación:

ID	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "*best practice*", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "*ad hoc*" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTENTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

"Figura 3: Niveles Modelo Madurez COBIT"

Al analizar los resultados del cumplimiento sobre la norma ISO 27001, se presenta un escenario donde no se observa que el organismo alcance un nivel elevado en la mayoría de sus apartados, lo cual no se condice con los esfuerzos que ha realizado en materia de seguridad de la información. Sin embargo podemos entender este desacople entre los controles implementados, como se verá más adelante, y los requisitos para el establecimiento de un Sistema de Gestión de la Seguridad se basa en que las medidas implementadas no han sido articuladas de manera organizada, ni con una visión integral de lo que es un SGSI. Estos esfuerzos han respondido a acciones aisladas o eventos que afectan la seguridad.

Nro	Apartado	Nivel
4	La Organización y su Contexto	L2
5	Liderazgo	L3
6	Planificación	L1
7	Soporte	L2
8	Operación	L1
9	Evaluación del desempeño	L2
10	Mejora	L2

"Figura 4: Niveles Madurez del Organismo"

Para llegar a estos resultados se han evaluado los siguientes aspectos:

4-La Organización y su Contexto

Si bien no ha comenzado aun el proyecto de implementación del SCGI ni determinado su alcance, el organismo ya ha identificado a las partes internas y externas que son relevantes determinando los requisitos de las mismas. También ha avanzado en la determinación de las cuestiones externas e internas que afectan al SCGI.

5- Liderazgo

En este aspecto debemos destacar que la dirección del organismo ha cumplido con lo estipulado en la DA 664/2004, asignado los roles asociados al manejo de la seguridad de la información y aprobando la política de seguridad vigente en el organismo. Quedan pendientes el establecimiento de objetivos de SI acordes y una revisión más activa de la eficacia.

6- Planificación

El organismo aun no ha iniciado el proceso de tratamiento de riesgos, solo posee una identificación de riesgos a nivel general. Tampoco ha iniciado la planificación del SCGI. NO obstante el nivel L1 se corresponde porque la nueva conducción ha reconocido la necesidad de iniciar ambos proceso en el corto plazo.

7- Soporte

Se han proporcionado recursos iniciales para el SCGI y los procesos de comunicación están bien definidos y ejecutados. Se ha avanzado en la generación de parte de la documentación requerida sin embargo la mayoría no está reglamentada ni versionada correctamente. Se evalúan las competencias del personal pero no en materia de SI en forma particular, tampoco se mantiene un registro de las mismas. El nivel de conciencia del personal fuera del área de tecnología en temas de SI es muy bajo.

8- Operación

En el control operacional hay varios procesos definidos, se realiza una evaluación de los riesgos antes pero ambos aspectos dependen de las personas más que en procedimientos. El análisis y tratamiento de riesgos no se ha realizado aún, pero el Responsable de SI ha expresado interés en realizarlo en forma conjunta con auditoria.

9- Evaluación del desempeño

La unidad de auditoría interna del organismo realiza auditorias todos los años sobre diferentes aspectos de la SI. Al no estar implementado el SGSI, no se han establecido procesos de monitoreo sobre la SI. Los informes a dirección se generan de forma no programada y con poca frecuencia en los últimos años.

10- Mejora

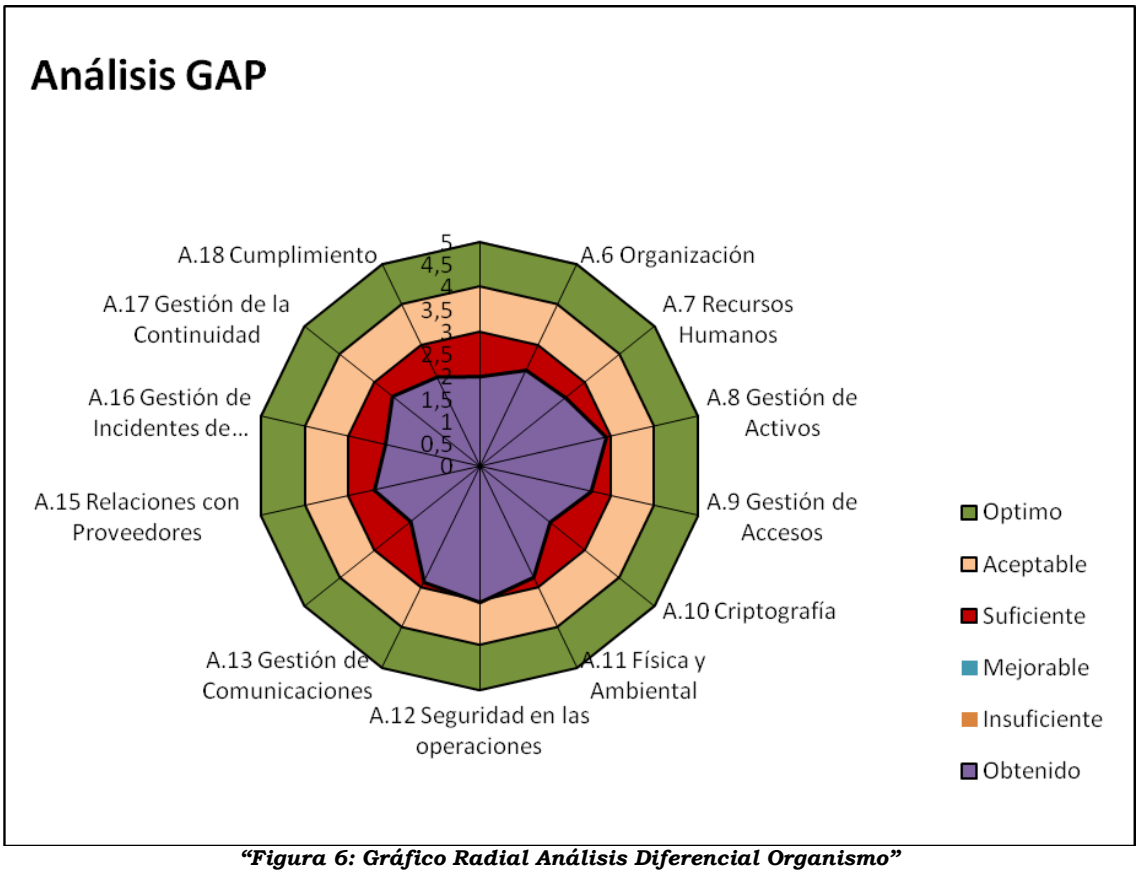
Al no estar implementado el SGSI, no hay un proceso de mejora continua asociado. Siguiendo la normativa de la APN el organismo maneja los hallazgos de la unidad de auditoría de acuerdo a los procedimientos establecidos por la Sindicatura General de la Nación

A continuación se expone el resultado del análisis sobre el cumplimiento de los controles implementados por la DISP 1/2015

Clausula	Valor
A.5 Política de Seguridad de la Información	2
A.6 Organización	2,38
A.7 Recursos Humanos	2,44
A.8 Gestión de Activos	2,89
A.9 Gestión de Accesos	2,54
A.10 Criptografía	2
A.11 Física y Ambiental	2,75
A.12 Seguridad en las operaciones	3,04
A.13 Gestión de Comunicaciones	2,88
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	1,98
A.15 Relaciones con Proveedores	2,42
A.16 Gestión de Incidentes de Seguridad	2,17
A.17 Gestión de la Continuidad	2,5
A.18 Cumplimiento	2,21

"Figura 5: Resultado Análisis Diferencial para el Organismo"

Como se puede observar los resultados de cumplimiento sobre estos controles muestra el nivel de madurez mucho mayor a los anteriores, reflejando la cantidad de controles que se han implementado a lo largo de los años. Para este análisis también utilizaremos el gráfico de tipo Radar en el cual se puede observar en forma integral el nivel de evolución de los controles en el organismo.



"Figura 6: Gráfico Radial Análisis Diferencial Organismo"

En un análisis detallado Para llegar a estos resultados se han evaluado los siguientes aspectos:

A.5 Política de Seguridad de la Información

Se ha aprobado la política de seguridad del organismo siguiendo los lineamientos de la DISP 3/2013; sin embargo no se ha avanzado en definir y aprobar una parte importante de los procedimientos y documentos requeridos por la misma, lleva a que muchos procesos se siga dependiendo de la discrecionalidad del usuario su aplicación. En cuanto a la revisión y debido al largo periodo de tiempo que llevó implementar la actual versión, la misma ya fue reemplazada por la incluida en la DISP 1/2015, con lo cual podemos concluir que la organización comprende la importancia de una política de seguridad pero aún no está a tomado conciencia de la necesidad de mantenerla actualizada.

A.6 Organización

La organización posee todos los roles de seguridad definidos, se ha nombrado el Responsable de Seguridad de la Información (es el Jefe del Dpto. de Informática y Comunicaciones) y está definido un comité de Seguridad del que participa la dirección. Se ha conseguido el apoyo de la dirección mediante la firma de los compromisos correspondientes. El alcance de los acuerdos de confidencialidad debe ampliarse incluya a todo el personal del organismo, ya que solo están alcanzados los terceros contratados. La revisión de la seguridad por parte de la unidad de auditoría se repite en forma periódica mediante los planes anuales y estratégicos de la UAI, siendo apoyado por un sistema informático propio. En cuanto al apartado de trabajo con dispositivos móviles, existe una política que sólo contempla los celulares, debería extenderse y

adecuarse para que incluya las notebooks que utiliza el personal fuera de sus oficinas. En el apartado de trabajo remoto el organismo no tiene nada normado ya que prácticamente no era utilizado excepto por personal de sistemas, estando la utilización de esta modalidad apoyada en la responsabilidad de usuarios y administradores.

A.7 Recursos Humanos

En cuanto a los controles previos al empleo están normados y se cumplen razonablemente las definiciones de puestos y la investigación de antecedentes; se siguen las normas de Administración Pública Argentina sobre revisión de antecedentes las cuales son compatibles con las propuestas por la norma. Sobre estos procesos, al igual que otros relacionados con la Adm. de RRHH se realizan auditarías periódicas. En el tema capacitación inicial de los empleados en SI, el organismo ha implementado la realización de una capacitación cuando se ingresa a trabajar al organismo, sin embargo esto no es suficiente ya que aprox. el 80% del personal ingresó antes de la implementación de este curso. Debería implementar un proyecto de capacitación para los empleados que aún no la han realizado. Esta falta de capacitación ha derivado que no hay una verdadera concientización del tema SI en el organismo, la cultura organizacional enfatiza la operatividad por sobre la seguridad.

Los procesos disciplinarios y las responsabilidades en el cese, se ajustan a la normativa del empleo público nacional, la cual es estricta al respecto. Sin embargo el foco está puesto en la devolución de activos físicos solamente. El proceso de retiro de derechos de acceso no está coordinado en todos los casos, el organismo debería implementar revisiones de los privilegios aplicados de manera más periódica hasta detectar la normalización de este tema.

A.8 Gestión de Activos

El organismo ha realizado el inventario de activos y la asignación de propietarios, cumpliendo de forma correcta con esta etapa. Sin embargo las directrices de clasificación no poseen una definición clara en algunos de los pilares que facilite la clasificación, dependiendo bastante del criterio del propietario. Esta pendiente la emisión de normativa referida al uso aceptable de los activos. Los criterios de etiquetado y manipulación solo han sido definidos para las cintas, dejando a los demás contenedores (no digitales) de información sin etiquetar. Las gestión de medios esta soportada por una aplicación de incidentes (GLPI), y se apoya en una normativa específica la cual se cumple de forma satisfactoria.

A.9 Gestión de Accesos

No existe una política de de gestión de accesos vigente, y las operaciones sobre las cuentas de usuarios son registradas mediante la aplicación informática GLPI, dejando el proceso con un excelente grado de trazabilidad. Sin embargo se detectan que existen muchas excepciones a esa política en el manejo de usuarios privilegiados en el entorno Windows y en los sistemas de aplicación. El organismo debe llevar a cabo revisiones de derechos de usuarios en forma periódica, ya que actualmente sólo son llevadas a cabo por la unidad de auditoría. Como parte de la baja cultura en SI se han registrado muchos casos de no seguimiento de buenas prácticas en la utilización de credenciales.

En lo referido al control de acceso a Sistemas y Aplicaciones el organismo cumplen con casi todos los controles estipulados, sin embargo las capacidades de auditoría del módulo de seguridad de los sistemas de gestión son reducidas, impidiendo una correcta trazabilidad de las acciones de los usuarios en esos sistemas.

