AGENCIA DE RECAUDACIÓN Y CONTROL ADUANERO
"2025 - AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA"

ANEXO

Número: IF-2025-01572785-AFIP-SGDADVCOAD#SDGPCI

CIUDAD DE BUENOS AIRES
Jueves 24 de Abril de 2025

Referencia: AGENCIA DE RECAUDACIÓN Y CONTROL ADUANERO. Estructura organizativa. S/Adecuación. ANEXO B01.

ANEXO B01

AGENCIA DE RECAUDACIÓN Y CONTROL ADUANERO

DIRECCIÓN DE AUDITORÍA INTERNA

RESPONSABILIDAD PRIMARIA

Asistir a la Dirección Ejecutiva en el análisis de las operaciones y la propuesta de mejoras para la efectividad de los procesos, evaluando el cumplimiento de la normativa legal y reglamentaria vigente, el sistema de control interno y la conducta de los agentes del Organismo, promoviendo la observancia de valores éticos y procurando la prevención de conductas irregulares.

ACCIONES

1. Intervenir en el análisis independiente, objetivo y sistemático sobre las operaciones del Organismo y la conducta de sus agentes.

2. Proponer los planes de auditoría en función de los riesgos identificados y proceder a la ejecución de los aprobados, asegurando el cumplimiento del cuerpo normativo externo e interno y la seguridad y confiabilidad de la información.

3. Identificar los principales riesgos inherentes a la gestión del Organismo, asistiendo a las dependencias para la adopción de medidas preventivas.

4. Coordinar la ejecución de los análisis y auditorías específicas que disponga la Dirección Ejecutiva y las decisiones que adopte el Comité de Control Interno.

5. Evaluar el ambiente de control interno del Organismo y aconsejar, en caso de corresponder, recomendaciones para su mejora y efectividad.

6. Informar a la Dirección Ejecutiva y al Comité de Control Interno sobre el estado de avance de la ejecución del Plan Anual de Auditoría y de los trabajos encomendados.

7. Entender en el diseño y ejecución de los programas que aseguren el mantenimiento de la integridad

de la conducta y de los valores éticos del personal del Organismo.

8. Coordinar sus actividades con las que realizan otras áreas del Organismo vinculadas a su competencia.

9. Representar al Organismo en materia de Ética Pública.

10. Actuar como enlace de integridad pública con la Oficina Anticorrupción para la promoción de estándares, el intercambio de buenas prácticas y la facilitación de la comunicación en el ámbito nacional e internacional.

11. Recepcionar, registrar y despachar la documentación que ingrese a la Dirección, realizar el adecuado suministro, mantenimiento y conservación de los bienes patrimoniales y recursos informáticos asignados, ejecutar las distintas tareas administrativas, atender los asuntos inherentes a los recursos humanos de la misma y administrar y comunicar al área pertinente los movimientos de los fondos de la caja chica asignada.

DEPARTAMENTO PLANIFICACIÓN CONTROL DE LEGALIDAD

ACCIÓN

Entender en la planificación, control y seguimiento de la ejecución del Plan Anual de Auditoría respecto de las intervenciones de carácter obligatorio, relativas a los procesos centrales, operativos y legales, a partir del análisis del sistema de control interno y la ponderación de los riesgos, promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Controlar el accionar de sus áreas dependientes asegurando el cumplimiento de los estándares y directivas establecidas por la SIGEN y demás instancias y/u organismos competentes, evaluando las respuestas de cumplimiento obligatorio y demás informes emitidos.

2. Supervisar la elaboración del Plan Anual de Auditoría y controlar su ejecución, participando en la definición de los procesos, los riesgos asociados y el análisis del control interno.

3. Aprobar los Programas de Auditoría propuestos por los demás Departamentos y sus modificaciones considerando el sistema de control interno y los riesgos involucrados y elevarlos para el conocimiento de la Unidad de Auditoría Interna.

4. Entender en la confección del mapa de riesgo organizacional y asegurar su actualización sobre la base del análisis de las modificaciones que se produzcan en el contexto en que el Organismo desarrolla sus actividades, y de la retroalimentación que surja de las observaciones de los informes de auditoría y del mapa de riesgos en materia de integridad y ética pública.

5. Controlar las intervenciones de carácter obligatorio vinculadas a los procesos de reconocimiento y consolidación de deuda pública.

6. Evaluar los proyectos de informes de auditoría y demás informes emitidos por las áreas que le dependen y ponerlos a consideración de la Unidad de Auditoría Interna.

7. Evaluar la calidad de los informes de auditoría emitidos por las áreas dependientes de la Unidad de Auditoría Interna y ponerlos a consideración de esta última.

8. Supervisar el análisis, de situaciones presuntamente anómalas o irregulares detectadas en las tareas

de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área competente.

9. Controlar las respuestas a los oficios y otros requerimientos jurídicos en los que se requiera la participación de la Unidad de Auditoría Interna.

10. Brindar asistencia técnica a las áreas dependientes de la Dirección de Auditoría Interna, así como intervenir en el dictado y actualización de la normativa interna, en materia de su competencia.

DIVISIÓN AUDITORÍA DE CUMPLIMIENTO LEGAL

ACCIÓN

Ejecutar el Plan Anual de Auditoría respecto de los procesos de reconocimiento y consolidación de deuda pública y las intervenciones de carácter obligatorio asignadas, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Ejecutar las auditorías relativas a los procesos de su competencia y efectuar el seguimiento de las observaciones y acciones correctivas, asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

2. Controlar el cumplimiento de las respuestas institucionales a brindar por la Dirección Ejecutiva, a organismos externos, en materia de procesos legales y operativos, en materia de gestión de recursos y tecnología de la información.

3. Proponer planes y procedimientos de trabajo para ejecutar las auditorías y controles asignados.

4. Efectuar el control del cumplimiento de los requerimientos de organismos externos y el seguimiento de las auditorias iniciadas por órganos externos de control, y comunicar al área competente los desvíos relevantes advertidos y las acciones institucionales adoptadas, generando la retroalimentación y optimización del sistema de control interno del Organismo.

5. Llevar un inventario actualizado de las deudas reconocidas en sede administrativa, en materia de su competencia.

6. Elaborar informes de auditoría y otros informes que sean solicitados y ponerlos a consideración del Departamento.

7. Elaborar los proyectos de respuesta a los oficios en los que se requiere la intervención de la Unidad de Auditoría Interna, elevándolos a consideración del Departamento.

8. Brindar asistencia técnica, en materia de su competencia, a las áreas dependientes de Unidad de Auditoría Interna.

9. Analizar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área competente.

DIVISIÓN RIESGOS, PLANIFICACIÓN Y CONTROL DE AUDITORÍAS

ACCIÓN

Intervenir en el proceso de planificación y coordinación de la elaboración del Plan Anual de Auditoría, a partir del análisis del sistema de control interno y la ponderación de los riesgos que afectan a los principales procesos del Organismo, brindando información tendiente a establecer prioridades que mejoren la planificación del Plan Anual de Auditoría, debiendo efectuar su control y seguimiento.

TAREAS

1. Identificar y evaluar los riesgos que puedan afectar al cumplimiento de los objetivos estratégicos del Organismo, confeccionando el mapa de riesgos, determinando la criticidad de los procesos así como las actividades y controles tendientes a mitigarlos.

