AUDITORIA GENERAL
DE LA CIUDAD DE BUENOS AIRES

Informe Final de Auditoría

Con Informe Ejecutivo

Proyecto Nº 10.20.04

ASI SEGURIDAD INFORMÁTICA

Auditoría de Relevamiento

Período 2019

Buenos Aires, Julio 2021

AUDITORÍA GENERAL DE LA CIUDAD DE BUENOS AIRES

Jean Jaures 220 – Ciudad Autónoma de Buenos Aires

PRESIDENTA

Dra. Mariana Inés GAGLIARDI

AUDITORES GENERALES

Dr. Juan José CALANDRI

Cdra. Mariela Giselle COLETTA

Dr. Pablo CLUSELLAS

Lic. María Raquel HERRERO

Dr. Daniel Agustín PRESTI

Dr. Lisandro Mariano TESZKIEWICZ

Nombre del Proyecto	ASI Seguridad Informática.
Número de proyecto	10.20.04
Organismo Auditado	Agencia de Sistemas de Información.
Tipo de Auditoría	Relevamiento.
Período bajo examen	2019
Jurisdic./ Programa / Inciso	Jurisdicción 21 - Jefatura de Gabinete - Unidad ejecutora 8056 - Agencia Sistemas de Información.
Supervisor	Lic. Hernán García
Objeto	Sistemas de la Dirección de Seguridad Informática
Objetivo	Relevar los sistemas utilizados para la gestión de seguridad informática.
Alcance	Analizar la infraestructura de seguridad, la gestión de la misma y la prevención de los incidentes.

Inicio de las tareas Julio 2020.

FECHA APROBACIÓN DEL INFORME: 28 DE JULIO DE 2021

APROBADO POR: UNANIMIDAD

RESOLUCIÓN AGC Nº: 196/21

INFORME EJECUTIVO

Lugar y fecha de emisión	Ciudad Autónoma de Buenos Aires, Julio 2021.
Código de Proyecto	10.20.04
Denominación del Proyecto	ASI Seguridad Informática.
Tipo de Auditoría	Relevamiento.
Dirección General	Dirección General de Seguridad Informática.
Período bajo examen	2019
Objeto de la Auditoría	Sistemas de la Dirección de Seguridad Informática.
Objetivo de la Auditoría	Relevar los sistemas utilizados para la gestión de seguridad informática.
Alcance	Analizar la infraestructura de seguridad, la gestión de la misma y la prevención de los incidentes.
Limitaciones al Alcance	La limitación en la circulación establecida por el GCABA durante la cuarentena impidió la ejecución de las pruebas sustantivas en los centros de datos de la Agencia de Sistemas de Información.
Debilidades relevantes	<u>Falta de independencia de la Dirección de Seguridad Informática</u> Para garantizar la seguridad de los sistemas informáticos deben establecerse lineamientos y controles para la tecnología en todos los niveles del organismo. La dependencia jerárquica y funcional de la Dirección de Seguridad Informática con la Dirección Ejecutiva de la Agencia de Sistemas de Información, debilita el ambiente de control interno.

	Controles de seguridad limitados en los sistemas no gestionados por ASInf ASInf no gestiona la totalidad de los sistemas utilizados por el GCABA. Existen otros centros de procesamiento y almacenamiento dependientes del Poder Ejecutivo que no se encuentran bajo la órbita de control de ASInf. La Agencia de Sistemas de información, como órgano de control, debe gestionar y asegurar el cumplimiento del Marco Normativo de Tecnología de Información vigente para la totalidad de los sistemas utilizados por el GCABA. Alcance limitado de la seguridad en los sistemas no gestionados por ASInf La falta de administración en los sistemas o el control parcial, no permite la gestión de la identidad y la cuenta de usuario. Por tal motivo, imposibilita el adecuado control del acceso y la correcta asignación a los recursos de TI autorizados. Carencia de un proceso de gestión de vulnerabilidades en los sistemas Para consolidar la seguridad de los sistemas debe llevarse a cabo un proceso con el objetivo de minimizar el impacto de las vulnerabilidades y los incidentes de seguridad. Es conveniente establecer un proceso de identificación y tipificación de las vulnerabilidades tecnológicas que impactan en los sistemas, definir los tiempos necesarios para su solución y asignar a los responsables afectados. La falta de un proceso de gestión de vulnerabilidades permite que los sistemas sean susceptibles a amenazas, comprometiendo la asignación a los recursos de TI autorizados. Aceptación del Marco Normativo de Tecnología de Información La publicación de las políticas tecnológicas en el boletín oficial no garantiza el conocimiento ni la aceptación de las mismas por parte de cada agente. Es conveniente documentar el conocimiento, la adhesión y responsabilidad del agente según su función en TI. Limitación en la seguridad de la infraestructura por sistemas no gestionados Los sistemas no gestionados o parcialmente gestionados por ASInf utilizan la totalidad o parte de la estructura tecnológica

perteneciente al GCABA. Las vulnerabilidades no controladas en los mencionados sistemas permiten materializar las amenazas a través de ataques a la infraestructura de TI del organismo que impactan en la continuidad de sus servicios.

Limitación en la firma digital

La firma digital, simplifica procesos, minimiza los costos y suministra seguridad durante el intercambio de la información digital. Utilizado en el envío de correos electrónicos, documentos de texto, imágenes, planillas y mayormente para formatos PDF. El auditado declara que la tecnología usada actualmente en firma digital posee limitaciones en los procesos de obtención de nuevos certificados al igual que para agregar nuevos procedimientos.

Las limitaciones tecnológicas en los procesos de firma digital pueden generar intercambios de información poco seguros a través de otros medios electrónicos o regresar al formato papel que, además, incrementaría los costos de dichos procesos.

Herramientas de monitoreo y prevención limitadas

La frecuencia, complejidad y diversidad de las amenazas que se presentan en la red, requiere de la vigilancia constante y actualización de las herramientas utilizadas para monitorear, detectar y prevenir los ataques cibernéticos. La utilización de herramientas básicas o saturadas para anticipar los intentos de daños informáticos no garantiza la continuidad de las operaciones informáticas ni la conservación y protección de la información.

Saturación de registros (log´s)

Los registros informáticos o log´s, almacenan información de los eventos que afectan a un sistema o proceso particular en forma secuencial. Los datos guardados son una fuente primordial para el análisis de los errores del sistema y sirven como evidencia para diagnosticar los problemas generados e implementar acciones correctivas. La saturación de los registros impide conocer y analizar los eventos ocurridos.