A.10 Criptografía

No existe una política específica para el tema de criptografía, pero si se siguen los procedimientos como autoridad de registro de la APN y algunas buenas prácticas en el desarrollo.

A.11 Física y Ambiental

En el aspecto de seguridad física el organismo ha definido correctamente las aéreas seguras y en las mismas se cumplen las condiciones físicas requeridas. El datacenter del organismo tiene un sistema electrónico de acceso y registro que automatiza el ingreso y facilita el monitoreo. Los procesos de trabajo en áreas seguras están definidos pero no formalizados; igual que las áreas de acceso público. El organismo está correctamente protegido en temas de suministro eléctrico, contando con una UPS y u generador de capacidad suficientes para abastecer el datacenter. Debido a la antigüedad de los equipos principales del organismo, el aseguramiento del mantenimiento se realiza a través de garantías extendidas. Se ha detectado que los equipos de uso externamente no están asegurados, y tampoco correctamente registrados en ningún sistema, dificultando el poder determinar si una notebook es utilizada dentro o fuera de la organización. Existe un procedimiento de retiro de equipos, pero no se lo ejecuta adecuadamente. Los procesos de Escritorios Limpios no están formalizados y su conocimiento es dispar, dando paso a diferentes interpretaciones del concepto. Dada la importancia de este tema se debería formalizar a la brevedad.

A.12 Seguridad en las operaciones

Este es el punto donde el organismo más se apoya en los conocimientos y las responsabilidades de los integrantes del DIC, ya que solo algunos procedimientos operativos están correctamente documentados, y casi ninguno está formalizado. No existe un registro de cambios en las operaciones. Existe separación de ambientes mediante aplicativos específicos.

En cuanto a la protección antivirus, el organismo cuenta con un software AV administrado en forma centralizada el cual funciona adecuadamente. En lo referido al registro y monitoreo de eventos, esta actividad no se realiza en forma periódica sino ante un evento o requerimiento puntual lo cual se suma a una política deficiente de retención de registros lo que puede derivar en problemas para el seguimiento de las actividades de los administradores. Finalmente se debería generar un procedimiento para la administración de vulnerabilidades que sea homogéneo en cuanto a sus estándares, ya que actualmente no es manejada de igual manera para los diferentes ambientes de producción.

A.13 Gestión de Comunicaciones

EL organismo posee un adecuado manejo de este aspecto, con redes adecuadamente segmentadas, al igual que los vínculos externos los cuales son protegidos con firewalls en

todos sus extremos. La transferencia de información tiene una política establecida, pero sin procedimientos aun. Todos los acuerdos de intercambio de información se realizan en el marco de la regulación de la APN el cual cumple con la normativa. Los acuerdos de confidencialidad están incluidos en los acuerdos con proveedores externos, cumpliendo también este aspecto.

A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas

Está avanzado el proceso de normar todos los procedimientos y metodologías para el área de desarrollo, enfocado en los nuevos sistemas y modificaciones sobre los ya existentes. Los sistemas actuales no han seguido una metodología uniforme, ni producido toda la documentación necesaria. En el marco del control de versiones automático, se posee sistema automático de control de versiones y pasaje a producción que cumple con los requerimientos de la norma, sin embargo aún no ha sido normado su utilización. Se ha iniciado el estudio de cómo gestionar las vulnerabilidades técnicas en la metodología de desarrollo.

A.15 Relaciones con Proveedores

Para las relaciones con Proveedores de bienes y servicios relacionados con tecnología se aplican las normativas de la APN y los Estándares Tecnológicos para la Administración Pública (ETAP), lo cual esta adecuado a la norma y es auditado en forma periódica. La supervisión y revisión de los servicios del proveedor aún no está estandarizada y depende del nivel de conocimiento de la persona encargada del mismo, siendo este un aspecto a implementar.

A.16 Gestión de Incidentes de Seguridad

La política está aprobada pero aún no han sido generados los procedimientos correspondientes. No hay una detección de incidentes activa, sino una respuesta a los efectos provocados por estos. El manejo del incidente depende del nivel de conocimiento de la persona encargada de gestionarlo, siendo diferente para distintos entornos.

A.17 Gestión de la Continuidad

La política está aprobada pero aún no han sido generados los planes y procedimientos correspondientes, aunque es un tema que ha sido destacado por auditaría hace bastante tiempo. Si existe dentro del organismo un alto nivel de redundancia en los equipos e instalaciones críticas del organismo.

A.18 Cumplimiento

El Cumplimiento de requisitos legales es acorde con un organismo de la APN, variando el grado de algunos de sus componentes entre definido y repetible. No se han realizado en forma periódica, ni en esta versión ni en anteriores revisión de la política de seguridad. Las auditorias de sistemas se realizan en ambientes separados al de producción

El resultado detallado de ambos análisis se puede consultar en los documentos de “Uso Reservado - Interno” Anexos A y B (archivos separados en esta versión).

2. ESQUEMA DOCUMENTAL

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo. Esto significa que en nuestro Sistema de Gestión de Seguridad de la Información tendremos que tener una serie de documentos, los cuales vienen establecidos en la propia norma ISO/IEC 27001

A continuación se detallan los documentos que formaran parte del presente trabajo:

2.1 Política de Seguridad

De acuerdo con lo expresado por la Decisión Administrativa N° 669/2004 de la Jefatura de Gabinete de Ministros la política de seguridad de la información del organismo está basada en la "Política de Seguridad de la Información Modelo" dictada por la Oficina Nacional de Tecnologías de la Información (ONTI). La política presentada en esta planificación se corresponde con la aprobada mediante Disposición 1/2015 de ONTI.

Las Políticas de Seguridad de la Información son agentes fundamentales para la concientización de los funcionarios, para la prestación adecuada de servicios y para la administración de los activos informáticos en un entorno moderno en el cual se utilizan tecnologías modernas, en un ambiente dinámico en el que la seguridad es fundamental para la protección ante amenazas de diferente tipo. Es función de estas políticas sentar las bases para la gestión de la Seguridad del Información en el ámbito del organismo, para la protección de los pilares fundamentales de la información: Confidencialidad, Integridad y Disponibilidad.

Las Políticas de Seguridad de la Información incluyen componentes de gestión de activos, gestión de usuarios, gestión de la infraestructura, disposición adecuada de servicios de información entre otros. Un listado de los 14 capítulos que la componen es el siguiente:

1. Introducción
2. Términos y Definiciones
3. Estructura de la política
4. Evaluación y tratamiento de riesgos
5. Política de Seguridad de la Información
6. Organización
7. Recursos Humanos
8. Gestión de Activos
9. Gestión de Accesos
10. Criptografía
11. Física y Ambiental
12. Seguridad en las operaciones
13. Gestión de Comunicaciones
14. Adquisición, Desarrollo y Mantenimiento de Sistemas
15. Relaciones con Proveedores
16. Gestión de Incidentes de Seguridad
17. Gestión de la Continuidad
18. Cumplimiento

La política de Seguridad de la Información para el organismo se adjunta como Anexo C del presente documento.

2.2 Procedimiento de Auditorías Internas

El organismo posee una Unidad de Auditoría Interna (UAI) la cual es parte integrante del sistema de control interno del mismo. Estas unidades dependen jerárquicamente de la autoridad superior de cada organismo y actúan coordinadas técnicamente por la Sindicatura General de la Nación.

La actividad de la unidad de Auditoría Interna del organismo está regulada por la Sindicatura General de la Nación, en particular la labor de auditoría se realiza siguiendo la Resol 125/2002 SGN la cual aprueba las "Normas de Auditoría Interna Gubernamental" en su artículo 1°, y luego indica que las mencionadas normas serán de aplicación en todo el Sector Público Nacional (artículo 2°). Dentro de esta normativa se indican la forma de planificar un proyecto de auditoría, los procedimientos que pueden aplicar durante una auditoría, los papeles de trabajo que deben acompañar a un proyecto, la elaboración de observaciones y recomendaciones y los elementos que deben incluirse en el informe, entre otros temas. Las "Normas de Auditoría Interna Gubernamental" se encuentran en el Anexo D del presente documento. Ampliando esta normativa se encuentra la Res 3/2011 "Manual Control Interno Gubernamental" la cual figura como Anexo E.

La composición actual de la UAI es de 6 personas, de las cuales solo 1 posee formación para realizar auditorías asociadas con tecnologías de la información.

- Auditor de Sistemas Informáticos (personal de planta): Ingeniero en Sistemas con 7 años de experiencia en auditoría.

Además todos los proyectos son supervisados por: Auditor Interno (cargo extraescalafonarío), el cual es un profesional en Ciencias Económicas con por lo menos 4 años de experiencia en auditoría, pero sin formación específica en sistemas de información.

Sería aconsejable para acelerar los tiempos y mejorar los resultados de la revisión la contratación de un consultor certificado como auditor líder de sistemas de gestión en ISO 27001:2013 y un experto en ethical hacking para algunos proyectos dentro del plan. Se elevará la propuesta a la dirección del organismo pero no se tendrá en cuenta para esta planificación.

Dentro de las pautas implementadas por SIGEN cada UAI debe presentar un "Plan Anual", el cual es una planificación detallada de la ejecución del próximo año, dentro de este plan se incluye un "Plan Estratégico" el cual enumera los proyectos de auditoría a realizar durante un ciclo de 4 años, en el cual se debe planificar la realización de por lo menos un proyecto a todos los procesos del organismo. Para la organización de estos proyectos dentro del plan estratégico se toma en cuenta un análisis de riesgo que se realiza sobre los procesos del organismo, y la disponibilidad de personal especializado dentro de la UAI. Los lineamientos para la realización de estos planes se encuentran en la RESOL-2018-176-APN-SIGEN "Instructivo para la elaboración de los planeamientos anuales de trabajo UAI". A continuación se presenta ese apartado tomando solo los planes asociados a la revisión del SGSI:

PROYECTOS DE AUDTORIA ASOCIADOS			Período de Ejecución			
Id	**Descripción**	**Área Temática**	**'21**	**'22**	**'23**	**'24**
1	*SI – Revisión implantación SCGI (ISO/IEC 27001 4-10)*	*Rev SGSI*	**X**	**X**	**X**	
2	*SI - Aspectos Organizacionales de Gestión y Seg. (Cap 5-6-7-8)*	*Rev PSI*	**X**			
3	*SI - Proveedores y Cumplimiento (Cap 15 -18)*	*Rev PSI*	**X**			
4	*SI - Adquisición, Desarrollo y Mantenimiento de Sistemas- Criptografía (Cap 10 - 14)*	*Rev PSI*	**X**			
5	*SI - Seguridad Física, Ambiental y Gestión de Accesos (Cap 9-11)*	*Rev PSI*		**X**		
6	*SI - Gestión de Comunicaciones y Operaciones (Cap 12 - 13)*	*Rev PSI*		**X**		
7	*SI - Gestión de Incidentes y Continuidad (Cap 16 - 17)*	*Rev PSI*			**X**	
8	*TI - Administración de prestación de servicios de proveedores*	*Aud Cumpl.*				**X**
9	*TI - Auditoria Técnica Seguridad Aplicaciones Web*	*Aud Tec*		**X**	**X**	**X**
10	*TI - Auditoria Técnica Gestión de Usuarios y Privilegios*	*Aud Tec*		**X**	**X**	**X**
11	*TI - Auditoria Técnica Verificación entorno Trabajo Remoto*	*Aud Tec*	**X**			
12	*TI - Auditoria Técnica Infraestructura Servidores Aplicación*	*Aud Tec*			**X**	
13	*TI - Auditoria Técnica Infraestructura Redes y Comunicaciones*	*Aud Tec*				**X**

"Figura 7: Plan Estratégico de Sistemas"

El auditor de sistemas también participa como apoyo en otros proyectos a lo largo del plan estratégico, tareas que no se ven reflejadas en el cuadro anterior.

En el anexo F se encuentra la planificación detallada de las auditorías de los Sistemas de Gestión de Seguridad de la Información y la Implementación de Controles del organismo para los próximos 3 años.

2.3 Gestión de Indicadores

Los indicadores se utilizan para medir la eficacia de los controles de seguridad implantados, de una manera continua. Actualmente el organismo no ha definido ningún indicador, siendo las evaluaciones de los controles a través de las auditorias que realiza el organismo las cuales están muy espaciadas en el tiempo.

Teniendo en cuenta lo arriba expresado, para esta en esta primera etapa se establecerán una serie de indicadores que permitan controlar el funcionamiento de las medidas de seguridad de la información implantadas basándonos en el análisis diferencial realizado en el presente trabajo, tomando los controles que creemos necesario reforzar o vigilar al implementar el SGSI.