2. Mantener actualizado el mapa de riesgo organizacional a partir del análisis de las modificaciones que se produzcan en el contexto en el que el Organismo desarrolla sus actividades y de la retroalimentación que surja de las observaciones de los informes de auditoría y del mapa de riesgos en materia de integridad y ética pública.

3. Elaborar el Plan Anual de Auditoría, junto con sus informes de ejecución, de conformidad con los lineamientos establecidos por la SIGEN.

4. Efectuar las actividades relacionadas con el inicio, programación y coordinación de las auditorías, estableciendo las fechas límite de ejecución de cada uno de los cargos de auditoría conforme al Plan Anual de Auditoría.

5. Verificar la ejecución de los cargos de auditoría según lo programado y elaborar los informes de retroalimentación que correspondan.

6. Monitorear la carga de horas asignadas al Plan Anual de Auditoría.

7. Emitir opinión respecto de las modificaciones propuestas al Plan Anual de Auditoría y de los cargos vigentes.

8. Controlar el registro de las observaciones pendientes de regularización que surgen de los informes, en conjunto con las demás áreas de la Unidad de Auditoría Interna.

9. Controlar la Ejecución del Plan Anual de Auditoría y mantener un registro actualizado que permita su seguimiento.

10. Analizar el cumplimiento de los estándares de calidad de los cargos en ejecución y/o archivados a requerimiento de la Unidad de Auditoría Interna.

11. Realizar el monitoreo y seguimiento del Sistema de Gestión de Calidad, en el ámbito de su competencia.

12. Elaborar los indicadores de gestión y realizar su seguimiento.

13. Recopilar y analizar la normativa vigente relacionada con el monitoreo, análisis y mitigación de riesgos.

14. Brindar asistencia técnica, en materia de su competencia, a las áreas dependientes de la Unidad de Auditoría Interna.

DEPARTAMENTO AUDITORÍA DE PROCESOS OPERATIVOS

ACCIÓN

Entender en el análisis y evaluación de las acciones vinculadas a procesos operativos en materia aduanera, impositiva y de los recursos de la seguridad social, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Colaborar en la elaboración del Plan Anual de Auditoría y participar en la definición de los procesos, los riesgos asociados y el análisis del control interno, en materia de su competencia.

2. Controlar, en la materia de su competencia, la ejecución del Plan Anual de Auditoría, por parte de sus unidades dependientes.

3. Planificar, dirigir y controlar el accionar de sus áreas dependientes, asegurando el cumplimiento de los estándares y directivas que en materia de auditoría interna sean establecidos por la SIGEN y demás instancias y/u organismos competentes, evaluando las respuestas de cumplimiento obligatorio y demás informes emitidos.

4. Proponer los programas de auditoría y sus modificaciones considerando el Sistema de Control Interno y los riesgos involucrados.

5. Evaluar los informes Unidad auditoría de los procesos de su competencia y ponerlos a consideración de la Unidad de Auditoría Interna.

6. Proponer a la Unidad de Auditoría Interna el tratamiento a otorgar a las observaciones pendientes de regularización, y efectuar su seguimiento, considerando la criticidad del riesgo involucrado.

7. Informar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento lo establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área competente.

8. Brindar asistencia técnica a las áreas dependientes de la Dirección de Auditoría Interna, así como intervenir en el dictado y actualización de la normativa interna, en materia de su competencia.

DIVISIÓN CONTRAVERIFICACIONES IMPOSITIVAS, ADUANERAS Y DE LOS RECURSOS DE LA SEGURIDAD SOCIAL

ACCIÓN

Ejecutar el Plan Anual de Auditoría respecto de la verificación y determinación de la razonabilidad de los procedimientos operativos aplicados en las tareas de fiscalización y control, en materia impositiva, aduanera y de los recursos de la seguridad social, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Ejecutar las contraverificaciones a procedimientos operativos en materia de impositiva y de los recursos de la seguridad social correspondientes a ciudadanos ya fiscalizados y/o a fiscalizaciones

que se encuentren en curso determinando la razonabilidad de lo actuado, y efectuar el seguimiento de las observaciones y acciones correctivas, asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

2. Ejecutar las contraverificaciones a procedimientos operativos en materia aduanera correspondientes a usuarios del servicio aduanero, responsables y/u operaciones ya fiscalizadas o controladas y/o las que se encuentren en curso, determinando la razonabilidad de lo actuado, y efectuar el seguimiento de las observaciones y acciones correctivas, asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

3. Evaluar la aplicación de la normativa e instructivos vigentes con relación a la verificación y fiscalización en materia aduanera, impositiva y de los recursos de la seguridad social, requiriendo, en caso de ser necesario, documentación a los ciudadanos y/o terceros en uso de las facultades de verificación y fiscalización previstas en la Ley N° 11.683, como también, a los operadores del comercio exterior en uso de las facultades de control, verificación y fiscalización previstas en el Código Aduanero.

4. Proponer planes y procedimientos de trabajo para ejecutar las contraverificaciones asignadas.

5. Elaborar informes de auditoría y otros informes que sean solicitados, y ponerlos a consideración del Departamento.

6. Brindar asistencia técnica, en materia de su competencia a las áreas dependientes de la Unidad de Auditoría Interna.

7. Analizar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento lo establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área competente.

DIVISIÓN AUDITORÍA OPERATIVA, IMPOSITIVA Y DE LOS RECURSOS DE LA SEGURIDAD SOCIAL

ACCIÓN

Ejecutar el Plan Anual de Auditoría respecto de los procesos operativos en materia impositiva y de los recursos de la seguridad social, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Ejecutar las auditorías relativas a los procesos operativos en materia de su competencia y efectuar el seguimiento de las observaciones y acciones correctivas, asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

2. Proponer planes y procedimientos de trabajo para ejecutar las auditorías asignadas.

3. Elaborar informes de auditoría y otros informes que sean solicitados, y ponerlos a consideración del Departamento.

4. Brindar asistencia técnica, en materia de su competencia, a las áreas dependientes de la Unidad de Auditoría Interna.

5. Analizar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría

que resultaren contrarias a los valores, principios básicos y pautas de comportamiento lo establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área competente.

DIVISIÓN AUDITORÍA LEGAL ADUANERA, IMPOSITIVA Y DE LOS RECURSOS DE LA SEGURIDAD SOCIAL

ACCIÓN

Ejecutar el Plan Anual de Auditoría respecto de los aspectos legales de los procesos en materia aduanera, impositiva y de los recursos de la seguridad social, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Ejecutar las auditorías relativas a los procesos operativos en materia de su competencia y efectuar el seguimiento de las observaciones y acciones correctivas, asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

2. Ejecutar las auditorías respecto de la gestión de juicios penales tributarios, en materia aduanera y demás procesos legales en materia de su competencia y realizar el seguimiento de las observaciones y acciones correctivas.

3. Proponer planes y procedimientos de trabajo para ejecutar las auditorías asignadas.

4. Elaborar informes de auditoría y otros informes que sean solicitados, y ponerlos a consideración del Departamento.

5. Brindar asistencia técnica, en materia de su competencia, a las áreas dependientes de la Unidad de Auditoría Interna.

6. Analizar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento lo establecido en el Código de Ética y demás normativa vigente, para su eventual evaluación por parte del área competente.