Carencia de grupos electrógenos en ciertos nodos de la red

Es necesario dar cobertura a las fallas provocadas por la falta de energía en los nodos que conforman la red que transmite información del GCABA. Ciertos nodos Core, como el ubicado

	en el edificio de Tránsito y otros nodos Borde tales como el Hospital Santojanni, Hospital Zubizarreta, Defensa Civil, los centros de Gestión y participación 12 y 13, entre otros, no poseen conexión a grupo electrógeno. La falta de cobertura de energía alternativa puede ocasionar fallas en la continuidad de los servicios por interrupción en el acceso a la red de datos del GCABA.
Conclusión / Dictamen	La Dirección General Seguridad Informática de la Agencia de Sistemas de Información provee al GCABA servicios tales como el correo institucional, evaluación de aplicaciones, prevención y monitoreo de alertas tempranas y atención de incidentes de seguridad informática, entre otros. Gestiona un inventario de activos de información, el cual se encuentra clasificado en una tabla mediante registros con campos que contienen su descripción. De acuerdo con la Resolución 177/ASInf/2013[1], gestiona la clasificación de los activos de información mediante niveles de confidencialidad, integridad y disponibilidad de la información. Asimismo, define la criticidad de la información como baja, media y alta. Identifica los activos de información con los responsables de las aplicaciones de las diversas áreas de GCABA. La lista de activos de información obtenida, mediante un vector en tres dimensiones, es utilizada para determinar la clasificación definitiva. De acuerdo con el marco normativo de tecnología vigente en el GCABA, ASInf gestiona el tratamiento de activos, el cual tiene como objetivo la protección del inventario tecnológico existente bajo la custodia del organismo. La asignación de las responsabilidades está clasificada como usuario, custodio o propietario. ASInf administra el control y los accesos a las áreas críticas, centros de datos, procesamiento y almacenamiento de copias de resguardo. La Dirección de Seguridad Informática de la Agencia de Sistemas de Información tiene dependencia jerárquica funcional de la Dirección Ejecutiva. Esta configuración en la estructura organizativa debilita el ambiente de control interno.

	Se destaca la conveniencia que la Dirección de Seguridad Informática dependa jerárquicamente de un nivel superior. Los controles de seguridad de la información están limitados ya que ASInf no administra la totalidad de los sistemas usados por el GCABA. Es necesario centralizar la gestión de los servicios con la finalidad de asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información. De esta manera se evita la duplicación de los datos existentes en el GCABA. Sería aconsejable que el personal de ASInf incremente el apoyo y brinde capacitación a los recursos humanos de los organismos del GCABA, teniendo en cuenta que, según el tamaño y complejidad, no siempre poseen personal idóneo en seguridad. Las cuentas de usuarios en sistemas que no dependen directamente de ASInf, conllevan un alcance limitado en cuanto a la verificación de la identidad. También sería adecuado establecer un proceso de identificación y tipificación de las vulnerabilidades tecnológicas que impactan en los sistemas. En cuanto a la seguridad y aceptación del marco normativo indicado por ASInf, sería apropiado que la misma sea formalizada, tomada conocimiento por los diferentes sectores de sistemas de los organismos del GCABA. Por otro lado, es importante incrementar la capacidad para evitar la saturación de los registros (log´s), almacenar la totalidad de los eventos ocurridos en los sistemas y el posterior análisis e implementación de las acciones correctivas necesarias. El auditado destaca que se encuentra aprobado el presupuesto y en proceso de implementación, el recambio tecnológico del SOC (Centro de Operaciones de Seguridad), a los fines de garantizar la continuidad de las operaciones informáticas y la conservación y protección de la información. Con dicho proyecto se lograría una mayor capacidad y velocidad en la prevención de ataques. Para asegurar la continuidad de los servicios, es ventajoso contar con grupos electrógenos que provean energía eléctrica a todos los nodos de la red. Por último, sería beneficiosa la implementación de los dos equipos Criptográficos HSM (Hardware Security Modules)

	adquiridos en el año 2020 con el objetivo de garantizar la seguridad en el intercambio de información. Así también, la existencia de un mayor número de herramientas de monitoreo con el propósito de mitigar y minimizar las amenazas informáticas.
Palabras Claves	Monitoreo, vulnerabilidades, firma digital, organismos GCABA.

INFORME FINAL DE AUDITORÍA
"ASI SEGURIDAD INFORMÁTICA"
PROYECTO Nº 10.20.04

DESTINATARIO

Presidente
Legislatura Ciudad Autónoma de Buenos Aires
Cdor. Diego César Santilli
S / D

En uso de las facultades conferidas por los artículos 131, 132 y 136 de la Ley 70 de la Ciudad Autónoma de Buenos Aires, y conforme a lo dispuesto en el artículo 135 de la Constitución de la Ciudad, la Auditoría General de la Ciudad de Buenos Aires procederá a realizar una auditoría de relevamiento en la Dirección General de Seguridad Informática, a su cargo con el objeto detallado en el apartado siguiente.

.

I. OBJETO DE AUDITORIA

Sistemas de la Dirección de Seguridad Informática de la Agencia de Sistemas de Información de la Ciudad de Buenos Aires.

II. OBJETIVO DE LA AUDITORIA

Relevar los sistemas utilizados para la gestión de seguridad informática.

III. ALCANCE DEL EXAMEN

Analizar la infraestructura de seguridad, la gestión de la misma y la prevención de los incidentes.

ANEXO I

- ORGANIGRAMA
- NÓMINA DE PERSONAL

MARCO NORMATIVO

Se utilizará el siguiente marco normativo:
Normas Básicas de Auditoria Externa de la AGCBA y las Normas Básicas de Auditoría de Sistemas de la AGCBA, la ley 70, ley 325 y complementarias.

Manual COBIT IV. (Control Objectives for Information and related Technology) de la Information Systems Audit and Control Association. Capítulo Buenos Aires.

Supletoriamente se utilizarán:
Las normas y recomendaciones de seguridad establecidas por la ASInf (Ex DGEySI).

PROCEDIMIENTOS REALIZADOS

Con fecha Junio de 2020 se cursó nota para la presentación del equipo y la solicitud de la documentación.

Se analizó la información recibida y se cursaron correos solicitando ampliaciones o aclaraciones de algunas respuestas.

Se analizó la información recibida respecto de la nómina de empleados.

Se evaluaron los planes y proyectos del organismo. Se verificaron los servicios provistos por ASInf a los organismos del GCABA y aquellos provistos por terceros a la agencia.

Se examinó la estructura del inventario de activos de información y la clasificación utilizada.

Se analizó el diagrama de flujo usado para la identificación de activos de información y la clasificación según su tipología.

Se revisaron las normas vigentes relativas al objeto de esta auditoría y su cumplimiento.

Se analizó el cumplimiento del Marco Normativo de IT vigente según la Resolución 177/ASInf/2013[1].