Se implementarán indicadores sobre los siguientes controles:

- A.6.1.5 Acuerdos de confidencialidad
- A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
- A.8.1.3 Uso aceptable de activos
- A.9.2.2 Registración de usuarios
- A.14.5.1 Vulnerabilidades técnicas
- A.12.2.1 Control contra malware
- A.12.6.1 Gestión de las vulnerabilidades técnicas
- A.16.1.1 Reporte de los eventos de la seguridad de información
- A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

La descripción de los indicadores para el organismo se adjunta como el documento de “Uso Reservado - Interno” Anexo G del presente documento.

2.4 Procedimiento Revisión por Dirección:

Un Sistema de Gestión de la Seguridad de la Información debe ser evaluación en forma periódica, sistemática y estructurada por parte de la alta dirección, con el propósito de asegurar el cumplimiento de los objetivos del mismo. En el caso del organismo esta revisión se realiza a través del Comité de Tecnología y Seguridad de la Información y Comunicaciones (CoTySIC), creado mediante la Res. A149/2014 del mismo. Analizando algunas de las funciones y responsabilidades asignadas mediante la DA 669/2004, en particular los artículos 2 y 4:

- Revisar y proponer a la máxima autoridad del organismo para su aprobación, la Política y las responsabilidades generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

Se ha generado un procedimiento para la revisión del SGSI el cual se adjunta como Anexo H del presente documento. Por reglamento de funcionamiento la frecuencia de reuniones del comité es trimestral, con la opción de ser convocado a reuniones extraordinarias cuando sea necesario, para estas revisiones se utilizará una reunión ordinaria.

2.5 Gestión de Roles y Responsabilidades

Para el correcto desarrollo de un Sistema de Gestión de la Seguridad de la Información es necesaria la asignación de diversos roles dentro de la organización, junto con las responsabilidades asociadas a estas cuya función será crear, mantener, supervisar y mejorar el SGSI.

El organismo mediante la Res. A149/2014 creó los principales roles dentro de un esquema de seguridad:

- Comité de Seguridad de la Información
- Responsable de Seguridad de la Información

En el organismo el Comité de Seguridad de la información es incluido dentro de la figura del "Comité de Tecnología y Seguridad de la Información y Comunicaciones" (CoTySIC), el cual está compuesto por:

- Presidencia del Organismo
- Coordinador del Comité de Seguridad de la Información
- Gerencia de Fiscalización
- Subgerencia de Planificación
- Subgerencia Operativa
- Coordinación de Alcoholes
- Subgerencia de Administración
- Subgerencia Jurídica
- Mesa de Ayuda del Dto. de Informática Y Comunicaciones
- Unidad de Auditoría Interna
- Responsable de Seguridad

En la misma Resolución se nombra como Coordinador del Comité al Responsable del Departamento de Informática y Comunicaciones.

Las funciones asignadas al comité son las siguientes:

- Revisar y proponer a la máxima autoridad del organismo para su aprobación, la Política y las responsabilidades generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

En cuanto al rol de Responsable de Seguridad de la Información también fue asignado al Jefe del Departamento de Informática y Comunicaciones; junto con las siguientes funciones:

- Funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye: la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

Además en la cláusula “5.Política de Seguridad de la Información”, en el apartado “Responsabilidades” se describen los otros roles necesarios dentro del organismo para la ejecución del SGSI. :

- Responsable de Seguridad de la Información.
- Propietarios de activos de información.
- Responsable del Área de Recursos Humanos.
- Responsable de Capacitación.
- Responsable del Área Informática.
- Responsable de Seguridad Física.
- Responsable del Área Legal o Jurídica.
- El Responsable del Área Administrativa.
- Usuarios de la información y de los sistemas.
- Unidad de Auditoría Interna.

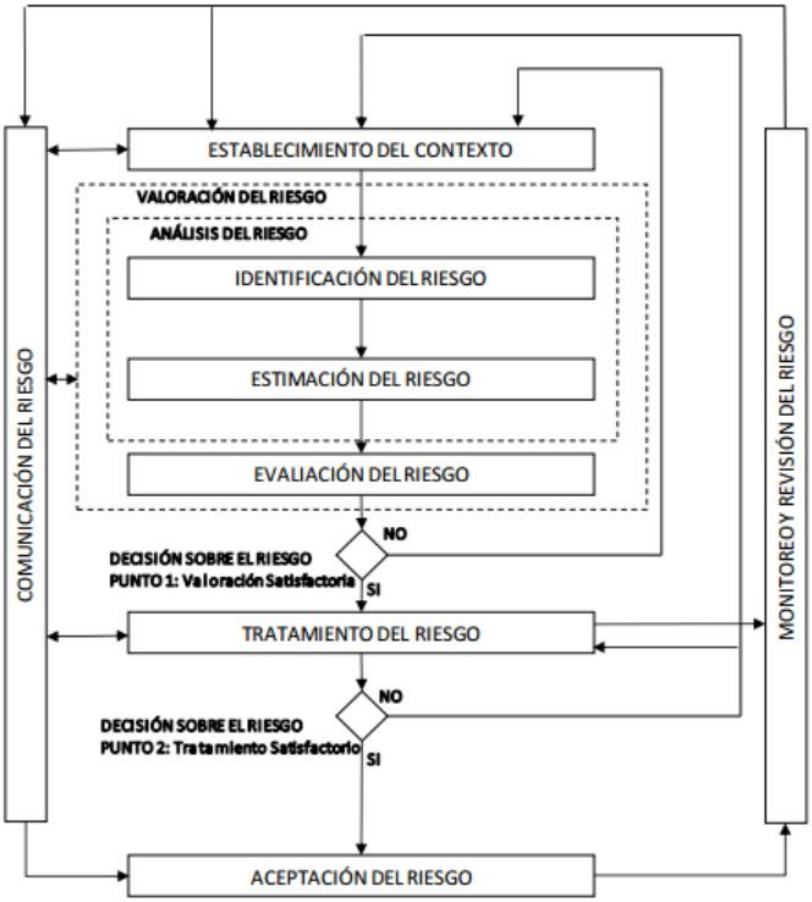
2.6 Metodología de Gestión del Riesgo

La realización de un análisis de Riesgos y su posterior tratamiento es un elemento imprescindible para la implementación de un Sistema de Gestión de la Seguridad de la Información. Teniendo en cuenta que la Disp. 1/2015 ONTI no indica una metodología en particular para el análisis de riesgo se ha optado por diseñar una que sea compatible con ISO 27005 y a la vez se adapte a las características del organismo.

La metodología propuesta se basa en activos, donde la identificación de los riesgos a los que estos están expuestos se realizará mediante la determinación de las amenazas existentes sobre los activos, para luego calcular la probabilidad y el impacto que van a causar.

Se ha tomado en cuenta la dificultad en la valoración de activos debido a la naturaleza de la organización y el enfoque en procesos de la Administración Pública Argentina para elegir una valoración cualitativa dentro de la metodología que proponemos.

Teniendo en cuenta los factores mencionados con anterioridad se propone que el cálculo del riesgo se realice teniendo en cuenta un análisis de las salvaguardas o controles implementados actualmente en el organismo, lo cual implica que el resultado del análisis arrojará un riesgo del tipo residual.



"Figura 8: Gestión de Riesgo de Seguridad ISO/IEC 27005"

La metodología cuenta con las siguientes etapas, adecuadas al estándar ISO 27005:

- Identificación del Riesgo
    i. Identificación de activos
    ii. Clasificación de activos
    iii. Identificación de amenazas
    iv. Análisis de controles existentes
- Estimación del Riesgo
    i. Análisis del impacto
    ii. Determinación del riesgo
- Evaluación del Riesgo
- Tratamiento de Riesgos

2.6.1 Identificación del Riesgo

El objetivo de este paso es conocer el nivel de exposición de los activos de información frente a las amenazas aplicables al entorno de funcionamiento de los procesos, es decir conocer los riesgos a los cuales se encuentra expuesto. Este paso incluye las siguientes etapas:

Identificación de activos: El primer paso para el análisis de riesgo es realizar el inventario de activos de información. Se entenderá por **activo de información/primarios** a cada sistema de información o aplicación informática utilizada para generar o manipular información del organismo. La otra categoría es la de los **activos de soporte**, los cuales refieren a activos físicos, activos de software, contenedores de datos, servicios de redes y telecomunicaciones e infraestructura tecnológica.

La dependencia entre activos se entiende en la medida que uno brinde servicios o soporte de algún tipo a otro, formando un árbol de dependencias que no implica jerarquía. Los activos incluidos en las categorías información son los que establecen los requisitos de seguridad para los otros los activos de soporte.

A cada activo se le asignará un propietario que deberá cumplir con las responsabilidades emanadas de la política de seguridad del organismo.

Clasificación de activos: La clasificación de los activos se realizará en base a la asignación de valores a tres dimensiones de la información: Confidencialidad (C), Integridad (I) y Disponibilidad (D). No se utilizaran criterios de valoración económica en el activo, pero si se identificará el tipo de proceso al que están asociados, siendo los valores de esta clasificación Sustantivo, Conducción y Apoyo en ese orden de importancia. El resultado de estas dimensiones nos dará una valoración del activo en función de la criticidad.

Los activos de soporte no serán clasificados, heredarán la criticidad del activo asociado al mismo, para el caso que sea más de uno se tomará la criticidad más alta entre todos los activos asociados. Cuando se trate de activos de redes o infraestructura se asignará la criticidad en base a la importancia en términos operativos de la unidad organizativa a la que presta servicio.

Identificación de amenazas: En el marco de esta metodología emplearemos la siguiente definición de amenaza: “Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

Para implementar esta metodología nos basaremos en el catálogo de amenazas propuesto por MAGERIT (Libro 2 “Catálogo de Elementos” - Punto 5), pero fusionando las categorías “Desastres Naturales” y “De origen industrial” en una sola llamada “Del Entorno”. Por lo tanto las amenazas quedan clasificadas en los siguientes bloques:

- Del Entorno
- Errores y fallos no intencionados
- Ataques intencionados

Luego de identificar las amenazas que pueden afectar nuestros activos, se realizará una valoración las características de cada uno para determinar la Frecuencia. Entendiendo por frecuencia cuan probable o improbable es la materialización de la amenaza.

Análisis de Controles: Este paso busca reflejar de manera práctica la minimización de la probabilidad de la amenaza teniendo en cuenta la madurez de las salvaguardas. Se evalúa el grado de implementación de los controles, donde se tiene en cuenta si están implementados controles técnicos, controles organizativos y el grado de supervisión sobre ambos.

2.6.2 Estimación del Riesgo

El riesgo es una función del impacto y la probabilidad de ocurrencia de una amenaza. Este paso incluye las siguientes etapas:

Análisis del Impacto: Ese calculara el impacto teniendo en cuenta el valor del activo, proveniente del campo valoración de la clasificación del activo y la degradación estimada.

Determinación del Riesgo: Teniendo calculado el impacto y la probabilidad podemos calcular el riesgo de acuerdo a la fórmula

Riesgo = Impacto x Probabilidad

RIESGO		Frecuencia				
		MB	B	M	MA	A
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	B	B	B

"Figura 9: Matriz de calificación en función de Impacto y Probabilidad"

Aún se están ajustando los parámetros de esta estimación.

2.6.3 Evaluación del Riesgo

Como se ha indicado en el comienzo de este punto el análisis del riesgo va a contemplar los controles implementados por lo tanto ya es un análisis de Riesgo Residual y no es necesario calcular nuevamente el riesgo residual, hasta el próximo periodo indicado en la política de seguridad.

Propiedad del Riesgo: Dada la estructura del organismo, se designa como propietario de todos los riesgos al "Comité de Tecnología y Seguridad de la Información y Comunicaciones" (CoTySIC).

Nivel de Riesgo Aceptable: En este punto debemos determinar lo que se considera el nivel de riesgo aceptable para el organismo. El punto a partir del cual se debe proceder a realizar el tratamiento del riesgo.

Teniendo en cuenta un correcto equilibrio entre costo de protección y costo de exposición, la utilización del riesgo residual como criterio de estimación se fija un umbral de riesgo igual a Medio.

2.6.4 Tratamiento del Riesgo

Los riesgos que se encuentran por arriba del nivel aceptable de riesgo deben ser tratados eligiendo entre una de las siguientes 4 opciones:

Mitigarlo: Esta acción implica implantar los controles necesarios con el fin de que el nivel de riesgo disminuya a un punto que se encuentre bajo el límite aceptable. Para conseguir este objetivo se pueden realizar acciones preventivas o reducir el impacto de la amenaza. Esta es la primera opción por defecto que debe aplicar el organismo, las demás serán tratadas como excepciones.