DIVISIÓN AUDITORÍA OPERATIVA ADUANERA

ACCIÓN

Ejecutar el Plan Anual de Auditoría respecto de los procesos operativos, en materia aduanera, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Ejecutar las auditorías relativas a los procesos operativos en materia aduanera y efectuar el seguimiento de las observaciones y acciones correctivas, asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

2. Proponer planes y procedimientos de trabajo para ejecutar las auditorías asignadas.

3. Elaborar informes de auditoría y otros informes que sean solicitados, y ponerlos a consideración del Departamento.

4. Brindar asistencia técnica, en materia de su competencia, a las áreas dependientes de la Unidad de Auditoría Interna.

5. Analizar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento lo establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área competente.

DEPARTAMENTO AUDITORÍA DE PROCESOS CENTRALES

ACCIÓN

Entender en el análisis y evaluación de las acciones vinculadas a los procesos centrales, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Colaborar en la elaboración del Plan Anual de Auditoría y participar en la definición de los procesos, los riesgos asociados y el análisis del control interno, en materia de su competencia.

2. Controlar, en la materia de su competencia, la ejecución del Plan Anual de Auditoría, por parte de sus unidades dependientes.

3. Planificar, dirigir y controlar el accionar de sus áreas dependientes, asegurando el cumplimiento de los estándares y directivas que en materia de auditoría interna sean establecidos por la SIGEN y demás instancias y/u organismos competentes, evaluando las respuestas de cumplimiento obligatorio y demás informes emitidos.

4. Proponer los programas de auditoría y sus modificaciones considerando el sistema de control interno y los riesgos involucrados.

5. Evaluar los informes de auditoría de los procesos de su competencia y ponerlos a consideración de la Unidad de Auditoría Interna.

6. Proponer a la Unidad de Auditoría Interna el tratamiento a otorgar a las observaciones pendientes de regularización, y efectuar su seguimiento, considerando la criticidad del riesgo involucrado.

7. Informar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento lo establecido en el Código de Ética y demás normativa vigente, para su eventual evaluación por parte del área competente.

8. Brindar asistencia técnica a las áreas dependientes de la Dirección de Auditoría Interna, así como intervenir en el dictado y actualización de la normativa interna, en materia de su competencia.

DIVISIÓN AUDITORÍA DE GESTIÓN DE RECURSOS

ACCIÓN

Ejecutar el Plan Anual de Auditoría respecto de los procesos de gestión y de procesos centrales de soporte en materia de recursos humanos y administrativo – financieros, así como los aspectos legales de los procesos centrales de soporte, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Ejecutar las auditorías relativas a los procesos en materia de su competencia y efectuar el seguimiento de las observaciones y acciones correctivas asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

2. Ejecutar las auditorías respecto de la gestión de juicios y demás procesos legales de soporte y realizar el seguimiento de las observaciones y acciones correctivas, asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

3. Proponer planes y procedimientos de trabajo para ejecutar las auditorías asignadas.

4. Elaborar informes de auditoría y otros informes que sean solicitados, y ponerlos a consideración del Departamento.

5. Brindar asistencia técnica, en materia de su competencia, a las áreas dependientes de la Unidad de Auditoría Interna.

6. Analizar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento lo establecido en el Código de Ética y demás normativa vigente, para su eventual evaluación por parte del área competente.

DIVISIÓN AUDITORÍA DE TECNOLOGÍA DE LA INFORMACIÓN

ACCIÓN

Ejecutar el Plan Anual de Auditoría respecto de los procesos de soporte en materia de tecnología de la información, evaluando el sistema de control interno y promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

TAREAS

1. Ejecutar las auditorías relativas a la tecnología de la información y efectuar el seguimiento de las observaciones y acciones correctivas, asegurando el cumplimiento de los estándares y directivas que sean establecidos por la SIGEN y demás instancias y/u organismos competentes.

2. Proponer modificaciones a los programas de auditoría asignados, así como evaluar los planes y procedimientos de trabajo para su ejecución.

3. Elaborar informes de auditoría y otros informes que sean solicitados y ponerlos a consideración del Departamento.

4. Brindar asistencia técnica, en materia de su competencia, a las áreas dependientes de la Unidad de

Auditoría Interna.

5. Analizar las situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento lo establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área competente.

DEPARTAMENTO ANÁLISIS Y TRÁMITE DE DENUNCIAS DE CONTENIDO ÉTICO

ACCIONES

Entender en el análisis de denuncias efectuadas contra el personal del Organismo relacionadas con el desempeño de sus funciones respecto de conductas que pudieran resultar contrarias a los valores, principios básicos y pautas de acuerdo con lo establecido en el Código de Ética y demás normativa vigente en la materia, promoviendo la observancia de las normas sobre ética y ejercicio de la función pública.

Entender en el cumplimiento de los principios generales y valores establecidos en la Política Institucional de Integridad y Ética Pública del Organismo.

TAREAS

1. Coordinar el análisis de las denuncias recibidas efectuadas contra el personal del Organismo relacionadas con el desempeño de sus funciones respecto de conductas que pudieran resultar contrarias a los valores, principios básicos y pautas de acuerdo con lo establecido en el Código de Ética y demás normativa vigente en la materia.

2. Controlar el trámite otorgado a las denuncias recibidas por el Canal Ético, las realizadas en las dependencias de la Dirección de Auditoría Interna, así como las remitidas por otras dependencias u organismos públicos, por presunto incumplimiento a los deberes de funcionarios y/o situaciones o conductas contrarias al Código de Ética y demás normativa vigente en la materia.

3. Supervisar el seguimiento de las denuncias recibidas.

4. Supervisar la evaluación de verosimilitud de las denuncias efectuadas contra los agentes del Organismo y terceras partes relacionadas, identificando conductas contrarias a los valores, principios básicos y pautas que deben orientar la conducta del personal de acuerdo con lo establecido en el Código de Ética y demás normativa vigente en la materia.

5. Controlar la carga de las denuncias recibidas a través del Canal Ético, como también su archivo.

6. Proponer la convocatoria del Comité de Integridad y Ética Pública cuando las denuncias recibidas tengan impacto de significativa relevancia institucional y/o económica.

7. Asistir al Comité de Integridad y Ética Pública para el cumplimiento de las tareas a su cargo, realizando las convocatorias a las reuniones, llevar adelante el orden del día, elaborar las minutas, las conclusiones y el tratamiento de los casos a reportar.

8. Supervisar el cumplimiento de las acciones adoptadas por el Comité.

9. Promover el cumplimiento de los valores, los principios básicos y las pautas de conducta por parte de los agentes del Organismo, contenidos en el Código de Ética y en las normas vigentes en la materia.

10. Intervenir y evaluar, a requerimiento de la Unidad de Auditoría Interna, situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resultaren contrarias a los valores, principios básicos y pautas de comportamiento de acuerdo con lo establecido en el Código de Ética y demás normativa vigente en la materia.

11. Proponer cursos de acción a seguir conforme a las hipótesis derivadas del análisis de los casos efectuados por las áreas dependiente dando intervención a las áreas con competencia, de corresponder.

12. Supervisar la elaboración del mapa de riesgos en materia de integridad y ética pública.

13. Prestar colaboración a otras unidades del Organismo en materia de integridad y ética pública, a requerimiento de la superioridad.

14. Participar en las acciones de difusión en materia de integridad y transparencia en la función pública.

15. Brindar asistencia técnica a las áreas dependientes de la Dirección de Auditoría Interna, así como intervenir en el dictado y actualización de la normativa interna, en materia de su competencia.

DIVISIÓN ASUNTOS DE INTEGRIDAD Y ÉTICA PÚBLICA

ACCIÓN

Ejecutar las acciones vinculadas al cumplimiento de los principios generales y valores establecidos en la Política Institucional de Integridad y Ética Pública del Organismo.