[1] Resolución N°177/ASInf/13 - Obtenido el 6 de Noviembre de 2013 en: https://n9.cl/12dwx [Accedido el 18/9/20]

IV. LIMITACIONES AL ALCANCE

La limitación en la circulación establecida por el GCABA durante la cuarentena impidió la ejecución de las pruebas sustantivas en los centros de datos de la Agencia de Sistemas de Información.

V. ACLARACIONES PREVIAS

Jurisdicción y Presupuesto

El Presupuesto 2019, en su Anexo III, Distribución Administrativa de Créditos, asigna a la Agencia de Sistemas de Información un crédito total por $ 1.345.344.758 (ver Anexo II).

Mediante la Jurisdicción 21, Entidad 270, Unidad Ejecutora 8056, Programa 7, concede a Seguridad Informática un total de $ 62.657.427 [2] (ver Anexo III).

Se atribuye al personal $ 271.432.566, a bienes de consumo $ 3.962.880, servicios no personales $ 903.014.056 y a bienes de uso $ 166.935.256 [3] (ver Anexo IV).

En Organismos Descentralizados, Entes Autárquicos, y Órganos de Control - Composición del Gasto por Finalidad y Función, y Entidad, del total de $ 1.345.344.758, se asignan $ 1.338.081.742 a la Dirección Ejecutiva y $ 7.263.016 al Control de la Gestión[3] (ver Anexo V).

Según describe la Administración del Gobierno de la Ciudad de Buenos Aires en su Plan Plurianual de Inversiones Públicas, entre los años 2019 - 2020, se asigna a ASInf inversiones por $ 571.628.443, de los cuales se estipulan $ 2.000.000 para la remodelación de edificios de ASInf, $ 50.000.000 a Seguridad Informática, $ 20.000.000 a Segurización y $ 30.000.000 a Ciberseguridad y Protección de la red y los datos [4] (ver Anexo VI).

[2] Anexo III - Distribución Administrativa de Créditos - Presupuesto 2019 - Obtenido el año 2019 en: https://n9.cl/3lvn9 [Accedido el 13/10/20]

[3] Planillas Anexas Presupuesto 2019 - Obtenido el año 2019 en: https://n9.cl/6p6i [Accedido el 13/10/20]

[4] Anexo Plan Plurianual de Inversiones Públicas 2019-2021 sanción - Obtenido el año 2019 en: https://n9.cl/oha4 [Accedido el 13/10/20]

Normativa:

En el año 2008, la Legislatura de la Ciudad Autónoma de Buenos Aires sanciona la ley 2689 mediante la cual crea la Agencia de Sistemas de Información.[5]

Durante el año 2009, se sanciona la ley 3304, Ley de Modernización de la Administración Pública, cuyo objetivo fue implementar un proceso de modernización administrativa en el Gobierno de la Ciudad Autónoma de Buenos Aires. [6]

La Resolución Nº 224/ASINF/2018 [7] modifica la estructura organizativa y las responsabilidades primarias de ASInf [8] (ver Anexo I).

ASinf, durante el año 2013 confeccionó un Marco Normativo de Tecnología de Información, publicado en la Resolución N° 177 [1], cuyo objetivo fue fomentar la estandarización de los bienes informáticos, equipos, recursos y sistemas para ser utilizados por el Poder Ejecutivo.

DIRECCIÓN GENERAL DE SEGURIDAD INFORMÁTICA

Responsabilidades Primarias

Las responsabilidades primarias de la Dirección General Seguridad Informática detalladas en la resolución, mencionan:

- "Elaborar y/o aprobar las pautas, políticas y normas de seguridad física y lógica de sistemas, equipos informáticos, datos y comunicaciones del Gobierno de la Ciudad Autónoma de Buenos Aires".

[5] Ley 2689 - Obtenido el año 2008 en: https://n9.cl/5b2c7 [Accedido el 13/10/20]

[6] Ley 3304 - Ley de Modernización de la Administración Pública - Obtenido el año 2009 en: https://n9.cl/zy8e [Accedido el 13/10/20]

[7] Resolución Nº 224/ASInf/2018 - Obtenido el 13 de Diciembre de 2018 en: https://n9.cl/8fb2 [Accedido el 13/10/20]

[8] Anexo de la Resolución Nº 224/ASInf/2018 - Obtenido el 13 de Diciembre de 2018 en: https://n9.cl/760m [Accedido el 13/10/20]

- "Intervenir en las definiciones de los esquemas de seguridad del software, datos y comunicaciones, de los programas de prevención y control de seguridad, y de los planes de contingencia".

- "Definir, implementar y administrar la Identidad de los usuarios del Gobierno de la Ciudad Autónoma de Buenos Aires".

- "Administrar la infraestructura de firma digital del Gobierno de la Ciudad Autónoma de Buenos Aires.

- "Administrar y controlar la operatividad de los sitios de internet, el servicio de correo electrónico y el servicio de acceso a internet".

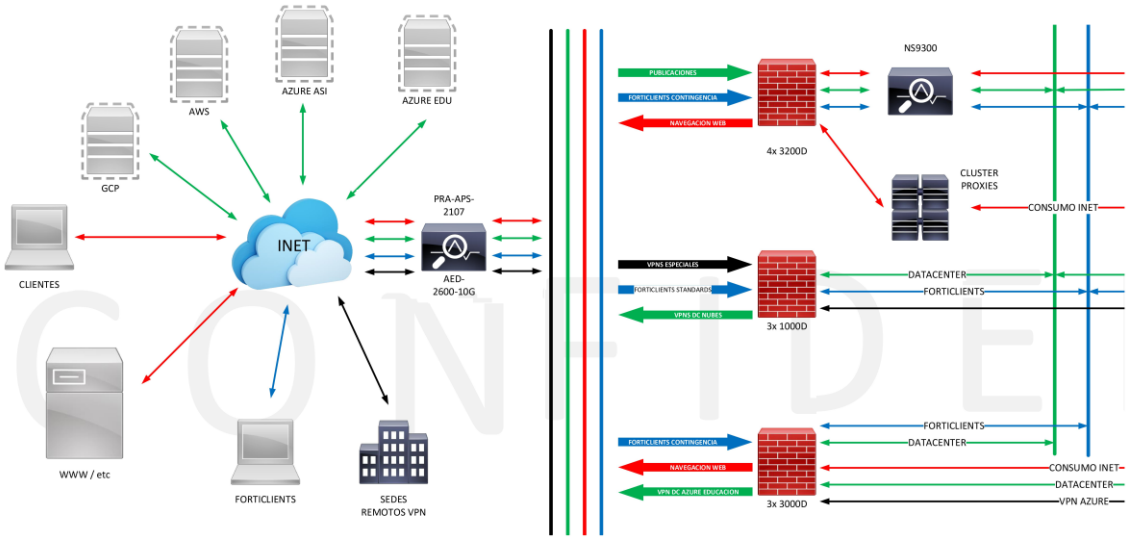
- "Administrar y controlar los procedimientos de seguridad lógica de acceso a los componentes del software de base y aplicativo de los servidores bajo responsabilidad de la Agencia de Sistemas de Información".