Transferirlo: Mediante esta acción la organización comparte o traspasa a terceros el riesgo con el fin que sean éstos quienes puedan reducir su impacto o gestionar el riesgo de mejor manera. Esta situación se presenta si el organismo no tiene los recursos o capacidad para mitigar el riesgo y no puede aceptarlo por la gravedad que representa. En el caso del organismo también puede darse esta opción cuando es indicado desde el poder ejecutivo nacional.

Evitarlo: Esta decisión implica tomar acciones tendientes a impedir que el riesgo se vuelva una realidad. Este puede realizarse mediante la sustitución del activo por uno que este dentro de un nivel de riesgo aceptable, o en última instancia no continuar la actividad relacionada con el activo.

Aceptarlo: Se entiende por aceptar un riesgo no realizar ninguna acción (de las 3 propuestas anteriormente) que permita evitar que se produzca. Esta decisión solo se debería tomar si no es posible ejecutar ninguna de las acciones anteriores, pero la probabilidad del mismo es baja o media-baja. La decisión de que la organización trabaje aceptando que está expuesta al riesgo si las probabilidades son mayores debe tomarse en forma excepcional y dejarse asentado en acta del comité.

Se realizará un documento de tratamiento de riesgos indicando la opción elegida y de medidas de seguridad de corresponder para todos los riesgos por encima del umbral.

La descripción detallada y aplicación de la presente metodología se incluye en el capítulo 3. Riesgos del presente trabajo.

2.7 Declaración de Aplicabilidad

La declaración de aplicabilidad es un documento exigido por la norma ISO/IEC 27001 en la cual se selecciona los controles a implementar o se justifica la omisión en el SGSI de la organización, basado en los resultados y conclusiones de la valoración y el tratamiento del riesgo. En el caso

del organismo nos basaremos en los controles enumerados en la Disp. 1/2015 como hemos realizado a lo largo de todo el trabajo.

Otro elemento que se incluirá en el análisis es el origen del control de acuerdo al siguiente detalle:

RL: Requerimiento Legal
OC: Obligación Contractual
RN: Requerimiento del Negocio
ER: Evaluación de Riesgos

Al ser obligatoria la implementación de la DISP 1/2015 para organismo de la administración pública nacional Argentina, todos los controles aplicables poseen como origen "RL" primario, pudiendo sumarse otro origen de los expuestos.

Finalizado el análisis de riesgos, se han detectado 19 controles que el organismo debe implementar o reforzar para alcanzar el nivel de riesgo estipulado.

Un resumen de la aplicabilidad de los controles es el siguiente:

Clausula	Controles Aplicados	Controles Desestimados
A.5 Política de Seguridad de la Información	2	-
A.6 Organización	10	-
A.7 Recursos Humanos	9	-
A.8 Gestión de Activos	7	1
A.9 Gestión de Accesos	21	1
A.10 Criptografía	5	1
A.11 Física y Ambiental	13	2
A.12 Seguridad en las operaciones	15	-
A.13 Gestión de Comunicaciones	6	-
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	17	-
A.15 Relaciones con Proveedores	5	-
A.16 Gestión de Incidentes de Seguridad	6	-
A.17 Gestión de la Continuidad	6	-
A.18 Cumplimiento	13	-

"Figura 10: Resumen Declaración Aplicabilidad"

La declaración de Aplicabilidad está incorporada en el documento de "Uso Reservado - Interno" Anexo I del presente trabajo.

3.ANÁLISIS DE RIESGOS

La realización de un análisis de Riesgos y su posterior tratamiento es un elemento imprescindible para la implementación de un Sistema de Gestión de la Seguridad de la Información. Se ha generado una metodología que sea compatible con ISO 27005 y a la vez se adapte a las características del organismo.

La metodología propuesta se basa en activos, donde la identificación de los riesgos a los que estos están expuestos se realizará mediante la determinación de las amenazas existentes sobre los activos, para luego calcular la probabilidad y el impacto que van a causar.

Se ha tomado en cuenta la dificultad en la valoración de activos debido a la naturaleza de la organización y el enfoque en procesos de la Administración Pública Argentina para elegir una valoración cualitativa dentro de la metodología que proponemos.

Teniendo en cuenta los factores mencionados con anterioridad se propone que el cálculo del riesgo se realice teniendo en cuenta un análisis de las salvaguardas o controles implementados actualmente en el organismo, lo cual implica que el resultado del análisis arrojará un riesgo del tipo residual.

3.1 Inventario de Activos

El primer paso para la gestión de riesgos es la identificación de los activos de información del organismo, los cuales se registraran dentro del inventario de acuerdo con las siguientes categorías:

- **Activo de información o primarios:** Aquí se incluirán todos los sistemas de información donde procesa información del organismo. No importa si los mismos son administrados dentro del organismo, o son parte de los que brinda el estado nacional para manejar aspectos centralizados de la gestión. En esta categoría no se realizará agrupamiento, pero no se trataran igual a todos sus elementos. Los activos del tipo "Externo" no se tomarán dentro del análisis de riesgo por no poder aplicar ningún control sobre los mismos y estar obligados a utilizarlos. En términos de gestión del riesgo los riesgos sobre esos activos son "Aceptados". Se incluyen en el inventario para identificar los contenedores de información del organismo y para formalizar quién es el funcionario encargada de autorizar el acceso a los mismos.
- **Activos de soporte:** Se ubican es esta categoría el Hardware, las aplicaciones, contenedores de datos (bases de datos, archivos, etc.), redes, Instalaciones, personal y servicios asociados a TIC's. Los activos de esta categoría se identificarán en grupos de elementos que comparten características similares para este estudio. Se tomará en cuenta naturaleza del activo, amenazas sobre el mismo y vulnerabilidades posibles para ese agrupamiento.

A su vez a los activos de información se les asignarán un subtipo, basado en la clasificación de procesos expuesta por la Sindicatura General de la Nación, de acuerdo al siguiente detalle:

Subtipos Activos de Información	
Sustantivos	Activos asociados a procesos que permiten el cumplimiento de los objetivos fundamentales de la organización, dando por resultado un producto (bien o servicio) que es recibido por el ciudadano/usuario, o por entes externos.
Conducción	Activos asociados a procesos destinados a dar sostén operativo para el cumplimiento de los objetivos de los procesos sustantivos.

Apoyo	Activos asociados a procesos dirigidos a organizar y facilitar la coordinación de la totalidad de los procesos de la organización (ejemplos: plan estratégico, gestión de riesgos, otros).
Externo	Sistemas asociados a todo tipo de proceso cuya administración no es llevada a cabo por el organismo, sin embargo brinda servicios y almacena datos relativos al organismo.

"Figura 11: Subtipos Activos de Información"

Para cada activo de información se le definirán los siguientes datos:

- Categoría: Tipo del activo de acuerdo con la figura 11.
- Identificación: Código alfanumérico de identificación única (Categ+Num).
- Nombre Activo: Identificación formal del activo para el organismo, generalmente se corresponde con el nombre del sistema pero hay excepciones.
- Proceso: Nombre del procesos de nivel superior al que presta servicio el activo
- Propietario: Unidad organizativa encargada de establecer los valores de disponibilidad, confidencialidad e integridad del activo. La responsabilidad siempre está en la máxima autoridad de la unidad mencionada.
- Responsable Operativo y Responsable Informático: Están asignados pero no se han colocado por un tema de confidencialidad
- Prioridad: Este valor se utiliza para calcular la criticidad del activo incluyendo otro factor además de los valores de DCI

Para los activos de soporte los subtipos son los siguientes:

Subtipos Activos de Soporte		
Hardware	HW	Equipos electrónicos que soportan directa o indirectamente los servicios que presta la organización.
Software	SW	Conjunto de componentes lógicos que contribuyen al procesamiento de la información. Por ejemplo: aplicaciones informáticas, software de sistemas. Están excluidos de esta categoría los activos de información
Infraestructura	IF	Equipamiento que brinda soporte auxiliar al funcionamiento de los activos de hardware
Redes - Comunicaciones	RC	Instalaciones y servicios de comunicaciones utilizados para transportar información
Contenedores Datos	CD	Dispositivos físicos o lógicos que permiten almacenar información
Personal	P	Grupos de Personas relacionados con los sistemas de información

Servicios	S	Todos los servicios contratados a un proveedor externo que intervienen en el manejo de la información

"Figura 12: Subtipos Activos de Soporte"

Para cada activo de soporte se le definirán los siguientes datos:

- Categoría: De acuerdo a lo descripto en la figura 12.
- Identificación: Código alfanumérico de identificación única (Categ+Num).
- Nombre Activo: Identificación del activo para el organismo.
- Activo de Información Relacionado
- Propietario
- Valoración
- Criticidad

La dependencia entre activos se generará en la medida que uno brinde servicios o soporte de algún tipo a otro, formando un árbol de dependencia que no implica jerarquía. Los activos de información dependerán de los activos de soporte, mientras que estos últimos pueden depender a su vez de otros activos de soporte.

Todos los activos de soporte son propiedad del Jefe del Departamento de Informática y Comunicaciones, exceptuando al personal no vinculado con tareas de tecnología.

3.2 Valoración de los Activos

No se utilizaran criterios de valoración económica en el activo de información, pero si se identificará el tipo de proceso al que están asociados, basada en la clasificación de procesos expuesta por la Sindicatura General de la Nación. Siendo los valores de esta clasificación Sustantivo, Conducción y Apoyo en ese orden de importancia. El resultado de esta priorización nos dará uno de los criterios de valoración del activo junto con la criticidad.

La escala de valores que se utilizará para la Confidencialidad es la siguiente:

Valor	Tipo
3	SUSTANTIVO
2	CONDUCCION
1	APOYO
0	EXTERNO

"Figura 13: Valoración Activos de Información"

La valoración de Activos de Información se compone de la siguiente fórmula

Valoración = Prioridad + Valor Criticidad

Mientras que para los Activos de Soporte se tomará el mismo criterio que con la Criticidad, heredando la mayor valoración de los activos de nivel superior a los que prestan soporte.

3.3 Clasificación de Activos

La clasificación de los activos se realizará en base a la asignación de valores a tres dimensiones de la información: Confidencialidad (C), Integridad (I) y Disponibilidad (D). Las dimensiones parten de los siguientes conceptos:

Dimensión	
Confidencialidad	Esta característica garantiza que la información contenida por el activo sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Integridad	Esta característica consiste en que la información del activo no ha sido modificada de manera no autorizada. Es la que salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Disponibilidad	Característica que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

"Figura 14: Dimensiones Seguridad de la Información"

Los activos de información serán clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen por el Propietario del activo

La escala de valores que se utilizará para la Confidencialidad es la siguiente:

Valor Confidencialidad	Nivel	Descripción
0	USO PÚBLICO	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleada del organismo o no.
1	USO RESERVADO-INTERNO	Información que puede ser conocida y utilizada por todos los empleados del INV y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el INV, el Sector Público Nacional o terceros.
2	USO RESERVADO-CONFIDENCIAL	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al organismo, al Sector Público Nacional o a terceros.
3	USO RESERVADO-SECRETA	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros.

"Figura 15: Tabla valores Confidencialidad"

La escala de valores que se utilizará para la Integridad se define de la siguiente manera:

Valor Integridad	Nivel	Descripción
0	NO APLICA	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del organismo.
1	BAJO	Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el organismo, el Sector Público Nacional o terceros.
2	MEDIO	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el organismo, el Sector Público Nacional o terceros.
3	ALTO	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al organismo, al Sector Público Nacional o a terceros.

"Figura 16: Tabla valores Integridad"

La escala de valores que se utilizará para la Integridad se define de la siguiente manera:

Valor Disponibilidad	Nivel	Descripción
0	NO APLICA	Información cuya inaccesibilidad no afecta la operatoria del organismo.
1	BAJO	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el organismo, el Sector Público Nacional o terceros.
2	MEDIO	Información cuya inaccesibilidad permanente durante dos días podría ocasionar pérdidas significativas al organismo, al Sector Público Nacional o a terceros.
3	ALTO	Información cuya inaccesibilidad permanente durante seis horas podría ocasionar pérdidas significativas al INV, al Sector Público Nacional o a terceros.

"Figura 17: Tabla valores Disponibilidad"

Calculo de la criticidad:

Valor Criticidad	Nivel	Descripción
De 0 a 3	BAJA	El activo interviene en procesos que no están directamente relacionados con el negocio, aunque son necesarios. Su indisponibilidad causa algún contratiempo pero en ningún caso se vería afectada la continuidad del negocio.