TAREAS

1. Confeccionar el mapa de riesgos en materia de integridad y ética pública.

2. Elaborar las normas en materia de integridad y ética, así como los procedimientos de actuación que colaboren al cumplimiento de los principios generales y valores establecidos en la Política Institucional de Integridad y Ética Pública del Organismo.

3. Elaborar informes referidos a denuncias recibidas tengan impacto de significativa relevancia institucional y/o económica a los efectos del análisis por parte del Departamento.

4. Realizar las convocatorias a las reuniones del Comité, indicadas por la Unidad de Auditoría Interna, llevar adelante el orden del día, elaborar las minutas, las conclusiones y el tratamiento de los casos a reportar.

5. Proyectar las normas en materia de integridad y ética, así como los procedimientos de actuación que colaboren al cumplimiento de los principios generales y valores establecidos en la Política Institucional de Integridad y Ética Pública del Organismo.

6. Efectuar el seguimiento del cumplimiento de las acciones adoptadas por el Comité de Integridad y Ética Pública.

7. Proponer cuestiones que ameriten acciones de difusión en materia de integridad y transparencia en la función pública.

8. Brindar asistencia técnica a las áreas dependientes de la Unidad de Auditoría Interna, así como a otras unidades del Organismo, en materia de su competencia.

9. Promover el cumplimiento de los valores, los principios básicos y las pautas de conducta por parte de los agentes del Organismo, contenidos en el Código de Ética y en las normas vigentes en la materia.

DIVISIÓN ANÁLISIS, TRÁMITE Y SEGUIMIENTO DE DENUNCIAS

ACCIÓN

Analizar las denuncias efectuadas contra el personal del Organismo relacionadas con el desempeño de sus funciones respecto de conductas que pudieran resultar contrarias a los valores, principios básicos y pautas de acuerdo con lo establecido en el Código de Ética y demás normativa vigente en la materia.

TAREAS

1. Administrar sistémicamente el módulo de denuncias recibidas a través del Canal Ético, así como también su archivo.

2. Tramitar las denuncias recibidas por el Canal Ético, las realizadas en las dependencias de la Dirección de Auditoría Interna, así como las remitidas por otras dependencias u organismos públicos, por presunto incumplimiento a los deberes de funcionarios y/o situaciones o conductas contrarias al Código de Ética y demás normativa vigente en la materia.

3. Analizar la verosimilitud de las denuncias efectuadas contra los agentes del Organismo y terceras partes relacionadas, identificando conductas contrarias a los valores, principios básicos y pautas que deben orientar la conducta del personal de acuerdo con lo establecido en el Código de Ética y demás normativa vigente en la materia.

4. Atender aquellas denuncias que constituyan o puedan constituir una represalia contra el denunciante.

5. Efectuar el seguimiento de las denuncias efectuadas contra el personal del Organismo relacionadas con el desempeño de sus funciones y que resulten contrarias a los valores, principios básicos y pautas que deben orientar su conducta de acuerdo con lo establecido en el Código de Ética y demás normativa vigente en la materia.

6. Elaborar Informes de seguimiento para ser sometidos a consideración del Departamento.

7. Elaborar informes de investigación y elevar al Departamento las propuestas de cursos de acción a seguir conforme a las hipótesis derivadas del análisis de los casos dando intervención a las áreas con competencia, de corresponder.

8. Brindar asistencia técnica, en materia de su competencia, a las áreas dependientes de la Unidad de Auditoría Interna.

DIRECCIÓN DE ESTUDIOS

RESPONSABILIDAD PRIMARIA

Coordinar la producción y el análisis de la información estadística tributaria del Organismo, así como producir informes sobre el comportamiento de las principales variables del sistema tributario.

ACCIONES

1. Coordinar el análisis del funcionamiento de la administración del sistema tributario en relación con los objetivos de la política fiscal.

2. Elaborar metodologías y aplicar técnicas estadísticas para el relevamiento de datos y la obtención, análisis e interpretación de la información.

3. Entender en el análisis e interpretación de la información estadística, evaluando el funcionamiento del sistema tributario y el comportamiento fiscal a través de la clasificación y categorización de los responsables y de indicadores que reflejen su conducta.

4. Estimar el rendimiento anual de los tributos que administra el Organismo y realizar los análisis cuantitativos ex post de la recaudación, considerando los factores que incidieron en la misma.

5. Controlar el análisis del impacto fiscal de las medidas e instrumentos de política económica.

6. Entender en la estimación de las metas de recaudación por dependencia y evaluar su cumplimiento.

7. Efectuar publicaciones de carácter general para la difusión del material estadístico y respecto de la evolución de la recaudación.

8. Intervenir, cuando le sea requerido, en proyectos de creación, modificación o actualización de normas tributarias e instrumentos de clasificación y categorización.

9. Coordinar el intercambio de información con organismos nacionales e internacionales en temas de su competencia.

DEPARTAMENTO ESTADÍSTICA

ACCIÓN

Elaborar la información vinculada al funcionamiento de la Repartición y al comportamiento de los responsables en el cumplimiento de sus obligaciones tributarias.

TAREAS

1. Elaborar la información para orientar la toma de decisiones en las funciones de aplicación, recaudación, fiscalización y administración de los tributos, para la investigación económico fiscal y para satisfacer requerimientos específicos.

2. Elaborar metodológicas y aplicar técnicas estadísticas para el relevamiento de datos, la obtención, análisis e interpretación de la información.

3. Coordinar los datos estadísticos a elaborar por las distintas dependencias, procurando su uniformidad y determinando la índole y periodicidad con que deben proporcionarlos.

4. Diseñar y elaborar publicaciones de carácter general para la difusión del material estadístico.

DEPARTAMENTO ESTUDIOS ECONÓMICOS

ACCIÓN

Analizar y evaluar la información estadística vinculada a la materia económico- tributaria realizando informes que contribuyan a la toma de decisiones de las dependencias del Organismo.

TAREAS

1. Analizar el funcionamiento de la administración del sistema tributario en relación con los objetivos de la política fiscal.

2. Proponer los sistemas de procesamiento de la información necesarios para la realización de los análisis y evaluaciones, en el ámbito de su competencia.

3. Analizar e interpretar la información estadística, evaluando el funcionamiento del sistema tributario y el comportamiento fiscal a través de la clasificación y categorización de los responsables y de indicadores que reflejen su conducta.

4. Realizar proyecciones y estimaciones de recaudación potencial y rendimiento anual referidos a los tributos a cargo del Organismo.

5. Analizar el impacto fiscal y los efectos económico-tributarios de la aplicación de los regímenes de promoción, desgravaciones y diferimientos de impuestos.

6. Estimar las metas de recaudación por dependencia y evaluar el incumplimiento.

7. Realizar los análisis cuantitativos ex-post de la recaudación tributaria, considerando los factores que incidieron en la misma.

8. Efectuar el seguimiento de la evolución técnico-formal de los tributos a cargo del Organismo.

9. Entender en los estudios y trabajos necesarios para la categorización del universo de ciudadanos y su actualización permanente.

10. Intervenir -cuando le sea requerido- en los estudios necesarios para la creación o modificación de formularios de declaración jurada y todo otro soporte de información, definiendo los requisitos de homogeneidad necesarios para que sea utilizable en agrupamientos o agregados.