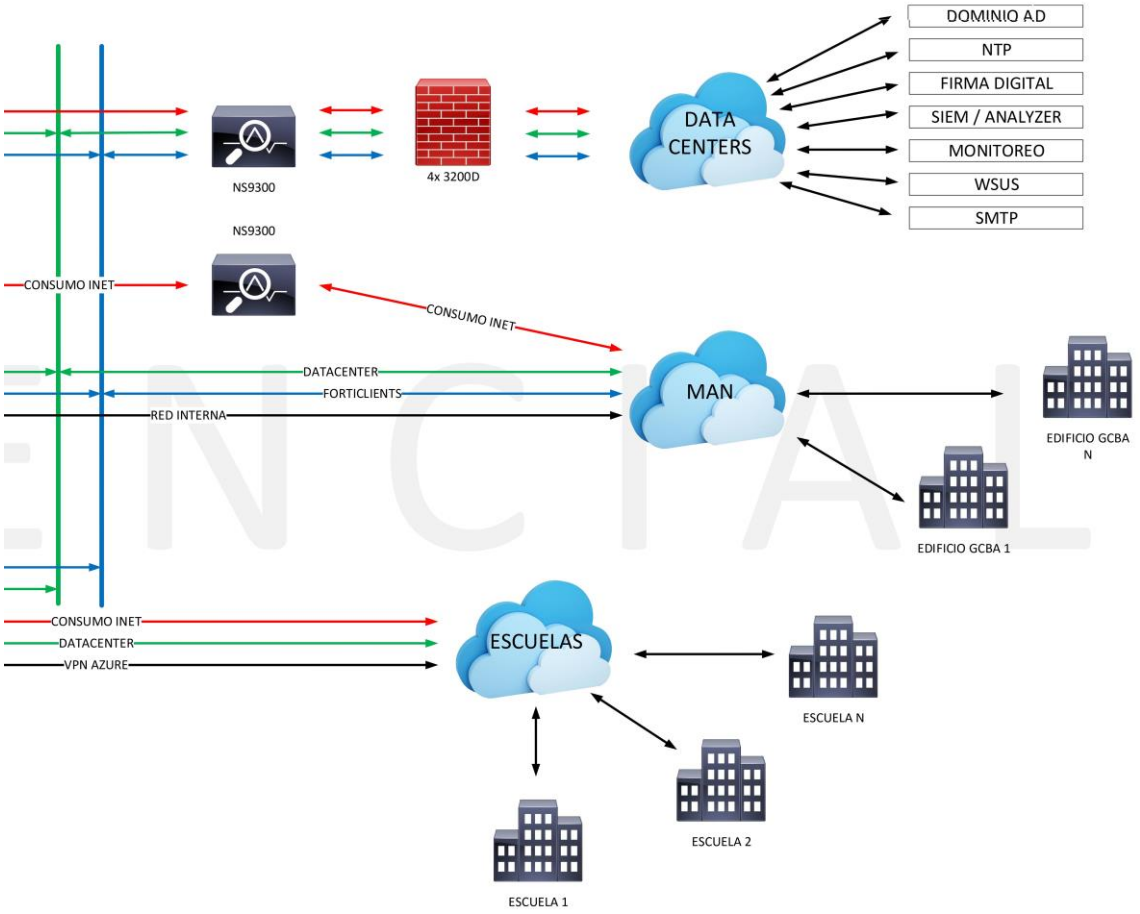
- "Definir los mecanismos de monitoreo, alarmas, y monitorear los sistemas y las redes de comunicaciones para detectar intentos de acceso no autorizados al software aplicativo, y a los datos almacenados en los servidores bajo la responsabilidad de la Agencia de Sistemas de Información".

- "Participar en la capacitación de usuarios con el objetivo de entrenar, informar y concientizar en materia de seguridad informática".

MAPA FÍSICO Y LÓGICO DEL GCABA

La siguiente imagen detalla el diagrama general de arquitectura de seguridad informática del GCABA.





AGENCIA DE SISTEMAS DE INFORMACION

Planes y proyectos

La planificación de ASInf en seguridad informática para el año 2020-2021destaca la protección de la información relacionada con los ciudadanos y el GCABA cumpliendo con los más altos estándares de seguridad. Proyecta el logro de beneficios tales como el análisis del 100% de las app, la cobertura total de las solicitudes de capacitación y educación, concientización sobre ciberseguridad y la visibilidad total del tráfico para la prevención.

Define la situación actual con un análisis de seguridad de las apps a publicar dentro del 70%. Expresa que el monitoreo y la visibilidad acusa una saturación, las campañas y la educación al ciudadano se encuentran en el 70% de la demanda (BA CSIRT) y la firma digital está limitada tecnológicamente.

BA-CSIRT "es un centro de expertos en ciberseguridad, que se dedica a asistir y concientizar a los ciudadanos y al Gobierno de la Ciudad de Buenos Aires en todo lo relacionado a la seguridad de la información" [9]

La planificación, incluye el mantenimiento de:

- Seguridad en aplicaciones WEB móviles
- Herramientas de análisis de app
- Herramientas de análisis de código
- Concientizaciones
- Visibilidad de tráfico
- Antivirus
- Certificados SSL (Secure Sockets Layer) [10]

Respecto de la nueva firma digital,[11] aún pendiente de aprobación, posee las siguientes características:

- Soporta capacidad mobile.
- GCABA mantiene autonomía y expande su funcionalidad.

[9] BA-CSIRT - Obtenido el año 2016 en: https://www.ba-csirt.gob.ar/ [Accedido el 15/10/20]

[10] SSL (Secure Sockets Layer), en español Capa de conexiones seguras, es un protocolo que utiliza certificados digitales para establecer comunicaciones seguras mediante internet.

[11] *FIRMA DIGITAL* es una solución tecnológica mediante la cual se agrega a mensajes de correo electrónico o documentos digitales, una marca única, mediante operaciones matemáticas.

Se reconoce la imposibilidad de seguir ofreciendo nuevos certificados y la existencia de limitaciones para incrementar nuevos procesos con la tecnología de firma digital vigente.

ASInf soporta operaciones complejas de 8 horas por 5 días semanales, existen carencias en las herramientas de análisis, incremento en el tráfico y sus requerimientos, además se evidencia la saturación de registros (log's).[12]

Se proyectan elevar las operaciones a 7 días las 24 horas para cumplimentar eficientemente los requerimientos diarios y consolidar las herramientas de alerta temprana de análisis manual y prevenir los ataques cibernéticos.