De 4 a 6	MEDIA	El activo interviene en procesos de apoyo a la organización. Su indisponibilidad puede retrasar un determinado proceso pero no se vería afectada la continuidad de negocio
De 7 a 9	ALTA	El activo interviene en procesos clave para la organización (aquellos que son necesarios y suficientes) y su no disponibilidad puede poner en peligro la continuidad del negocio o contiene información con implicaciones legales

"Figura 18: Tabla valores Criticidad"

Los activos de soporte heredarán la criticidad del activo asociado al mismo, para el caso que sea más de uno se tomará la criticidad más alta entre todos los activos asociados.

3.4 Tabla Resumen de Valoración

Del proceso realizado se obtiene un inventario valorizado y clasificado, similar al mostrado en la figura 19 para la categoría "Activos de Información".

ID	NOMBRE	PROCESO	PROPIETARIO	PRIOR.	C	I	D	VALOR CRIT.	VALORACION	CRITICIDAD
IS1	XXX	CONTROL DE VOLUMEN	Gerencia de Fiscalización - Subgerencia Operativa	3	2	2	2	6	9	MEDIA
IS2	YYY	CONTROL DE VOLUMEN	Gerencia de Fiscalización	3	2	2	3	7	10	ALTA

"Figura 19: Inventario activos de Información con clasificación"

Dada la característica de este documento como "Uso Reservado - Interno" (confidencial), el inventario completo se adjunta como Anexo J del presente informe y no se debería hacerse público.

3.5 Análisis de Amenazas

Los activos del organismo, tanto de información como de soporte, están expuestos a amenazas, las cuales definimos como: "Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

Para implementar el análisis de amenaza nos basaremos en el catálogo de amenazas propuesto por MAGERIT (Libro 2 "Catálogo de Elementos" - Punto 5), pero fusionando las categorías "Desastres Naturales" y "De origen industrial" en una sola llamada "Del Entorno". Por lo tanto las amenazas quedan clasificadas en los siguientes bloques:

- Del Entorno [NI]
- Errores y fallos no intencionados [E]
- Ataques intencionados [A]

A continuación se detalla el catálogo de amenazas utilizado:

Tipo	Amenaza	Código	Cod. Magerit
Del Entorno	Fuego	NI1	N1-I1
	Daños por agua	NI2	N2-I2
	Tormenta Eléctrica	NI3	[I.*]
	Terremoto	NI4	[I.*]
	Fluctuaciones/Sobrecarga Eléctrica	NI5	[I.*]
	Explosiones	NI6	[I.*]
	Derrumbes	NI7	[I.*]
	Contaminación mecánica	NI8	[I.3]
	Contaminación electromagnética	NI9	[I.4]
	Avería de Origen Físico o lógico	NI10	[I.5]
	Corte Suministro Eléctrico	NI11	[I.6]
	Condiciones inadecuadas de temperatura o humedad	NI12	[I.7]
	Fallo de servicios de comunicaciones	NI13	[I.8]
	Interrupción de otros servicios y suministros esenciales	NI14	[I.9]
	Degradación de los soportes de almacenamiento de la información	NI15	[I.10]
	Emanaciones electromagnéticas	NI16	[I.11]
Errores y fallos no intencionados	Errores de los usuarios	E1	[E.1]
	Errores del administrador	E2	[E.2]
	Errores del monitorización	E3	[E.3]
	Errores de configuración	E4	[E.4]
	Deficiencias en la organización	E5	[E.7]
	Difusión de software dañino	E6	[E.8]
	Errores de [re-]encaminamiento	E7	[E.9]
	Errores de secuencia	E8	[E.10]
	Escapes de información	E9	[E.14]
	Alteración accidental de información	E10	[E.15]
	Destrucción de información	E11	[E.18]
	Fugas de información	E12	[E.19]
	Vulnerabilidades de los programas (software)	E13	[E.20]
	Errores de mantenimiento / actualización de programas (software)	E14	[E.21]
	Errores de mantenimiento / actualización de equipos (hardware)	E15	[E.23]
	Caída del sistema por agotamiento de recursos	E16	[E.24]
	Pérdida de equipos	E17	[E.25]
	Indisponibilidad del personal	E18	[E.28]
	Manipulación de los registros de actividad (log)	A1	[A.3]

Ataques intencionados	Manipulación de la configuración	A2	[A.4]
	Suplantación de la identidad del usuario	A3	[A.5]
	Abuso de privilegios de acceso	A4	[A.6]
	Uso no previsto	A5	[A.7]
	Difusión de software dañino	A6	[A.8]
	[Re-]encaminamiento de mensajes	A7	[A.9]
	Alteración de secuencia	A8	[A.10]
	Acceso no autorizado	A9	[A.11]
	Análisis de tráfico	A10	[A.12]
	Repudio	A11	[A.13]
	Interceptación de información (escucha)	A12	[A.14]
	Modificación deliberada de la información	A13	[A.15]
	Destrucción de información	A14	[A.18]
	Divulgación de información	A15	[A.19]
	Manipulación de programas	A16	[A.22]
	Manipulación de los equipos	A17	[A.23]
	Denegación de servicio	A18	[A.24]
	Robo	A19	[A.25]
	Ataque destructivo	A20	[A.26]
	Ocupación enemiga	A21	[A.27]
	Indisponibilidad del personal	A22	[A.28]
	Extorsión	A23	[A.29]
	Ingeniería social (picaresca)	A24	[A.30]

"Figura 20: Catálogo de Amenazas implementado"

Frecuencia	Nivel	Descripción
MA	MUY ALTA	Eventos que ocurren con frecuencia diaria o menor
A	ALTA	Eventos que ocurren con una frecuencia mensual
M	MEDIA	Eventos que ocurren cada 6 meses
B	BAJA	Eventos de ocurrencia anual
MB	MUY BAJA	Eventos que ocurren cada 5 o más años

"Figura 21: Tipificación de frecuencias de amenazas"

Luego de identificar las amenazas que pueden afectar nuestros activos, se realizará una valoración las características de cada uno para determinar la Probabilidad. Entendiendo por probabilidad es cuan probable o improbable es la materialización de la amenaza.

Se ha incluido la etapa de Análisis de Controles dentro del análisis de amenazas, para tener una visión del impacto de los controles sobre las probabilidades de cada amenaza sobre los activos del organismo. Se evalúa el grado de implementación de los controles, donde se tiene en cuenta si están implementados controles técnicos, controles organizativos y el grado de supervisión sobre ambos.

El grado de implementación de los controles o salvaguardas sobre los activos, los cuales reducen las probabilidades de que las amenazas se materialicen, se evalúa de acuerdo a la siguiente escala:

Valor	Nivel	Descripción
1	NO IMPLEMENTADO	No se ha implementado ningún control que mitigue la vulnerabilidad.
0.75	EN IMPLEMENTACION	Se ha iniciado la implementación del control.
0.50	IMPLEMENTACIÓN PARCIAL	Existe un control implementado, sin embargo aun puede perfeccionarse.
0.25	IMPLEMENTACIÓN TOTAL	EL control esta implementado en un nivel optimo, y su supervisión es la adecuada.

"Figura 22: Grado implementación Controles"

La evaluación sobre los controles se realiza en forma individual para cada amenaza, tomando los activos o grupos de activos sobre los que actúa. Luego se procede a calcular una "Probabilidad" que resulta de multiplicar la "Frecuencia" de la amenaza por el "Grado de Implementación" de los controles.

Probabilidad = Frecuencia x Grado de Impl. Controles

En la figura 23 podemos observar un resumen del resultado del cálculo de la probabilidad por cada tipo de amenaza:

TIPO AMENZA	PROBABILIDAD
Del Entorno	0,77
Errores y fallos no intencionados	1,02
Ataques intencionados	0,75

"Figura 23: Probabilidad por Tipo Amenaza"

En el anexo K se encuentra el documento de "Uso Reservado - Interno" Análisis de Amenazas.

3.6 Impacto Potencial y Cálculo del Riesgo

Habiendo calculado la Probabilidad debemos ahora determinar impacto de las amenazas en nuestros activos. Para eso realizaremos el Análisis del Impacto, esto es calcular las consecuencias que tendría la materialización de una amenaza sobre el activo, la degradación, teniendo en cuenta el valor del mismo estimado en la clasificación.

Para este análisis utilizaremos la degradación total de la amenaza sobre un activo o grupo de activos, entendiendo por esto el valor más alto de afectación sobre cualquiera de las dimensiones de la información de ese activo y las consecuencias que tendría cada una de las amenazas en caso de materializarse sobre el activo.

Los factores a tener en cuenta en el concepto de degradación son los siguientes:

- La información ha sido visualizada por personas que no tienen permisos para ello. Se produce una pérdida de Confidencialidad.
- La información ha sido modificada sin aprobación. La información sufre una pérdida de Integridad.
- Interrupción del Sistema. No existe posibilidad de acceder a la información. Existe una pérdida de Disponibilidad.
- Destrucción / Pérdida. Parte o toda la información se ha perdido.
- El sistema sigue funcionando con alguna limitación.
- El sistema se interrumpe con consecuencias limitadas.
- Interrupción del sistema con consecuencias severas.

El grado de afectación se medirá en porcentaje, y de acuerdo a la siguiente escala

Valor	Nivel	Descripción
0 %	NULO	La materialización de la amenaza no tiene impacto en el activo, o su impacto es insignificante. Funcionamiento normal.
25 %	BAJO	Se registran pérdidas menores en alguna dimensión, o interrupciones no significativas.
50 %	MEDIO	Afecta a más de una dimensión del activo, o sólo a una pero de manera grave. Se afecta la operatividad del organismo de manera intermedia.
75 %	ALTO	La materialización de la amenaza provoca la pérdida total de una o más dimensiones de la información y/o la interrupción del sistema.
100 %	MUY ALTO	La materialización de la amenaza provoca la perdida de activos o interrupción de procesos críticos de la organización.

"Figura 24: Porcentaje degradación activos"

Con la degradación ya determinada, vamos a proceder a tomar el valor del activo de acuerdo con el cálculo que realizamos en la clasificación de activos (campo Valoración), donde recordemos se tomó en cuenta no solo su criticidad, sino también el tipo de proceso al que da soporte el activo. Con estos 2 valores vamos a calcular el impacto de activo de acuerdo con la fórmula.

Impacto = Degradación x Valor

TIPO AMENZA	SUMA IMPACTO
Del Entorno	353,5
Errores y fallos no intencionados	364,5
Ataques intencionados	591

"Figura 25: Impacto por Tipo Amenaza"

Una vez que tenemos el valor del impacto podemos iniciar la **Determinación del Riesgo**, la cual se realizará utilizando el impacto y la probabilidad de acuerdo a la fórmula

Riesgo = Impacto x Probabilidad

La aplicación de esta fórmula se puede observar en el anexo L, documento de "Uso Reservado - Interno" Análisis de Riesgo.

3.7 Nivel de Riesgo Aceptable y Riesgo Residual

Sabiendo que el análisis realizado ya contempla los controles implementados por el organismo, siendo entonces un análisis de Riesgo Residual, se fijará un **Nivel de Riesgo Aceptable** acorde con esta premisa, y que en principio es más exigente con el nivel de riesgo permitido.

De acuerdo a lo decidido por el Comité de Tecnología y Seguridad de la Información y Comunicaciones el nivel de riesgo medio aceptable se fija en **Medio**, lo cual equivale a valores de riesgo iguales o mayores a **14** de acuerdo con la siguiente tabla.

Valor	RIESGO	
1 al 6	Muy Bajo	
7 al 13	Bajo	
14 al 20	Medio	
21 al 27	Medio Alto	
28 al 34	Alto	

"Figura 26: Niveles de Riesgo"

Los riesgos que se encuentren por debajo de este valor, se consideran aceptables y no deben ser tratados.

Se han identificado riesgos por arriba de este umbral en 5 tipos de amenazas, afectando a 9 categorías de activos. El siguiente es un detalle de las amenazas cuyos riesgos debería reducir el organismo

Errores de los usuarios [E1]
Errores de monitorización [E3]
Vulnerabilidades del software [E13]
Caída del sistema por agotamiento de recursos [E16]
Modificación deliberada de la información [A13]

El detalle completo de los resultados obtenidos en la clasificación de riesgos se puede observar en el anexo L, documento de "Uso Reservado - Interno" Análisis de Riesgo.

4.PROPUESTA DE PROYECTOS

Luego de realizado el Análisis de Riesgos, que nos permitió identificar los riesgos que superaron el umbral establecido, se proponen una serie de proyectos orientados a disminuir la brecha identificada, pero también a cumplir con los objetivos planteados para el plan director.