11. Participar en los proyectos de creación y/o modificación de nuevas normas tributarias cuando le sean giradas en consulta y evaluar sus efectos económico-tributarios.

12. Asesorar en los trabajos encaminados al intercambio de información con otros organismos nacionales e internacionales cuando implicaren acuerdos referidos a los criterios adoptados para la clasificación de las actividades económicas u otros que impliquen su categorización.

DIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

RESPONSABILIDAD PRIMARIA

Supervisar y coordinar la definición y ejecución de los programas, políticas y controles de seguridad de la información, planificando y administrando los recursos necesarios para minimizar los riesgos sobre la confidencialidad, integridad y disponibilidad de los activos de información, de acuerdo a los objetivos del Organismo.

ACCIONES

1. Administrar los controles de seguridad sobre la información del Organismo, controlando la definición de las políticas, normativas, estándares y procedimientos de seguridad.

2. Proporcionar el apoyo y revisión para garantizar que los activos de información sean identificados y se minimice el riesgo de seguridad asociado.

3. Definir la implementación de controles, procesos y herramientas de apoyo que permitan asegurar el cumplimiento de las políticas de seguridad.

4. Presentar a la superioridad los riesgos de seguridad de la información a los que se expone el Organismo, para definir el tratamiento de los mismos.

5. Planificar el programa de gestión de riesgos de la información para identificar y tratar los riesgos que amenacen la información del Organismo.

6. Controlar el cumplimiento de las políticas de seguridad y brindar soporte en la definición de procesos de auditoría interna y autoevaluación de control para asegurar dicho cumplimiento.

7. Planificar y administrar los recursos asignados por el Organismo a tareas de seguridad de la información, gestionando el presupuesto anual y proponiendo las contrataciones de bienes y servicios asociados.

8. Analizar métricas de incidentes de seguridad de la información.

9. Colaborar en la investigación y reparación de incidentes de seguridad de la información u otras violaciones a las políticas de seguridad.

10. Coordinar proyectos de innovación tecnológica en materia de seguridad relacionados con los aspectos de infraestructura y gestión de identidades.

11. Interactuar con las áreas del Organismo o de organismos externos para el cumplimiento de las tareas.

12. Difundir normativas y políticas, organizando campañas de concientización al personal sobre la seguridad de la información, desarrollando una cultura de protección de los activos de información del Organismo.

13. Realizar el seguimiento y control de la evolución de los proyectos ejecutados, coordinando las acciones necesarias para su cumplimiento, en forma conjunta con las áreas involucradas.

14. Recepcionar, registrar y despachar la documentación que ingrese a la Dirección, realizar el adecuado suministro, mantenimiento y conservación de los bienes patrimoniales y recursos informáticos asignados, ejecutar las distintas tareas administrativas, atender los asuntos inherentes a los recursos humanos de la misma y administrar y comunicar al área pertinente los movimientos de los fondos de la caja chica asignada.

DEPARTAMENTO INGENIERÍA DE SEGURIDAD Y ACTIVOS

ACCIÓN

Coordinar y supervisar la definición e implementación de los controles de seguridad de la información en la infraestructura tecnológica, minimizando los riesgos informáticos y de acuerdo a los requerimientos del Organismo.

TAREAS

1. Diseñar los esquemas de seguridad para servidores, estaciones de trabajo y redes de comunicaciones, previniendo ataques o accesos no autorizados y garantizando el cumplimiento de las políticas definidas por el Organismo.

2. Diseñar los mecanismos que permitan aplicar y controlar los esquemas de seguridad en servidores, estaciones de trabajo y redes de comunicaciones.

3. Planificar y coordinar las acciones necesarias para mantener actualizada la infraestructura de seguridad del Organismo.

4. Controlar los proyectos de investigación y pruebas de concepto, definiendo la viabilidad de las nuevas tecnologías y arquitecturas de seguridad, según las necesidades del Organismo.

5. Participar en la especificación de servicios y/o equipamiento necesario para la provisión del servicio de seguridad de la información requerido por el Organismo.

6. Diseñar e implementar el Plan de Continuidad operativo sobre los controles de seguridad perimetrales y en la seguridad de los activos de información.

7. Proponer a la superioridad los cambios que optimicen los niveles de seguridad, efectuando las especificaciones necesarias, en materia de su competencia.

8. Coordinar los procesos y la implementación de las medidas de seguridad física, así como el control de accesos al centro de cómputos y a las infraestructuras críticas del Organismo.

9. Elaborar informes y estadísticas operativas para la Dirección, cumpliendo objetivos y métricas de gestión.

DIVISIÓN SEGURIDAD DE ACTIVOS

ACCIÓN

Implementar y configurar los esquemas de seguridad y acceso a los activos de información como servidores y estaciones de trabajo, definiendo acciones que tiendan a minimizar los riesgos.

TAREAS

1. Implementar los estándares de seguridad de la información que deben cumplir los servidores, estaciones de trabajo y cualquier otro dispositivo que se conecte a la red del Organismo.

2. Gestionar el proceso de actualización de seguridad sobre los activos de información y controlar su cumplimiento.

3. Definir e implementar facilidades tecnológicas que permitan gestionar una política de contraseñas que cumpla con los estándares de seguridad establecidos por el Organismo.

4. Definir e implementar las políticas de seguridad en directorios de acceso o dominios donde se deban integrar los distintos grupos de usuarios con distintos grupos de activos de información.

5. Colaborar en las tareas de identificación y clasificación de activos, de acuerdo a las políticas de seguridad de la información.

6. Implementar las políticas de administración y control de usuarios privilegiados.

7. Definir e implementar, sobre las estaciones de trabajo y servidores del Organismo, soluciones de protección contra código malicioso, prevención de intrusiones y cualquier otra herramienta de seguridad tendiente a minimizar los riesgos en los activos de información.

DIVISIÓN SEGURIDAD PERIMETRAL

ACCIÓN

Efectuar la definición e implementación de los esquemas de seguridad y acceso a la red de telecomunicaciones, estableciendo acciones que tiendan a minimizar los riesgos.

TAREAS

1. Definir e implementar los dispositivos que protegen a la red de comunicaciones del Organismo.

2. Definir e implementar los dispositivos y software relacionados con la detección y mitigación en tiempo real de ataques y/o intentos de acceso no autorizado a las redes y servidores del Organismo.

3. Definir, implementar y configurar los dispositivos de seguridad perimetrales que protegen la infraestructura tecnológica y permiten accesos seguros y conexiones encriptadas (VPN).

4. Definir, implementar y configurar los dispositivos relacionados con la detección y mitigación de ataques de denegación de servicio de la infraestructura tecnológica.

5. Definir e implementar los dispositivos perimetrales para favorecer el control de cumplimiento de las políticas de protección de datos.

6. Colaborar con las pruebas de concepto sobre nuevas tecnologías de hardware y/o software inherente a proteger la seguridad perimetral.

7. Mantener actualizada, en términos de tecnología, la infraestructura de seguridad, analizando nuevas soluciones que cumplan con los estándares tecnológicos.

DEPARTAMENTO ARQUITECTURA DE SEGURIDAD DE APLICACIONES Y DATOS

ACCIONES

Supervisar y coordinar la definición, implementación y comunicación de los estándares, metodologías y medios tecnológicos de seguridad para el desarrollo de software y permisos de acceso a los recursos informáticos del Organismo.

Desarrollar proyectos de innovación tecnológica en materia de seguridad relacionados con los aspectos de infraestructura y gestión de identidades que involucren desde la capa de aplicación hasta la capa de transporte.