Actualmente realizan tareas once agentes especializados en análisis forense, que a través del modelo BA CSIRT incorporado al FIRST (en español, Foro de equipos de seguridad y respuesta a incidentes),[13] colaboran internacionalmente para la resolución de incidentes.

Servicios provistos

La Dirección General Seguridad Informática de la Agencia de Sistemas de Información provee al GCABA los siguientes servicios:

- Correo transaccional - correo personalizado a gran cantidad de destinatarios, originado en transacciones de aplicación.
- Plataforma colaborativa - sistema basado en la nube para almacenar y compartir documentos mediante el uso de herramientas de edición web.
- Evaluaciones de Aplicaciones Web, Mobile y WebServices - administración y control de vulnerabilidades de desarrollo.
- Pentest[14] - control de activos en la DMZ[15].
- Forense - servicio desarrollado a pedido de algún incidente.

[12] *LOG* es el almacenamiento del historial secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular.

[13] *FIRST* - Obtenido el año 1988 en: https://www.first.org/ [Accedido el 15/10/20]

[14] *PENTEST* es el ataque a un sistema informático con la finalidad de encontrar debilidades de seguridad que permitan el acceso a su funcionalidad y datos.

[15] *DMZ*, en seguridad informática, es una red perimetral o local ubicada entre la red interna de un organismo y una red externa, generalmente en Internet.

- Prevención y Monitoreo de Alertas Tempranas - análisis del tráfico sobre equipos de seguridad.
- Análisis preventivos, proactivos y forenses de aplicaciones, servicios e incidentes - análisis del diseño de la arquitectura, bases de datos e integraciones de aplicaciones. Definiciones de los esquemas de seguridad del software, datos y comunicaciones, de los programas de prevención y control de seguridad y de los planes de contingencia.
- Atención a la ciudadanía ante incidentes de seguridad informática - recepción, atención y asesoramiento técnico, legal y administrativo, vía telefónica, correo y/o redes sociales respecto de los incidentes de seguridad informática derivados del uso de la tecnología.
- Charlas, capacitaciones y actividades de formación de BA-CSIRT - actividades de concientización, capacitación y formación en seguridad informática, ciberseguridad y áreas afines.
- Gestión de accesos a los sistemas de gobierno, monitoreo permanente de seguridad y certificados de seguridad (SSL) - registro y mantenimiento de los dominios del GCABA en la entidad NICAR.[16] Definición, implementación y administración de la identidad de los usuarios del GCABA. Administración y mantenimiento de los Certificados de Seguridad SSL. Administración de bienes y recursos por compras y contrataciones. Registración de "Derechos de Autor" de desarrollos propios y bases de datos a nivel GCABA.
- Firma digital - emisión y administración de los Certificados de Firma Digital.

Inventario

ASInf ha establecido un diseño de la estructura del inventario de activos de información que se encuentra bajo su gestión. Se han identificado e inventariado los activos más importantes, los servicios entregados a través de los mismos, la relación con las aplicaciones, el software adquirido y el desarrollado, la infraestructura tecnológica afectada y los agentes responsables de los activos mencionados.

[16] *NICAR* es la Dirección Nacional del Registro de Dominios de Internet, dependiente de la Secretaría Legal y Técnica de la Presidencia de la Nación, responsable de administrar el dominio de nivel superior .ar y registrar los nombres de dominio de internet de las personas físicas y jurídicas.

El inventario se encuentra clasificado en una tabla, cada registro está compuesto por los siguientes campos con su descripción:

- Activo: nombre (unívoco) del activo.
- Descripción: texto descriptivo del activo.
- Detalle: tipología del activo en la lista de detalles.
- Primario: si el activo forma parte de un grupo de redundancia, su nombre es el del activo primario.
- Estado: estado del ciclo de vida del activo (Producción, Revisar, Prueba, Baja).
- Tipo de Área: se calcula automáticamente en función de lo ingresado en el campo Área.
- Área: nombre del área responsable del activo.
- Custodio Principal: nombre del Custodio principal del activo.
- Propietario Principal: nombre del Propietario principal del activo.
- Custodio Delegado: nombre del Custodio delegado del activo.
- Propietario Delegado: nombre del Propietario delegado del activo.
- IP: en los activos que corresponda, se ingresa la dirección IP.
- URL: en las Aplicaciones, se ingresa su URL.

Asimismo, existen cuatro campos de verificación que se completan automáticamente según los datos ingresados. En las dependencias se registran las relaciones entre los activos del inventario realizando una verificación automática a través de cinco campos que se completan automáticamente en función de los datos ingresados. Ante la detección de un error, se genera un alerta, marcando los registros en color naranja y obligando a ser corregido.

Clasificación de Activos de Información

ASInf clasifica los activos bajo su gestión según el Marco Normativo de IT vigente según la Resolución 177/ASInf/2013.[1]

Los activos de información se clasificarán de acuerdo a los atributos de la información según el siguiente esquema:

- Nivel de Confidencialidad de la información
  - ✓ Pública - puede ser conocida y utilizada sin autorización por cualquier persona.

- ✓ Uso interno - puede ser conocida y utilizada por los agentes del GCABA y algunas entidades externas, su divulgación o uso no autorizados podría ocasionar un leve impacto a nivel operativo en el GCABA.
- ✓ Confidencial - puede ser conocida y utilizada por algunos agentes del GCABA para cumplir sus funciones y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a nivel directivo en el GCABA.
- ✓ Secreta - información que sólo puede ser conocida y utilizada por un grupo reducido de agentes del GCABA cuya divulgación podría ocasionar pérdidas graves a nivel estratégico en el GCABA.

- Nivel de Integridad de la información
  - ✓ Reemplazable - la modificación no autorizada de la información no impacta en la operatoria diaria del GCABA.
  - ✓ Baja - es el caso de información que es posible obtener con facilidad nuevamente y su modificación no autorizada podría ocasionar pérdidas menores en el GCABA.
  - ✓ Alta - es la información difícil de obtener nuevamente, su modificación no autorizada podría ocasionar pérdidas significativas al GCABA.
  - ✓ Crucial - es aquella información irremplazable, su modificación no autorizada podría ocasionar un impacto grave a nivel estratégico al GCABA.

- Nivel de Disponibilidad de la información
  - ✓ Estándar - la inaccesibilidad a la información no impacta en la operatoria del GCABA.
  - ✓ Relevante - la falta de acceso a la información durante una semana o más, podría ocasionar un impacto a nivel operativo en el GCABA.
  - ✓ Delicada - la inaccesibilidad a la información durante un día o más, podría ocasionar pérdidas significativas al GCABA.
  - ✓ Vital - la falta de acceso a la información durante unas horas podría ocasionar un impacto grave a nivel estratégico en el GCABA.