De entre esos objetivos destacamos los siguientes:

- Actualizar los estándares de desarrollo para incluir metodología que contemple la seguridad en todo el proceso de desarrollo de aplicaciones.
- Generar las normas y procedimientos faltantes en las clausulas de Desarrollo, Comunicaciones y Operaciones.
- Generar un Plan de Continuidad de Negocios.
- Generar una cultura en Seguridad de la Información, mejorando la formación y concientización del personal del organismo en temas relativos a la misma.

Para la formulación de los proyectos se debe tener en cuenta los resultados del Análisis Diferencial, pero teniendo en cuenta que la implementación de controles ya está considerada en el análisis de riesgos, lo cual se refleja en la probabilidad de las amenazas y que las principales cláusulas que presentan un bajo nivel de madurez están contempladas en los objetivos del plan director, no se utilizará en la mencionada formulación del portafolio de proyectos.

Para la formulación de los proyectos se ha tenido en cuenta una asignación de recursos un poco superior a la habitual con los que cuentan el Departamento de Informática y Comunicaciones, sin embargo está enmarcada dentro de las pautas que recibe el organismo, por lo que se entiende que se puede cumplir la misma en un marco de la ejecución de 1.5 años para que abarque recursos de 2 presupuestos.

Los proyectos propuestos se dividen en 2 categorías proyectos netamente tecnológicos, asociados con inversiones en hardware, software e infraestructura; y proyectos asociados a la gestión de la seguridad los cuales tienen como objetivo mejorar la organización de procesos y personal dentro del organismo.

Categoría	ID	Proyecto	Plazo Ejec.	Valor
TECNOLOGICO	PRT-1	RENOVACIÓN INFRAESTRUCTURA CRÍTICA DE ALTA DISPONIBILIDAD	Medio (6 meses)	USD 500.000
	PRT-2	IMPLEMENTACIÓN DE UN DATACENTER ALTERNATIVO UTILIZANDO TECNOLOGÍA IASS	Largo (9 meses)	USD 100.000
GESTIÓN	PRG-3	IMPLEMENTACIÓN PLAN DE CONTINUIDAD DEL ORGANISMO	Medio (6 meses)	S/C
	PRG-4	FORMACIÓN DEL PERSONAL EN SEGURIDAD DE LA INFORMACIÓN	Corto (3 meses)	USD 8.000
	PRG-5	MEJORA EN EL PROCESO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN	Medio (4 meses)	S/C
	PRG-6	DESARROLLO PROCEDIMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Medio (4 meses)	S/C
	PRG-7	CREACIÓN ÁREA SEGURIDAD DE LA INFORMACIÓN EN EL ORGANISMO	Medio (6 meses)	USD 2.000

"Figura 27: Listado Proyectos a Implementar"

4.1 Desarrollo Propuestas Tecnológicas

A continuación se desarrollan los 2 proyectos de corte tecnológico listados en la figura 27:

PRT-1	**RENOVACIÓN INFRAESTRUCTURA CRÍTICA DE ALTA DISPONIBILIDAD**
OBJETIVO	Adquirir hardware de alta disponibilidad para soportar los procesos de misión crítica del organismo. Migración del software hipervisor en los servidores de misión crítica.
DESCRIPCIÓN	La infraestructura crítica del organismo ha envejecido y se acerca al final de su ciclo de mantenimiento por parte de los proveedores. Es necesario renovar estos equipos no solo para poder dar una respuesta adecuada al crecimiento del organismo sino para evitar riesgos innecesarios. Se propone reemplazar a los servidores de misión crítica del organismo, el equipo NAS, los switches centrales y el robot de cintas. Además en esta renovación se propone migrar al software de virtualización que da soporte a estos servidores hacia VMware.
RESPONSABLE	Jefe Departamento de Informática y Comunicaciones
CONTROLES REL	A.11.2.4 Mantenimiento de los equipos A.12.1 Procedimientos y responsabilidades operativas A.17.2 Redundancias
ACTIVOS REL	HW1-HW2-HW3-HW8-HW9-SW3-SW4
RIESGOS A MITIGAR	Caída del sistema por agotamiento de recursos [E16]
PLAZO IMPL.	6 Meses (Medio)
PRESUPUESTO	USD 500.000

PRT-2	**IMPLEMENTACIÓN DE UN DATACENTER ALTERNATIVO UTILIZANDO TECNOLOGÍA IASS**
OBJETIVO	Implementar un Centro de Procesamiento de Datos (Datacenter) secundario para evitar la salida de servicio de los servicios informáticos que brinda el organismo ante una contingencia grave en el datacenter principal.
DESCRIPCIÓN	Instalar un datacenter alternativo en una delegación del organismo, lo cual incluye hardware, software, redes e infraestructura replicando las configuraciones necesarias para poder brindar un nivel de servicio aceptable. Se propone utilizar tecnología IaaS para implementar el respaldo de los servicios orientados a los inscriptos, mientras que los servicios de respaldo orientados al cliente interno se alojen en el CPD alternativo. Para instalar este CPD alternativo se necesita acondicionar la seguridad física del lugar, adquirir una UPS y un generador,

	equipos de refrigeración, instalar todo el cableado estructurado del nuevo sitio y reforzar los vínculos MPLS de la delegación seleccionada. Se propone reutilizar el hardware reemplazado en el PR-1 para disminuir el costo del proyecto.
RESPONSABLE	Jefe Departamento de Informática y Comunicaciones
CONTROLES REL	A.12.3 Resguardo (Backup) A.15 Relaciones con Proveedores A.16.2 Gestión de los incidentes y mejoras de la seguridad de la información A.17 Gestión de la Continuidad
ACTIVOS REL	HW1-HW2-HW3-HW7-HW8-HW9-RC4-RC7-SW.*
RIESGOS A MITIGAR	Fuego [NI1] Daños por agua [NI2] Explosión [NI6] Derrumbe [NI7] Difusión de software dañino [E6] / [A6] Caída del sistema por agotamiento de recursos [E16] Ataque destructivo [A20] Ocupación enemiga [A21]
PLAZO IMPL.	9 Meses (Largo)
PRESUPUESTO	USD 100.000

4.2 Desarrollo Propuestas Gestión de la Seguridad

A continuación se desarrollan los proyectos de Gestión de la Seguridad listados en la figura 27:

PRG-3	**IMPLEMENTACIÓN PLAN DE CONTINUIDAD DEL ORGANISMO**
OBJETIVO	Definir los planes de Contingencia del organismo para garantizar que las actividades del organismo puedan restablecerse dentro de los plazos requeridos.
DESCRIPCIÓN	Se deben analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro. Establecer planes que incluyan al menos las siguientes etapas: a) Determinación de la estrategia de contingencia. b) Identificación del alcance. c) Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan. d) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original. e) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.
RESPONSABLE	Responsable Seguridad de la Información
CONTROLES REL	A.15.2 Administración de prestación de servicios de proveedores A.16 Gestión de Incidentes de Seguridad A.17 Gestión de la Continuidad

ACTIVOS REL	*-IS.*-IA.*-IE.*
RIESGOS A MITIGAR	Fuego [NI1] Daños por agua [NI2] Explosión [NI6] Derrumbe [NI7] Difusión de software dañino [E6] / [A6] Caída del sistema por agotamiento de recursos [E16] Ataque destructivo [A20] Ocupación enemiga [A21]
PLAZO IMPL.	6 meses (Medio)
PRESUPUESTO	Se realizará todo con personal del organismo (responsable de seguridad, y Comité de Seguridad) por lo que no tiene costo adicional.

PRG-4	**FORMACIÓN DEL PERSONAL EN SEGURIDAD DE LA INFORMACIÓN**
OBJETIVO	Definir e implementar un Plan de Capacitación para en temas de seguridad de la información enfocado en las necesidades de cada grupo de empleados.
DESCRIPCIÓN	Se proponen 3 tipos de cursos a dictar para grupos de empleados con necesidades diferentes: - Curso básico de Seguridad orientado a todos los empleados que no forman parte del DIC. Temario mínimo: principios básicos de seguridad de la información, Política de Seguridad de la Información, Responsabilidades y Medidas disciplinarias. - Curso Desarrollo Seguro orientado a todos los desarrolladores del organismo. El temario debe ser orientado al Desarrollo Seguro y Modelado de Amenazas aplicado al Ciclo de Vida del Desarrollo del Software (SDLC) y la prevención de vulnerabilidades OWASP Top 10. - Curso Ciberseguridad orientado al personal de redes y seguridad de la información del organismo. El temario debe ser orientado al Hacking Ético, Hardening de Servidores, Seguridad en Cloud Computing e Informática Forense.
RESPONSABLE	Responsable Seguridad de la Información
CONTROLES REL	A.7.2 Durante el empleo
ACTIVOS REL	
RIESGOS A MITIGAR	Errores de los usuarios [E1] Errores de monitorización [E3] Difusión de software dañino[E6] Vulnerabilidades del software [E13] Uso no previsto [A5] Modificación deliberada de la información [A13]
PLAZO IMPL.	3 meses (Corto)
PRESUPUESTO	USD 8.000

PRG-5	MEJORA EN EL PROCESO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN
OBJETIVO	Implementar una Metodología de Análisis, Diseño y Desarrollo de Software que contemple los requisitos de seguridad durante todo el CVDS o la adquisición de software de aplicación.
DESCRIPCIÓN	La metodología a implementar debe contemplar los siguientes aspectos: - Gestión Requerimientos - Aprueba Las Especificaciones De Análisis/Diseño: - Estándares De Diseño, Programación Y Documentación - Procedimiento De Aseguramiento De La Calidad - Automatización Procedimiento De Pasaje A Producción. - Control Automático De Versiones De Software De Aplicación - Requerimientos de seguridad de los sistemas - Seguridad en el desarrollo y los procesos de soporte - Seguridad en los datos de pruebas
RESPONSABLE	Jefe División Desarrollo de Sistemas
CONTROLES REL	A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas
ACTIVOS REL	IS.*-IA.*
RIESGOS A MITIGAR	Avería de origen física o lógico [NI10] Errores de los usuarios [E1] Vulnerabilidades del software [E13] Suplantación de la identidad del usuario [A3] Abuso de privilegios de acceso [A4] Modificación deliberada de la información [A13]
PLAZO IMPL.	4 meses (Medio)
PRESUPUESTO	Se realizará todo el trabajo con personal del organismo (responsable de seguridad, y jefe DIC, jefe de desarrollo y auditor sistemas) por lo que no tiene costo adicional.

PRG-6	DESARROLLO PROCEDIMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
OBJETIVO	Desarrollar las políticas, procedimientos, estándares y guías, necesarios para finalizar la implementación de la política de seguridad de la información en el organismo.
DESCRIPCIÓN	Desarrollar, implementar y publicar la normativa necesaria para finalizar de implementar los siguientes aspectos del PSI: - Estándar de configuración conexiones remotas - Procedimiento autorización de Trabajo Remoto. - Acuerdos de Confidencialidad - Política de gestión de accesos - Procedimiento de "registro de usuarios, asignación de privilegios y administración de contraseñas" - Política de uso de controles criptográficos - Política de uso de correo y otros recursos de comunicación - Procedimientos operativos de redes identificados en el control

	A.12.1.1 “Documentación de los procedimientos operativos” - Procedimiento de cambios en los ambiente operativo y de comunicaciones - Política de retención y revisión de registros de auditoría. - Política de gestión de vulnerabilidades - Procedimiento de Gestión de Incidentes de Seguridad - Procedimiento de comunicación y registro de debilidades de seguridad y anomalías de software
RESPONSABLE	Jefe División Administración Sistemas
CONTROLES REL	A.6 Organización A.9 Gestión de Accesos A.10 Criptografía A.12 Seguridad en las operaciones A.13 Gestión de Comunicaciones A.16 Gestión de Incidentes de Seguridad
ACTIVOS REL	
RIESGOS A MITIGAR	Errores de monitorización [E3] Errores de los administradores [E2] Vulnerabilidades del software [E13] Manipulación de los registros de actividad [A1] Modificación deliberada de la información [A13]
PLAZO IMPL.	4 Meses (Medio)
PRESUPUESTO	Se realizará todo el trabajo con personal del organismo (responsable de seguridad, y jefe DIC, jefe de redes y auditor sistemas) por lo que no tiene costo adicional.