TAREAS

1. Coordinar el diseño e implementación de los medios tecnológicos necesarios para el control de acceso a los recursos informáticos del Organismo.

2. Entender en la definición de esquemas de seguridad, así como herramientas y metodologías de desarrollo, de las aplicaciones que permitan maximizar los estándares de seguridad de la información del Organismo.

3. Promover acciones tendientes al mejoramiento de la seguridad en la arquitectura de los sistemas y aplicaciones implementadas en el Organismo.

4. Planificar las estrategias y acciones en torno a la arquitectura y controles de seguridad de bases de datos en el marco de gestión de la seguridad de la información del Organismo.

5. Diseñar e implementar la infraestructura tecnológica de las Autoridades Certificantes de la Organización.

6. Supervisar el análisis de las nuevas aplicaciones o modificaciones a aplicaciones existentes en los aspectos relacionados a los lineamientos de la normativa establecida en la materia, realizando las recomendaciones pertinentes.

7. Definir e implementar los sistemas e infraestructura que implementan las facilidades de gestión de identidades a través de autoridades certificantes y mecanismos de autorización de acceso a los sistemas.

8. Proponer a la superioridad los cambios que optimicen los niveles de seguridad en los controles de acceso a los recursos informáticos del Organismo.

9. Diseñar e implementar el Plan de Continuidad operativo en lo que se refiere a la gestión de identidades y desarrollo seguro.

10. Administrar los medios tecnológicos, para controlar el cumplimiento de las políticas de protección de datos.

11. Elaborar informes y estadísticas operativas para la Dirección, cumpliendo objetivos y métricas de gestión.

DIVISIÓN ARQUITECTURA DE SEGURIDAD

ACCIONES

Entender en el análisis de vulnerabilidades, diseño de estrategias y definición de acciones en torno a la arquitectura y la gestión de la seguridad de bases de datos en el marco de de la seguridad de la información del Organismo.

Definir la arquitectura de seguridad de los sistemas, estándares tecnológicos y metodologías aplicables al ciclo de vida e implementación de las aplicaciones.

TAREAS

1. Definir las políticas de seguridad y controles de acceso a bases de datos, así como aquellas correspondientes a la asignación de roles y perfiles.

2. Relevar la infraestructura de los repositorios de datos, diagrama general de conexiones y puntos de mejora.

3. Asesorar a las áreas del Organismo en la clasificación de los datos almacenados en los repositorios de información, de acuerdo a la criticidad y a la política de clasificación del Organismo.

4. Implementar y gestionar herramientas, políticas y procesos, que garanticen una correcta aplicación de las medidas de seguridad, para la protección de los repositorios de datos.

5. Definir la política de depuración de datos, teniendo en cuenta su relevancia, requerimientos legales de guarda y ciclo de vida.

6. Establecer los procesos de enmascaramiento y encriptación de datos.

7. Asegurar la correcta implementación de técnicas de cifrado de conexiones de bases de datos.

8. Diseñar y definir la estrategia, gestión y control de acceso a datos en reposo, limitados en el tiempo, según el principio de mínimos privilegios.

9. Homologar canales de uso ocasional para la transmisión interna de información extraída de las bases de datos de producción y definir su procedimiento.

10. Implementar chequeos automáticos en busca de abuso de privilegios o extracciones abusivas de datos en los repositorios.

11. Participar en la definición de las herramientas y metodologías de desarrollo de las aplicaciones, garantizando los estándares de seguridad del Organismo.

12. Investigar y proponer mejoras a los procesos de control de cambios y actualizaciones, así como a los estándares de desarrollo de aplicaciones utilizados en el Organismo, priorizando la seguridad de la información.

13. Proponer tecnologías de encriptación y controles por parte de las aplicaciones, tendientes a salvaguardar los activos en función a su clasificación.

14. Investigar nuevas tecnologías que permitan robustecer la arquitectura de la seguridad de las aplicaciones del Organismo, efectuando pruebas de concepto y determinando su viabilidad.

15. Investigar y proponer mejoras a los procesos de control de cambios y actualizaciones utilizados en el Organismo, priorizando la seguridad de la información.

16. Participar en la definición de la infraestructura informática, proponiendo la implementación de controles de seguridad por capas a nivel aplicación, para proteger los activos del Organismo.

17. Analizar las nuevas aplicaciones o modificaciones a aplicaciones existentes en los aspectos relacionados a los lineamientos de la normativa establecida en la materia, realizando las recomendaciones pertinentes.

DIVISIÓN GESTIÓN DE IDENTIDADES Y ACCESOS

ACCIÓN

Diseñar los medios tecnológicos para el acceso a los recursos informáticos del Organismo, controlando y monitoreando su implementación.

TAREAS

1. Diseñar, controlar y monitorear los sistemas e infraestructura que implementan las facilidades de Single Sign-On (SSO) interno y externo a la Organización.

2. Diseñar, controlar y monitorear los sistemas y aplicaciones que permitan automatizar, administrar y controlar la operación de otorgamiento de accesos lógicos a las aplicaciones internas del Organismo, así como la asignación de mecanismos multifactor de autenticación y la administración de reglas de acceso a las aplicaciones.

3. Coordinar y supervisar la gestión de la infraestructura tecnológica de las Autoridades Certificantes Internas del Organismo.

4. Diseñar, controlar y monitorear modelos y tecnologías referentes a mecanismos de autenticación, accesos a la información, web services y todo esquema donde se requiera identificación de usuarios.

5. Efectuar revisiones periódicas de los accesos y métodos de identificación otorgados.

DEPARTAMENTO GOBIERNO, RIESGOS Y CUMPLIMIENTO

ACCIÓN

Definir la normativa que resguarde la integridad, confidencialidad y disponibilidad de la información del Organismo, así como la política de gestión de riesgos, supervisando el cumplimiento de regulaciones y controles internos, y generando los mecanismos de gestión de la seguridad de la información.

TAREAS

1. Diseñar el programa de seguridad de la información de la del Organismo, basándose en los marcos regulatorios, legales, estándares de la industria y mejores prácticas.

2. Determinar las políticas, estándares y procedimientos que dan marco a la gestión de la seguridad de la información del Organismo.

3. Definir el plan de comunicación al personal del Organismo acerca de los temas de competencia de la Dirección de Seguridad de la Información.

4. Definir el programa de concientización en seguridad de la información, generando una cultura de protección de los activos de información del Organismo.

5. Coordinar la elaboración de respuestas a las auditorías internas y externas y a los oficios judiciales y sumarios administrativos de competencia de la Dirección, asegurando el cumplimiento de los estándares definidos.

6. Definir e implementar el esquema de revisión, actualización y aprobación de los procesos de seguridad de la información.

7. Definir el Plan de Continuidad del Negocio en materia de Seguridad de la Información en conjunto con las áreas competentes, analizando los riesgos asociados y documentando los procesos y procedimientos requeridos.

8. Definir la metodología y estrategia de gestión de riesgos de seguridad de la información que mejor se adapte a las necesidades del Organismo, conforme la normativa y las mejores prácticas existentes en la materia.

9. Definir y mantener los reportes del estado de riesgos tecnológicos asociados a la seguridad de la información del Organismo.

10. Definir el Plan de Gestión de Cumplimiento que incluya los objetivos y metas anuales de la Dirección de Seguridad de la Información y la participación de sus áreas dependientes.