Según el Marco Normativo de IT vigente, ASInf define la Criticidad de la Información con una escala de tres niveles.

- Baja
- Media
- Alta

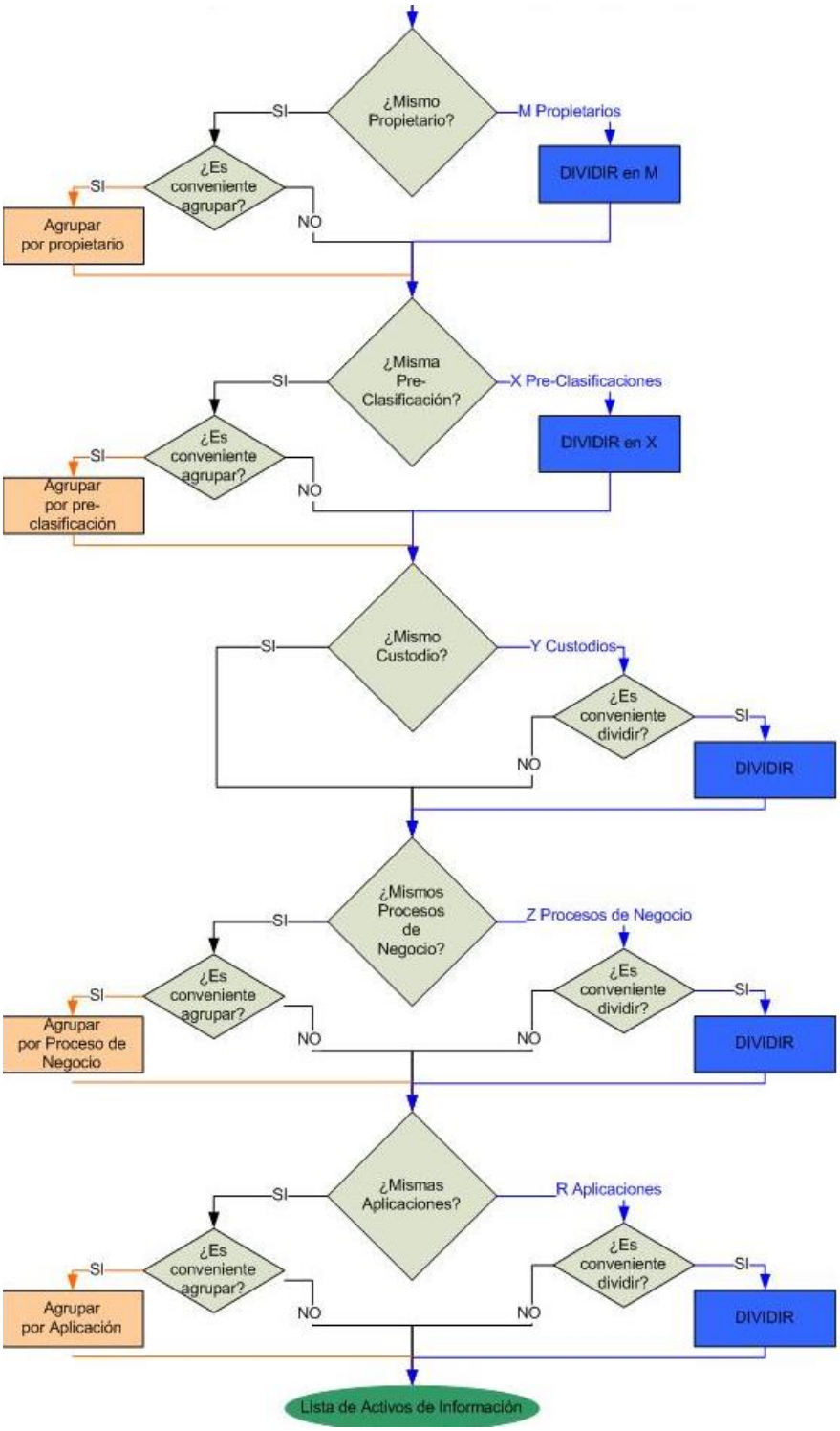
Identificación de Activos de Información

A través de entrevistas llevadas a cabo con los responsables de las aplicaciones y de las diversas áreas de GCABA, ASInf identifica los activos de información. Se aplica un proceso de deducción sobre los activos de información partiendo del conocimiento de los procesos (top-down) y del conocimiento de las aplicaciones o sistemas (bottom-up). El proceso de comprensión se lleva adelante mediante:

- Actividades con los responsables de las aplicaciones:
  - ✓ Identificando las aplicaciones bajo su responsabilidad.
  - ✓ Identificando la información que provee cada aplicación.

- Actividades con los responsables de las áreas:
  - ✓ Entendiendo los procesos/subprocesos bajo su responsabilidad.
  - ✓ Identificando la información necesaria para soportar cada proceso.

Mediante un proceso de pre clasificación se define una valoración temprana sobre los activos identificados. Los propietarios de los activos de información especifican los niveles de clasificación en cada una de las dimensiones, según necesidades y/o conocimientos. El resultado obtenido es una lista de Activos de Información con su vector en tres dimensiones utilizado para determinar posteriormente la clasificación definitiva. El siguiente diagrama de flujo permite establecer una serie de criterios para agrupar o dividir los activos de información dentro de su misma tipología.



Luego del proceso de clasificación, identificación del inventario, pre-clasificación y agrupación/división de los activos de información, se lleva adelante la clasificación definitiva. Se modifican y/o confirman los parámetros de clasificación obtenidos con la finalidad de elaborar una lista definitiva de Activos de Información con su vector en tres dimensiones.

La siguiente imagen es un ejemplo de Activos Identificados por Tipología:

Aplicaciones adquiridas	62
Aplicaciones propias	492
Datos informatizados	114
Edificaciones	4
HW de Almacenamiento	1
Instalaciones físicas	4
Otro HW	3
Servidor virtual	197
Servidores	6
Sistema Gestor de BD	72
Total general	**955**

La siguiente figura ejemplifica los Activos Identificados por Área:

ASI	**201**
Aplicaciones propias	2
Datos informatizados	1
HW de Almacenamiento	1
Servidor virtual	145
Servidores	1
Sistema Gestor de BD	51

Las Dependencias definidas por Tipología se exhiben según los próximos parámetros:

P_Detalle	H_Detalle	Total
Aplicaciones adquiridas	Otro HW	1
	Servidor virtual	260
	Servidores	1
	Sistema Gestor de BD	30
Aplicaciones propias	HW de Almacenamiento	11
	Otro HW	3
	Servidor virtual	1.866
	Servidores	11
	Sistema Gestor de BD	433
Datos informatizados	Aplicaciones adquiridas	177
	Aplicaciones propias	493
Instalaciones físicas	Edificaciones	4
Servidor virtual	Servidores	8
Servidores	Instalaciones físicas	5
Total general		**3.303**

Los Activos de Información según su criticidad pueden clasificarse por área.