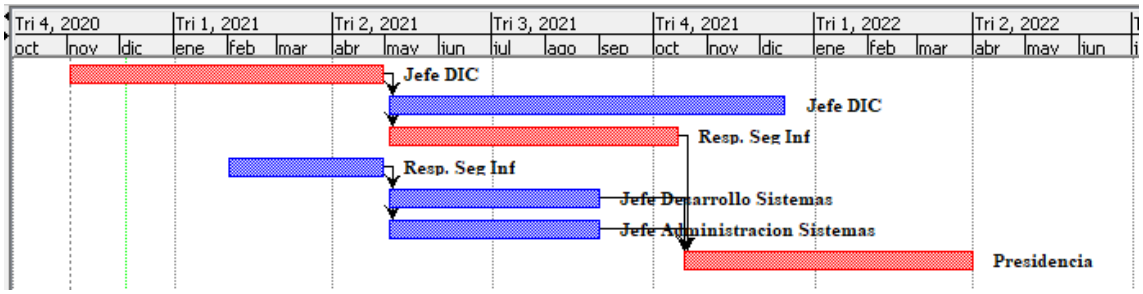
PRG-7	**CREACIÓN ÁREA SEGURIDAD DE LA INFORMACIÓN EN EL ORGANISMO**
OBJETIVO	Crear en la estructura del organismo una unidad organizativa abocada a la gestión de la seguridad de la información dependiente de Presidencia.
DESCRIPCIÓN	Para la creación de una nueva estructura se deben realizar los siguientes pasos: - Presentación de propuesta modificación estructura organismo mediante expediente. - Obtener la aprobación de las áreas intervinientes en este tipo de expedientes. - Formalización de la nueva área - Asignación de personal a la nueva área Se propone como composición para esta área - Responsable de Seguridad de la Información. - Analista Senior Seguridad de la Información.
RESPONSABLE	Presidencia
CONTROLES REL	A.6.1 Organización interna
ACTIVOS REL	
RIESGOS A MITIGAR	La jerarquización y especialización del personal abocado a la gestión de la seguridad de la información contribuye a disminuir

	todos los riesgos de la empresa.
PLAZO IMPL.	6 meses (Medio)
PRESUPUESTO	El costo es el de 2 sueldos de un profesional de la APN.

4.3 Calendarización Ejecución Proyectos

A continuación se muestra un diagrama de Gantt con la propuesta de ejecución de los proyectos desarrollados en los apartados 4.2 y 4.3

		Nombre	Duracion	Inicio	Terminado	Pred...	Nombres del Recurso
1		RENOVACIÓN INFRAESTRUCTURA CRÍTICA DE ALTA DISPONIBILIDAD	130 days	02/11/20 08:00	30/04/21 17:00		Jefe DIC
2		IMPLEMENTACIÓN DE UN DATACENTER ALTERNATIVO UTILIZANDO TECNOLOGÍA IASS	163 days	03/05/21 08:00	15/12/21 17:00	1	Jefe DIC
3		IMPLEMENTACIÓN PLAN DE CONTINUIDAD DEL ORGANISMO	120 days	03/05/21 08:00	15/10/21 17:00	1	Resp. Seg Inf
4		FORMACIÓN DEL PERSONAL EN SEGURIDAD DE LA INFORMACIÓN	65 days	01/02/21 08:00	30/04/21 17:00		Resp. Seg Inf
5		MEJORA EN EL PROCESO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN	87 days	03/05/21 08:00	31/08/21 17:00	4	Jefe Desarrollo Sistemas
6		DESARROLLO PROCEDIMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	87 days	03/05/21 08:00	31/08/21 17:00	4	Jefe Administracion Sistemas
7		CREACIÓN ÁREA SEGURIDAD DE LA INFORMACIÓN EN EL ORGANISMO	120 days	18/10/21 08:00	01/04/22 17:00	3;5;6	Presidencia



"Figura 28: Diagrama Gantt Proyectos a Implementar"

5.0 AUDITORÍA DE CUMPLIMIENTO

El objetivo de esta fase es evaluar el grado de cumplimiento de la buenas prácticas en materia de seguridad alcanzado en la implementación de los controles de la Disposición 1/2015.

Para poder analizar el grado de madurez, se requiere la realización de auditorías de cumplimiento sobre los controles, las cuales se corresponden en sus objetivos con las planificadas para los años 2021, 2022 y 2023 del área Revisión PSI (Id 2, 3, 4, 5, 6 y 7 de la figura 7). Sin embargo esos proyectos han sido diseñados no solo pensado en el cumplimiento, sino que también incluyen pruebas sustantivas sobre la efectiva ejecución de los procedimientos, normas y otros elementos incluidos en los controles. Por una cuestión de tiempo la revisión que se realizó para este apartado es sólo de cumplimiento y sirve como punto de partida, pero no invalida la planificación realizada para los años siguientes.

Idealmente esta auditoría deberíamos realizarla tras la finalización de los proyectos enumerados en el apartado 4, los cuales tienen por objetivo mitigar los riesgos identificados y solucionar los hallazgos detectados. Teniendo en cuenta que el organismo recién ha comenzado a ejecutarlos al momento de realizar esta auditoría nos encontramos con una situación de cumplimiento similar a la presentada en el análisis diferencial, sin embargo es

importante remarcar el trabajo realizado en esta etapa para presentar una visión completa del estado de situación de la implementación de los controles de la Política de Seguridad de la Información del organismo.

5.1 Desarrollo de la Auditoria

Esta auditoría de cumplimiento sigue la metodología indicada en el anexo D del presente trabajo, y fue llevada a cabo por un auditor en Sistemas Informáticos que es empleado del organismo.

Como se mencionó a lo largo del trabajo, el organismo ya poseía una política de seguridad con un proceso de implementación que se ha alargado en el tiempo y con auditorías realizadas sobre muchos de los dominios de la política. Los hallazgos pendientes resultantes de esas auditorías anteriores, revisando su vigencia obviamente, han sido incluidos dentro de esta etapa junto con la revisión del cumplimiento de los aspectos no revisado con anterioridad o los nuevos dominios que se incluyeron en esta versión de la política de seguridad.

Para determinar el alcance de la auditoría tuvimos en cuenta el Sistema de Gestión de la Seguridad implementado en el presente trabajo, y la declaración de aplicabilidad realizada en el punto 2.7, con lo cual las revisiones se aplicaron a los siguientes controles:

Clausula	Controles Aplicados
A.5 Política de Seguridad de la Información	**2**
A.6 Organización	**10**
A.7 Recursos Humanos	**9**
A.8 Gestión de Activos	**7**
A.9 Gestión de Accesos	**21**
A.10 Criptografía	**5**
A.11 Física y Ambiental	**13**
A.12 Seguridad en las operaciones	**15**
A.13 Gestión de Comunicaciones	**6**
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	**17**
A.15 Relaciones con Proveedores	**5**
A.16 Gestión de Incidentes de Seguridad	**6**
A.17 Gestión de la Continuidad	**6**
A.18 Cumplimiento	**13**

"Figura 29: Resumen Controles Alcanzados por la Auditoría"

Hay diferentes aspectos en los cuales las salvaguardas actúan reduciendo el riesgo, ya hablemos de los controles Disposición 1/2015 o de cualquier otro catálogo. Estos son en general:

- Formalización de las prácticas mediante documentos escritos o aprobados.
- Política de personal.
- Solicitudes técnicas (software, hardware o comunicaciones).
- Seguridad física.

La protección integral frente a las posibles amenazas, requiere de una combinación de salvaguardas sobre cada uno de estos aspectos.

La planificación de la auditoría se realizó siguiendo lo estipulado en el IT 6/2015-GNyPE "Revisión-Política-de-Seguridad-de-la-Información" que incluye los dominios arriba mencionados y el Análisis de Riesgo realizado sobre la institución

Para la presente auditoría se entrevistaron a los siguientes funcionarios:

- Responsable de Seguridad de la Información
- Responsable de Informática (DIC)
- Jefe de División Desarrollo (DIC)
- Jefe de División Administración de Sistemas (DIC)
- Responsable de Recursos Humanos
- Responsable de Seguridad Física
- Responsable del Área Administrativa
- Responsable del Área Legal:

Además se realizó una inspección visual del Datacenter del organismo y de todas las Áreas Seguras detalladas en el Listado de Sitios Protegidos.

5.2 Resultado de la Auditoria

Para acomodar la terminología expuesta en el anexo D y utilizada por SIGEN (Sindicatura General de la Nación) se expone la equivalencia los tipos de hallazgos utilizados en la terminología ISO/IEC 27001:2013

INFORME	CUMPLIMIENTO IT 6/2015	ISO/IEC 27001:2013
OBSERVACIÓN IMPACTO ALTO	NO – ALTO / MEDIO	NO CONFORMIDAD MAYOR
OBSERVACIÓN IMPACTO MEDIO	PARCIAL – ALTO PARCIAL – MEDIO	NO CONFORMIDAD MAYOR NO CONFORMIDAD MENOR
OBSERVACIÓN IMPACTO BAJO	NO – BAJO PARCIAL – BAJO	NO CONFORMIDAD MENOR NO CONFORMIDAD MENOR
		OPORTUNIDAD DE MEJORA

"Figura 30: Equivalencia terminología ISO/IEC 27011 y SIGEN"

Como se puede observar esta metodología no posee una clasificación para las oportunidades de mejora, motivo por el cual se expresarán como un comentario dentro de un control cuyo cumplimiento es "SI" identificándolo como "OpMejora:".

La metodología tampoco contempla las Observaciones, y dado la similitud del término con el utilizado por SIGEN para identificar hallazgos no se utilizará en esta etapa del proyecto.

A continuación se presenta un resumen de los hallazgos identificados de acuerdo con la terminología ISO/IEC 27001:2013

Punto Modelo Política	CLÁUSULA / CATEGORÍA / CONTROL	ASPECTO A VERIFICAR	NO CONFORMID.			
			Mayor	Menor	Observ	OPM
4.	Evaluación y Tratamiento de Riesgos					
4.1	Evaluación de los riesgos de seguridad					
4.2	Tratamiento de riesgos de seguridad					
5.	Política de Seguridad de la Información					
5.1	Política de Seguridad de la Información					
6.	Organización					
6.1	Organización interna			1		
6.2	Dispositivos móviles y trabajo remoto			2		
7.	Recursos Humanos					
7.1	Antes del empleo			1		
7.2	Durante el empleo			1		
7.3	Cese del empleo o cambio de puesto de trabajo			1		
8.	Gestión de Activos					
8.1	Responsabilidad sobre los activos			1		
8.2	Clasificación de la información			1		
8.3	Gestión de Medios			2		
9.	Gestión de Accesos					
9.1	Requerimientos para el control de acceso			1		
9.2	Administración de accesos de usuarios		2	1		
9.3	Responsabilidades del usuario		1			
9.4	Control de acceso a Sistemas y Aplicaciones			3		
9.5	Control de acceso al sistema operativo			1		
10.	Criptografía					
10.1	Cumplimiento de requisitos legales		2	1		
11.	Física y Ambiental					
11.1	Áreas seguras			2		
11.2	Seguridad de los equipos			4		
12.	Seguridad en las operaciones					
12.1	Procedimientos y responsabilidades operativas			2		
12.2	Protección contra malware (código malicioso)					
12.3	Resguardo (back-up)			1		
12.4	Registro y monitoreo			2		
12.5	Control de Software Operacional					
12.6	Administración de vulnerabilidades técnicas			1		
12.7	Consideraciones sobre la auditoría de sistemas de información					
13.	Gestión de Comunicaciones					
13.1	Gestión de la red			1		
13.2	Transferencia de Información			1		
14.	Adquisición, Desarrollo y Mantenimiento de Sistemas					

14.1	Requerimientos de seguridad de los sistemas		1		
14.2	Seguridad en los sistemas de aplicación		3		
14.3	Seguridad de los archivos del sistema	1	2		
14.4	Seguridad de los procesos de desarrollo y soporte	2	3		
14.5	Gestión de vulnerabilidades técnicas		1		
15.	Relaciones con Proveedores				
15.1	Seguridad de la información en las relaciones con el proveedor				
15.2	Administración de prestación de servicios de proveedores				
16.	Gestión de Incidentes de Seguridad				
16.1	Informe de los eventos y debilidades de la seguridad	1	2		
16.2	Gestión de los incidentes y mejoras de la seguridad de la información	1	1		
17.	Gestión de la Continuidad				
17.1	Gestión de continuidad del organismo	1	3		
17.2	Redundancias		1		
18.	Cumplimiento				
18.1	Cumplimiento de requisitos legales	1	3		
18.2	Revisiones de la Política de Seguridad y la compatibilidad técnica	1	1		
18.3	Consideraciones de auditorías de sistemas				

"Figura 31: Listado resumen de hallazgos auditoría controles Disp. 1/2015 ONTI"

El resultado completo de la evaluación se encuentra en el ANEXO M "IT_6-2015-GNyPE-Revision-Politica-de-Seguridad-de-la-Informacion" siguiendo la terminología de SIGEN.