11. Asistir a la Dirección en la redacción y revisión de acuerdos, actas y convenios a suscribir con terceros y/u otros organismos, en materia de Seguridad de la Información.

12. Elaborar informes y estadísticas operativas para la Dirección, cumpliendo objetivos y métricas de gestión.

DIVISIÓN CUMPLIMIENTO

ACCIÓN

Definir e implementar el marco de control, métricas, indicadores y reportes del programa de seguridad; así como supervisar el cumplimiento de los procesos y procedimientos del sistema de seguridad de la información, conforme la normativa vigente y estándares tecnológicos.

TAREAS

1. Verificar la existencia e implementación de procedimientos operativos documentados de las áreas dependientes de la Dirección.

2. Definir, en conjunto con las áreas competentes de la Dirección, los indicadores necesarios para medir el grado de cumplimiento de los procedimientos internos.

3. Colaborar en la definición del Plan de Gestión de Cumplimiento que incluya los objetivos y metas anuales de la Dirección de Seguridad de la Información y la participación de sus áreas dependientes.

4. Supervisar el cumplimiento de la normativa de seguridad de la información, proponiendo mecanismos de control en aquellos procesos donde resulten insuficientes.

5. Promover la mejora continua de los procesos de control de la seguridad de la información, en el ámbito del Organismo.

6. Definir métricas, indicadores y reportes sobre el cumplimiento del programa de seguridad de la información.

7. Realizar el seguimiento periódico del Plan de Gestión de Cumplimiento, interactuando con las áreas de la Dirección y elaborando los informes de gestión pertinentes.

8. Administrar la elaboración de respuestas a las auditorías internas y externas de la Dirección e incorporar las acciones de mejora al Plan de Gestión de Cumplimiento.

9. Colaborar en la elaboración de respuestas, que deba brindar la Dirección, ante solicitudes de información de organismos locales y/o internacionales, así como de oficios judiciales y sumarios administrativos.

DIVISIÓN GESTIÓN DE RIESGOS

ACCIÓN

Identificar, analizar y evaluar los riesgos relacionados a la seguridad de la información y la

infraestructura del Organismo, poniendo a disposición los datos relevantes para gestionar los niveles de riesgo aceptables, de acuerdo a los requerimientos del Organismo.

TAREAS

1. Evaluar e implementar la metodología y estrategia de gestión de riesgos de seguridad de la información que mejor se adapte a las necesidades del Organismo, conforme la normativa vigente y las mejores prácticas existentes.

2. Determinar los niveles aceptables de riesgo, conjuntamente con las áreas competentes del Organismo.

3. Establecer mecanismos que permitan una gestión de riesgos adecuada a los objetivos estratégicos del Organismo, promoviendo la mejora continua de metodologías y estrategias.

4. Relevar, en forma continua y en conjunto con las áreas involucradas, los riesgos de seguridad de la información.

5. Establecer los procesos que permitan catalogar los potenciales de las amenazas y vulnerabilidades que enfrente el Organismo.

6. Definir los mecanismos para clasificar los activos de información del Organismo, de acuerdo a parámetros de confidencialidad, integridad y disponibilidad.

7. Desarrollar e implementar los canales de comunicación para definir el tratamiento de riesgos, gestión de excepciones y verificación de avance de los planes de remediación.

8. Participar en el Ciclo de Desarrollo de Software del Organismo, analizando los riesgos en las distintas etapas y colaborando con los procesos de gestión de la demanda.

9. Implementar, mantener y gestionar el sistema informático integrado de gobierno, riesgos y cumplimiento.

10. Analizar los riesgos de seguridad de la información en los procesos de intercambio de datos entre el Organismo y entidades externas o proveedores de servicios informáticos, garantizando que las conexiones o servicios entre las partes cumplan con el nivel de seguridad de la información aceptable para el Organismo.

11. Implementar y documentar el Plan de Continuidad del Negocio, en conjunto con las áreas competentes, incluyendo los procesos, procedimientos y sistemas requeridos y basándose en buenas prácticas y estándares tecnológicos.

DIVISIÓN POLÍTICAS Y PROGRAMAS

ACCIÓN

Definir las políticas que resguarden la integridad, confidencialidad y disponibilidad de la información del Organismo, acompañando las necesidades del Organismo y conforme la normativa y mejores prácticas existentes en la materia.

TAREAS

1. Definir la política de seguridad de la información, conjuntamente con otras normas, políticas y procedimientos accesorios.

2. Implementar y promover la mejora continua del programa de formación y concientizaciónen seguridad de la información, generando una cultura de protección de la información del Organismo.

3. Diseñar y proponer el programa de seguridad y su plan de comunicación al personal del Organismo.

4. Definir las políticas y procedimientos que establezcan las medidas de protección de los activos de información, jerarquizándolas por la criticidad y clasificación establecidas por las áreas definidoras del Organismo.

5. Evaluar actualizaciones a la normativa en seguridad de la información, de acuerdo a nuevos estándares tecnológicos, legislación vigente y/o necesidades del Organismo.

6. Redactar, revisar y proponer mejoras en acuerdos, actas, contratos y convenios a suscribir con terceros u otros organismos, en materia de Seguridad de la Información.

7. Brindar asistencia, a las áreas dependientes de la Dirección, en la definición, revisión y actualización de políticas y procedimientos, siguiendo las buenas prácticas y estándares tecnológicos.

DEPARTAMENTO MONITOREO Y EVALUACIÓN DE SEGURIDAD

ACCIÓN

Definir e implementar las herramientas y procesos necesarios para la detección continua e identificación de posibles ataques, explotación de vulnerabilidades y demás incidentes contra la red, equipos, sistemas y bases de datos del Organismo.

TAREAS

1. Gestionar la detección y análisis de amenazas, vulnerabilidades e incidentes de seguridad de la información.

2. Evaluar conductas riesgosas ante posibles casos de fraude digital y ciberdelincuencia, originados por ciudadanos y/o agentes del Organismo, estableciendo mecanismos de prevención.

3. Mantener actualizada la base de datos de incidentes de seguridad informática.

4. Proporcionar alertas y notificaciones de amenazas, así como informes de incidentes de seguridad, a las áreas competentes del Organismo, minimizando los plazos de comunicación.

5. Analizar la información provista por los activos informáticos del Organismo para identificar, rastrear, predecir y proveer a las áreas operativas la información necesaria para contrarrestar las intenciones y actividades de los atacantes, ofreciendo cursos de acción en base al contexto del Organismo que mejoren la toma de decisiones.

6. Identificar los vectores de ataque de seguridad para el tratamiento y clasificación de los incidentes, mejorando la postura de seguridad del Organismo.

7. Constituir el equipo de respuesta a incidentes de seguridad (SIRT); así como coordinar, en conjunto con la Dirección, la confección y ejecución de los planes de acción que se definan.

8. Elaborar procesos de monitoreo (SOC) que estén alineados con estándares de seguridad aceptados por la industria y coordinar un grupo de trabajo físico y virtual para cubrir el monitoreo 24/7.

9. Diseñar e implementar las herramientas y procesos que permitan la correlación de registros de seguridad, sistemas, aplicaciones, redes y servidores, de manera consistente.

10. Construir el mapa o panel de seguridad de aplicaciones, infraestructura y fuentes de información, a partir de los incidentes detectados, así como el descubrimiento de sus vulnerabilidades, brindando información consolidada a la Dirección.

11. Desarrollar capacidades forenses para poder reconstruir la serie de eventos ocurridos durante un incidente y asesorar a otras dependencias del Organismo en casos de necesidad de peritajes informáticos.