Cuenta de Activo		
Área	Criticidad	Total
	Alta	1
	Media	2
Agencia Gubernamental de Control	Media	3
ASI	Media	1
Jefatura de Gabinete	Alta	2
	Media	4
Jefe de Gobierno	Alta	2
	Media	4
	Baja	2

Tratamiento de Activos

El tratamiento de los activos tiene por objetivo proteger el inventario tecnológico existente bajo la custodia de ASInf. Está basado en la clasificación de los activos por su confidencialidad, integridad y disponibilidad de los sistemas de información, las áreas y el personal involucrado en sus procesos.

Las responsabilidades del tratamiento de la información son asignadas como:

- Propietario: funcionarios con responsabilidad de gestión y uso de un activo o proceso en particular.
- Custodio: encargado de la gestión de los sistemas que administran la información y los procesos de negocio. La custodia de los activos de información está a cargo de la ASInf.
- Usuario: es el agente con acceso autorizado a la información para cumplir las funciones que le fueron asignadas.

ASInf es la responsable de la Gestión de la Clasificación de la Información, la revisión periódica de la clasificación y la modificación o supresión sólo con el consentimiento del Propietario de la Información.

A través de un proceso se gestionan los riesgos del tratamiento de la Información Clasificada cuya finalidad será determinar los riesgos de seguridad conocidos y definir las medidas de seguridad para reducir los mencionados riesgos a un nivel aceptable acordes a los definidos en la normativa vigente en el GCABA.

Asimismo, se gestiona la seguridad ligada al personal mediante la implementación de medidas que garantizan la obtención de la Información Clasificada por el GCABA a los agentes que necesitan acceder para cumplir las funciones laborales asignadas. Se implementan medidas que aseguren la protección técnica y física que impida o disuada el acceso sin autorización a la Información Clasificada tratada por el GCABA. Las áreas de almacenamiento de información clasificada como confidencial están protegidas con un acceso restringido y los dispositivos utilizados son sólo los autorizados.

La protección de la información se estructura a través de criterios aplicados según su confidencialidad, integridad y disponibilidad, establecen distintos niveles y sus correspondientes actividades aplicadas, las cuales garantizan el tratamiento de la información con seguridad física y lógica.

Los resultados obtenidos en el tratamiento según los atributos de confidencialidad, integridad y disponibilidad, muestran los activos de información clasificados por activo, nivel, área y propietario principal (agente responsable).

Control y acceso a las áreas críticas

La clasificación de áreas críticas por parte de ASInf incluye tanto los centros de procesamiento de datos como los de almacenamiento de copias de resguardo. Todos aquellos que contengan información del GCABA, sean propios o de terceros.

El acceso físico al centro de cómputos ubicado en la Av Independencia 635, Caba se encuentra protegido mediante sensores biométricos. Se ingresa mediante dos puertas controladas. Pasado el primer control se accede a la sala de operaciones, donde se encuentran los operadores. Para ingresar al centro de datos, se debe atravesar el control de la segunda puerta, también con controles biométricos que permite ingresar sólo al recurso humando autorizado.

Sólo accede personal autorizado o terceros con fines labores, acompañado por personal del área correspondiente al organismo, dejando registrada su firma en la bitácora de ingreso.

Asimismo, el acceso de entrada al edificio posee personal de vigilancia las 24 horas y un circuito cerrado de cámaras de video.

Además, existe otro centro de cómputos, situado en la calle Uspallata 3160, Caba, el cual permite seguir operando en caso que el centro de cómputos emplazado en Av Independencia fuera afectado por un incidente que impidiera su continuidad operativa. El acceso a este último también se encuentra

protegido por controles de acceso biométricos y recurso humano que realiza tareas de vigilancia.

Ambos centros poseen sistemas de protección contra incendios y controles ante fallos de energía (UPS[17] y generadores).

Análisis de fallas y contingencias

El backbone IP/MPLS [18] del GCABA está compuesto por equipos tipo Carrier Class[19], ubicados en diversos edificios gubernamentales dentro de la Ciudad Autónoma de Buenos Aires. La vinculación de los equipos se realiza mediante fibras ópticas propias del GCABA.

El backbone IP/MPLS del GCABA está formado por:

- 6 equipos de Core[20]
- 15 equipos de Borde[21]
- 14 equipos Satélites

ASInf establece el análisis de fallas considerando que la ocurrencia podría producirse una a la vez. La estructura implementada es la siguiente:

1. Fallas en la electrónica de red
   1.1 Los equipos de Core proveen redundancia ante fallas en procesadores (dos procesadores), Switch-fabric[22] (poseen cinco),

[17] *UPS* - Uninterruptible Power Supply, (Sistemas de Alimentación Ininterrumpida), es un dispositivo que posee baterías o elementos almacenadores de energía, que en los casos de interrupción de suministro eléctrico, proporciona energía por un tiempo determinado a todos los dispositivos que se encuentren conectados.

[18] BACKBONE IP/MPLS Se refiere a la "columna vertebral" en la que se apoyan todas las conexiones troncales principales de Internet. Los enlaces están compuestos de un amplio número de enrutadores interconectados a través de fibra óptica.

[19] CARRIER CLASS Es un sistema compuesto por hardware y/o software que provee conexiones con un alto nivel de confiabilidad por su calidad, velocidad y redundancia.

[20] CORE Es la parte central de una red de telecomunicaciones que brinda varios servicios a diferentes usuarios que se conectan a través de la red de acceso.

[21] BORDE Es el acceso de los equipos a los servicios mediante una red que se conecta a la red principal.

[22] *SWITCH FABRIC* Es la estructura de conmutación de los datos que ingresan a un nodo de red por un puerto hacia el siguiente nodo de la red.

fuentes de alimentación (cuatro), ventiladores (dos bandejas de redundancia) y puertos de servicio (redundancia de cuatro líneas con cuatro puertos de servicio cada una).

1.2 Los equipos de Borde proveen redundancia ante fallas en los procesadores (tienen dos procesadores), cinco Switch-fabric de redundancia, cuatro fuentes de alimentación y dos bandejas de ventiladores. En los puertos de servicio, cuentan con redundancia de dos líneas con dos adaptadores modulares de puertos en cada una.