Un detalle de las observaciones identificadas en la implantación de los controles de la Disp. 1/2015, señalando el proyecto propuesto para su solución, se encuentra en el Anexo N "Hallazgos Pendientes Organismo"

5.3 Evaluación de la Madurez

Finalmente evaluaremos la madurez de la implementación del SGSI, a través de los dominios 4 a 10 de la norma ISO/IEC 27001:2013.

Esta estimación la realizaremos según la siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM):

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	**L0**	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las

			buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

"Figura 32: Tabla Modelo de Madurez CMM"

El resultado luego de analizar la organización es el siguiente cuadro:

Nro.	Capitulo	Nivel	Efect.	Comentarios
4	**La Organización y su Contexto**	**L3**	**80%**	
4.1	Entendiendo la Organización y su contexto	L3	90%	La organización ha identificado adecuadamente el contexto interno y externo con injerencia en el SGSI
4.2	Expectativas de las partes interesadas	L3	90%	La organización ha identificado adecuadamente las partes interesadas y sus requisitos involucradas en el SGSI
4.3	Alcance del SGSI	L3	90%	Se ha definido correctamente el alcance el SGSI
4.4	SGS Sistema de Gestión de la Seguridad de la información	L2	50%	Se ha iniciado el proceso de implantación, pero aún no está concluido
5	**Liderazgo**	**L4**	**93 %**	
5.1	Liderazgo y compromiso	L4	95%	La dirección ha impulsado y dado apoyo aprobando los proyectos asociados a la implementación del SGSI
5.2	Política de la Seguridad de la Información	L3	90%	Se ha aprobado y la nueva política de información. Falta su comunicación formal
5.3	Roles y Responsabilidades	L4	95%	Están definido los roles y sus responsabilidades dentro del nuevo SGSI, permitiendo su inclusión dentro de la evaluación de personal
6	**Planificación**	**L3**	**90%**	
6.1	Tratamiento de Riesgos y Oportunidades	L3	90%	Se ha realizado la evaluación y tratamientos de riesgos de acuerdo a la metodología propuesta en el presente trabajo y se han propuesto los proyectos correspondientes para su mitigación, sin embargo aún no se terminan de ejecutar estos últimos.
6.2	Planificación para consecución de objetivos	L3	90%	Están correctamente definidos los objetivos y planteados los proyectos para concretarlos, sin embargo aún no se

				terminan de ejecutar estos últimos
7	**Soporte**	**L3**	**75 %**	
7.1	Recursos	L4	95%	Los recursos destinados para el SCGI en los presupuestos 2020 y 2021 son los adecuados.
7.2	Competencia	L2	50 %	Aún es necesario mejorar las competencias de seguridad de la información de varios roles, lo cual se finalizará al momento de ejecutar 2 proyectos relacionados.
7.3	Concienciación	L2	50 %	El nivel de conciencia del personal en general se mantiene igual, se está a la espera de la ejecución del proyecto correspondiente.
7.4	Comunicación	L3	90%	Los procesos de comunicación están bien definidos, sin embargo aún no se termina de comunicar adecuadamente la nueva política.
7.5	Información documentada	L3	90%	Se ha generado la información documentada correspondiente al SGSI.
8	**Operación**	**L3**	**75 %**	
8.1	Control Operacional	L2	50 %	Se ha avanzado muy poco en la generación de la documentación requerida para los procesos, se está a la espera de la ejecución del proyecto correspondiente.
8.2	Análisis de riesgos de la Seguridad de la Información	L3	90%	Se ha realizado la evaluación y tratamientos de riesgo, pero es muy pronto aún para poder determinar el funcionamiento de este punto.
8.3	Tratamiento de riesgos de la Seguridad de la Información	L3	90%	Se ha realizado la evaluación y tratamientos de riesgo, pero es muy pronto aún para poder determinar el funcionamiento de este punto.
9	**Evaluación del desempeño**	**L3**	**92%**	
9.1	Seguimiento y medición	L3	90%	Se han identificado los elementos a monitorear, y se han propuestos los índices pero es demasiado pronto aún para poder determinar el funcionamiento de este punto
9.2	Auditorías Internas	L4	95 %	La unidad de auditoría interna del organismo realiza auditorias todos los años sobre diferentes aspectos de la SI. Este proceso está soportado por un sistema e información.
9.3	Informe de Revisión por la Dirección	L3	90%	Aún no hay ningún informe realizado sobre el tema, sin embargo es de esperar ya que aún no se termina de implementar el SGSI
10	**Mejora**	**L3**	**70%**	
10.1	No Conformidades y acciones correctivas	L3	90%	Se han generado una serie de proyectos que van a tratar prácticamente todas las

				no conformidades, para los pocos puntos pendientes se seguirá la normativa de SIGEN.
10.2	Mejora continua	L2	50%	Al no estar implementado el SGSI, no hay un proceso de mejora continua asociado.

"Figura 33: Aplicación del modelo CMM a los dominio de ISO/IEC 27001:2013"

Como podemos observar en este punto si se notan los avances realizados mediante el presente proyecto de implementación.

Conclusiones

Este trabaja ha servido para que el organismo, y en cierta medida yo también, comprenda la diferencia entre implementar una política de seguridad e implantar un Sistema de Gestión de la Seguridad. El sistema de Gestión de la Seguridad, a través del Plan Director, ha permitido que la organización explicite y tome acciones concretas para cumplir sus objetivos de seguridad, lo cual no se estaba realizando de forma eficaz mediante la implementación de una política de seguridad y sus controles.

La adaptación de varias herramientas y documentos planteados para los controles incluidos en ISO/IEC 27002, hacia los controles de la Disp. 1/2015 no fue difícil de realizar, sin embargo presentó una carga de trabajo extra sobre todo porque algunos apartados de esta última no son totalmente fieles o coherentes con los objetivos que persigue el capítulo de la norma.

Otro punto a destacar ha sido la realización del análisis de riesgos que ha dado un marco conceptual a los controles ya implementados, y ha validado la necesidad de avanzar con los controles faltantes. Para este punto se armó una metodología que tomó elementos de la utilizada en la materia SGSI y de Magerit para armar un procedimiento acorde a las necesidades del organismo y que se continúe utilizando en forma activa dentro del mismo.

Los resultados alcanzados en la implementación de los dominios de la ISO/IEC 27001:2013 son muy importantes, ya que es el punto de mayor retraso en el organismo. Si bien no hubo un avance de igual magnitud en la implementación de los controles faltantes de la Disp. 1/2015 ONTI, el nivel de cumplimiento al momento de finalizar los proyectos planteados será el deseado.

Cuando se finalicen los proyectos descriptos, se habrán cumplido con los siguientes objetivos planteados para el Plan Director:

1. Mejorar la seguridad en los servicios de información brindados por el organismo eliminado la brecha entre implementación y política. Implementar controles faltantes.
2. Actualizar los estándares de desarrollo para incluir metodología que contemple la seguridad en todo el proceso de desarrollo de aplicaciones.
3. Generar las normas y procedimientos faltantes en las clausulas de Desarrollo, Comunicaciones y Operaciones.
4. Generar un Plan de Continuidad de Negocios.
5. Cumplir con el marco legal de la ONTI el cual indica que se debe actualizar la política de seguridad acorde con la versión de la Disp. 1/2015.
6. Generar una cultura en Seguridad de la Información, mejorando la formación y concientización del personal del organismo en temas relativos a la misma.

Quedó pendiente un estudio más profundo de la normativa ISO 27002 para adaptar algunos controles que entiendo están mejor desarrollados que los incluidos dentro de la Disp. 1/2015 (Categoría 9.4; 14.4; 14.5 y 16.1).

Glosario

- **Análisis de riesgos:** Proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta la Organización
- **Activos de Información:** Información y recursos asociados, que tienen valor para la organización
- **Amenaza:** causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **APN (Administración Pública Nacional):** La Administración Pública Es el conjunto de organismos estatales que realizan las funciones administrativas del Estado argentino
- **Acción Correctiva:** Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable para evitar que vuelva a ocurrir
- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- **Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado con el fin de determinar el grado en el que se cumplen los criterios de auditoría.
- **Autenticación:** Asegurar que una característica declarada de una entidad es correcta.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, Recogen, gestionan, transmiten y destruyen
- **Disponibilidad:** Propiedad de que la información se accesible y utilizable por solicitud de una entidad autorizada.
- **Eficiencia:** Capacidad de disponer de alguien o de algo para conseguir un efecto determinado
- **Eficacia:** Grado en el cual se realizan las actividades planificadas y se logran los resultados planificados
- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

- **Gestión de incidentes de seguridad de la información:** Procesos para la detección, reporte, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de la información
- **Incidente de Seguridad de la Información:** Un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información documentada:** Información que requiere ser controlada y mantenida por una organización y el medio en el cual está contenida.
- **Impacto:** Es la evaluación del efecto o consecuencia de la materialización del riesgo. Generalmente, la implicación del riesgo se mide en aspectos económicos, legales imagen de la empresa, disminución de capacidad de respuesta y competitividad, interrupción de operaciones, entre otros.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **No conformidad:** Incumplimiento de un requisito. Puede ser no conformidad de los servicios, de los procesos o del Sistema de Gestión de Seguridad de la Información.
- **Objetivo de control:** Declaración que describe lo que se quiere lograr como resultado de la implementación de controles.
- **Organización:** Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus objetivos
- **Política:** Intenciones y dirección de una organización, como las expresa formalmente su alta dirección
- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan, que transforma elementos de entrada en elementos de salida
- **Requisito:** Necesidad o expectativa que está establecida, generalmente implícita u obligatoria.
- **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización
- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la Institución suministra a otra, como los externos, aquellos que la Institución suministra a clientes y usuarios
- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- **SIGEN (Sindicatura General de la Nación):** Órgano de control interno del Poder Ejecutivo de la república Argentina.

- **SGSI (Sistema de Gestión de Seguridad de la Información):** parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar operar hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Sistema de gestión:** Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.
- **Vulnerabilidad:** Debilidad de un activo o de un control que puede ser explotada por una o más amenazas

Bibliografía

Materiales asignatura del MISTIC, Sistemas de Gestión de la Seguridad:

- Análisis de riesgos (PID_00253143)
- Implantación de un sistema de gestión de la seguridad de la información (PID_00253140)
- Desarrollo de algunos objetivos de control del SGSI (PID_00253142)

Daniel Cruz Allende, Arsenio Tortajada Gallego, Antonio José Segovia Henares

Sistemas de Gestión de la Seguridad de la Información - MISTIC / MEI - UOC "Creación del SGSI"
http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/Creaci%C3%B3n+del+SGSI

[1] "POLITICA DE SEGURIDAD DE LA INFORMACION" - Decisión Administrativa 669/2004
https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-669-2004-102188/actualizacion [Último acceso: 15 de Agosto 2020]

[2] "POLITICA DE SEGURIDAD DE LA INFORMACION MODELO" - Disposición 1/2015 ONTI
https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-1-2015-242859/texto [Último acceso: 15 de Agosto 2020]

ISO/IEC 27000, Information Technology. Security Techniques. InformationSecurity Management Systems. Overview and Vocabulary

ISO/IEC 27001, Information Technology. Security Techniques. InformationSecurity Management Systems. Requirements

ISO/IEC 27005, Information Technology. Security Techniques. Informationsecurity risk Management

MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNPV8m_hDIU [Último acceso: 16 Octubre 2020]

El portal de ISO 27001 en Español. Gestión de Seguridad de la Información. http://www.iso27000.es/iso27000.html

NORMA ISO 27001 https://normaiso27001.es

Oficina Nacional de Tecnologías de la Información
https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/onti

Anexos

Anexo A – Análisis Diferencial ISO 27001_2013.doc
Anexo B – Análisis Diferencial ISO Disp1_2015.xlsx
Anexo C - Política de Seguridad de la Información.docx
Anexo D - Normas Auditoría Interna Gubernamental.pdf
Anexo E - Manual Control Interno Gubernamental.pdf
Anexo F - Descripción de Proyectos Auditoria SGSI.doc
Anexo G - Indicadores SGSI.docx
Anexo H - Reglamento funcionamiento CoTySIC.docx
Anexo I - SOA 27002_2013.xlsx
Anexo J - Inventario Activos de Información.xlsx
Anexo K - Análisis Amenazas.xlsx
Anexo L - Análisis Riesgo.xlsx
Anexo M - IT_6-2015-GNyPE-Revision-PSI.xlsx
Anexo N - Hallazgos Pendientes Organismo.xlsx