12. Brindar la información necesaria que le permita a la Dirección relacionar los temas técnico-operativos con elementos críticos del negocio.

13. Implementar mecanismos que permitan reportar vulnerabilidades o incidentes de seguridad por parte de los ciudadanos y por los usuarios internos al Organismo.

14. Colaborar con la concientización del personal del Organismo, sobre la importancia de reportar en tiempo y forma los incidentes de seguridad.

15. Asesorar a la Dirección en la interacción con otros Organismos nacionales de ciberseguridad o respuesta ante incidentes, en el marco de los lineamientos y acuerdos de cooperación suscriptos por el Organismo.

16. Colaborar con otros organismos especializados en la lucha contra el fraude digital, forensia digital y ciberdelincuencia, coordinando las medidas necesarias para la prevención y tratamiento de los casos.

17. Diseñar e implementar el Plan de Continuidad operativo en lo que se refiere al monitoreo de seguridad, análisis de incidentes y vulnerabilidades de seguridad.

18. Elaborar informes y estadísticas operativas, cumpliendo objetivos y métricas de gestión.

DIVISIÓN DETECCIÓN Y ANÁLISIS DE INCIDENTES

ACCIÓN

Definir e implementar las herramientas y procesos que permitan detectar y reaccionar ante incidentes de seguridad en los sistemas de información, excepto casos de fraude digital, minimizando los tiempos de respuesta, identificando las causas y colaborando con otras áreas del Organismo para la gestión de medidas que permitan minimizar el impacto de las amenazas.

TAREAS

1. Coordinar los procesos de detección y análisis de incidentes en seguridad de la información, estableciendo medidas de respuesta y proponiendo mejoras a los sistemas.

2. Supervisar el monitoreo de la información generada por los dispositivos que componen la infraestructura de seguridad, telecomunicaciones, estaciones de trabajo y sistemas del Organismo, así como de la infraestructura tecnológica.

3. Entender en los alertas sobre eventos, ataques y/o amenazas de seguridad que puedan afectar los activos del Organismo.

4. Comunicar amenazas, en materia de su competencia, a las dependencias del Organismo.

5. Asistir en materia de políticas y procedimientos sobre gestión de incidentes.

6. Realizar el relevamiento de los sistemas y la solicitud de logs o pistas de auditoría para que sean incorporados a la herramienta centralizada de logs.

7. Identificar posibles eventos de seguridad, en conjunto con las áreas operativas.

8. Desarrollar y ejecutar pruebas para medir la capacidad de respuesta ante incidentes, determinando la efectividad y capacidad ante un incidente de seguridad, documentando los resultados.

9. Colaborar en la definición de medidas preventivas para favorecer el cumplimiento de la política de seguridad vigente.

10. Obtener mejores prácticas y casos, para implementar la ciberinteligencia de amenazas como parte de la estrategia de seguridad de la información del Organismo.

DIVISIÓN PREVENCIÓN DE FRAUDE DIGITAL

ACCIONES

Detectar y analizar posibles casos de fraude digital y ciberdelincuencia, originados por ciudadanos y/o agentes del Organismo, estableciendo mecanismos de prevención, minimizando el riesgo de ocurrencia.

Entender en la obtención y análisis de evidencia digital.

TAREAS

1. Analizar conductas riesgosas y accionar ante posibles modalidades de fraude digital.

2. Evaluar riesgos de fraude digital y conductas irregulares de ciudadanos y/o agentes del Organismo en los procesos de negocio, identificando debilidades en los controles y estableciendo indicadores de rendimiento.

3. Analizar las aplicaciones de negocio, junto con las áreas competentes, detectando comportamientos anómalos.

4. Investigar eventos relacionados con fraude informático, identificando acciones que puedan llevar a cabo los agentes del Organismo o ciudadanos que realizan actividades anómalas, emitiendo informes y recomendaciones.

5. Diseñar planes de capacitación y comunicación sobre prevención, detección y lucha contra el fraude digital y obtención de evidencia digital.

6. Establecer canales de comunicación y mecanismos de denuncia para que los ciudadanos puedan alertar sobre posibles casos de fraude digital y ciberdelitos.

7. Proponer acciones correctivas para el daño provocado por el fraude y la conducta irregular, disminuyendo la probabilidad de ocurrencia.

8. Impulsar mecanismos para la definición y detección de patrones de comportamiento que puedan

derivar en un fraude informático, utilizando herramientas de explotación de datos e inteligencia artificial.

9. Brindar asistencia a las áreas del Organismo que lo requieran, en materia de su competencia.

10. Investigar fuentes abiertas, canales IRC, redes sociales, etc, que permitan identificar potenciales indicadores de fraude.

11. Analizar las tendencias y patrones en el uso de tecnologías proponiendo las modificaciones necesarias a los sistemas para prevenir y combatir el fraude digital y los ciberdelitos.

12. Elaborar los procedimientos relacionados con la recopilación, preservación, análisis y desintervención de evidencia digital, acorde los estándares establecidos.

13. Realizar la obtención, preservación y/o análisis de evidencia digital cuando un incidente de seguridad así lo requiera.

14. Monitorear en forma continua los datos, identificando posibles fraudes de componentes internos y externos.

DIVISIÓN ANÁLISIS DE VULNERABILIDADES

ACCIÓN

Supervisar el análisis y evaluación de las vulnerabilidades y amenazas en materia de seguridad de la infraestructura, redes, aplicaciones y servicios del Organismo, en cumplimiento con las políticas de seguridad de la información, gestionando su tratamiento de acuerdo a su prioridad y la criticidad de los sistemas.

TAREAS

1. Coordinar el análisis y gestión de las vulnerabilidades y amenazas relacionadas con la seguridad de la infraestructura, así como de las aplicaciones y servicios del Organismo.

2. Emplear técnicas y software de escaneo de vulnerabilidades facilitando la interoperabilidad entre las herramientas automatizadas mediante el uso de estándares.

3. Supervisar la configuración de los controles implementados en los dispositivos de seguridad informática, así como la efectividad de las configuraciones de seguridad de los dispositivos que se conecten a la red del Organismo.

4. Mantener actualizado un plan para la gestión de vulnerabilidades.

5. Definir la metodología de análisis de vulnerabilidades y proponer las herramientas para su implementación.

6. Definir prioridades para el análisis, gestión y tratamiento de vulnerabilidades, de acuerdo a la criticidad de los sistemas.

7. Elaborar informes dirigidos a las áreas de negocio, en materia de vulnerabilidades detectadas en los sistemas y ponerlos a disposición para su priorización y remediación.

8. Coordinar la ejecución periódica de ejercicios de intrusión para verificar las capacidades de ataque y detección, promoviendo la mejora continua de los procesos de seguridad.

9. Impulsar la práctica de trabajo DevSecOps, integrando las pruebas de seguridad en cada etapa del proceso de desarrollo de software.

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2025.04.24 12:49:48 -03'00'

SESANA, VICTORIA
Jefa de Sección
Sección Gestión de Documentación de Autoridades Superiores (DI GEDO)
Agencia de Recaudación y Control Aduanero

Digitally signed by GDE AFIP
DN: cn=GDE AFIP, c=AR, o=ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS, ou=SUBDIRECCION GENERAL DE COORDINACION TECNICO INSTITUCIONAL, serialNumber=CUIT 33693450239
Date: 2025.04.24 12:49:50 -03'00'