1.3 Los equipos Satélite brindan redundancia ante fallas en los procesadores (tarea asignada a 2 equipos), Switch-fabric (tarea delegada a 2 equipos), redundancia de dos fuentes de alimentación y dos ventiladores.

2. Fallas en los vínculos de fibra

- ✓ Los equipos de Core forman una topología full mesh[23] entre sí a través vínculos de fibra óptica propios del GCABA con velocidades de hasta 100Gbps. Los vínculos llegan a cada equipo de Core por caminos diferentes y se conectan a distintos puertos. Esto garantiza que ante la caída de cualquiera de los vínculos en la red de Core, siempre existen como mínimo dos caminos de reserva mediante los cuales los equipos pueden continuar transportando la información.

- ✓ Cada equipo de Borde se conecta a dos equipos de Core a través de vínculos de fibra óptica propios del GCABA. Vinculado mediante caminos diferentes, con velocidades de hasta 100Gbps cada uno y conexiones a distintos puertos. Existen sólo cuatro casos, en donde los equipos de Borde se conectan a un sólo equipo de Core, tales como Tránsito, CUCC[24], etc. Estos casos

[23] MESH Es una configuración de malla completa en donde cada nodo de la red (dispositivo o estación de trabajo) se conecta en forme directa con cada uno de los otros.

[24] CUCC Centro Único de Coordinación y Control, es el centro de coordinación de acciones entre agencias para dar solución en casos de emergencia, tales como las Direcciones de Defensa Civil, Guardia de Auxilio y Emergencias, Logística, Bomberos, Policía de la Ciudad, SAME, Dirección Cuerpo de Agentes de Control de Tránsito y Transporte, etc.

se dan en los sitios donde el equipo de Core y el equipo de Borde se encuentran ubicados físicamente en la misma sala, en racks contiguos. Por tal motivo, ante la ocurrencia de una falla en un vínculo de fibra óptica en un equipo de Borde, el dispositivo continuará enviando los paquetes mediante el vínculo de reserva correspondiente.

- ✓ Los equipos Satélites se vinculan a dos equipos de Borde mediante fibras ópticas propias del GCABA con velocidades de hasta 100Gbps mediante caminos diferentes. Ante la ocurrencia de una falla en uno de los vínculos de fibra, los paquetes continuarán siendo transmitidos a través del vínculo de reserva hacia el equipo de Borde correspondiente.

En el caso que ocurriera una falla en cualquiera de los vínculos de fibra óptica, se genera una notificación y una acción correctiva a través de un ticket a la compañía proveedora del servicio de mantenimiento de fibras ópticas, la cual debe brindar una solución al problema en cumplimiento a los SLA[25] del contrato correspondiente.

3. Fallas de energía en el nodo

La mayoría de los nodos poseen conexión a UPS[17] propias de ASInf o centrales propias del edificio en donde se encuentran instalados. La UPS tiene el objetivo de mitigar los cortes de energía de corta duración. No todos los nodos, ya sean Core o de Borde, están conectados a un grupo electrógeno.

Algunos nodos Core, como el ubicado en el edificio de Tránsito y otros nodos Borde tales como el Hospital Santojanni, Hospital Zubizarreta, Defensa Civil, los centros de Gestión y participación 12 y 13, entre otros, no poseen conexión a grupo electrógeno. Varios sitios cuentan con un paquete de baterías externas con la finalidad de incrementar la autonomía provista por la UPS y permitir la reparación de fallas y el mantenimiento necesario.

[25] SLA Service Level Agreement, (en español, Acuerdo de Nivel de Servicio), es un acuerdo firmado entre el proveedor de un servicio y su cliente. El objetivo es establecer el nivel de servicio y sus parámetros, tales como los plazos de entrega, responsables, tiempos de respuesta, tipo de soporte técnico, etc.

Para los casos de fallas en la UPS o batería externa que sean propiedad de ASInf, se genera una acción correctiva a través de un ticket a la empresa proveedora del servicio de mantenimiento de infraestructura, la cual debe intervenir y solucionar la problemática dando cumplimiento al SLA[25] correspondiente.

SERVICIOS SUMINISTRADOS POR PROVEEDORES EXTERNOS

ASInf, regida por la normativa vigente, Ley N° 2.095 [26] a través de: www.buenosairescompras.gob.ar, con un pliego de Contratación Menor, gestionó un Servicio para la Evaluación de la Seguridad de Aplicaciones Web/Móviles de la Agencia de Sistemas de Información.
El pliego solicitaba exponer las técnicas y herramientas que se utilizarían para la detección y el análisis de las vulnerabilidades y solicitaba la realización de tareas mínimas como:

- Identificar el rango de direcciones IP activas, evaluando vínculos de conexión.
- Utilizar diversas técnicas de escaneo (SYN, TCP CONNECT, FIN, XMAS, NULL, ACK) en distintos puertos de los equipos (hosts) encontrados.
- Identificar Web Servers, Mail Servers y FTP Servers.
- Enumerar servicios activos en los equipos (hosts) encontrados.
- Enumeración de contenido web.
- Analizar banners y respuestas de cada uno de los servicios.
- Identificar de forma remota los Sistemas Operativos en uso.
- Identificar sistemas de gestión de bases de datos (Oracle, SQL Server, PostgreSQL, etc.)
- Identificar el uso del protocolo SNMP para administración remota.
- Identificar protocolos y algoritmos de cifrado utilizados en las comunicaciones.
- Identificar transacciones críticas dentro de las aplicaciones web.

También se detallaba la confección de un informe, para ser presentado a la Dirección General de Seguridad Informática de la Agencia de Sistemas de

[26] Ley 2.095 - Ley de Compras y Contrataciones de la Ciudad Autónoma de Buenos Aires - Obtenido el 21 de Septiembre de 2006 en: https://n9.cl/u5b6 [Accedido el 20/10/20]

Información, en el cual se describa el estado de seguridad de la Aplicación/Infraestructura analizada, compuesto, como mínimo por:

- Documentación de hallazgos.
- Documentación de riesgo asociado.
- Documentación de medidas de mitigación.
- Desarrollo de informe detallado final técnico incluyendo la evidencia de las pruebas realizadas.
- Desarrollo de informe ejecutivo final.

VI. DEBILIDADES

Falta de independencia de la Dirección de Seguridad Informática

Para garantizar la seguridad de los sistemas informáticos deben establecerse lineamientos y controles para la tecnología en todos los niveles del organismo. La dependencia jerárquica y funcional de la Dirección de Seguridad Informática con la Dirección Ejecutiva de la Agencia de Sistemas de Información, debilita el ambiente de control interno.

Controles de seguridad limitados en los sistemas no gestionados por ASInf

ASInf no gestiona la totalidad de los sistemas utilizados por el GCABA. Existen otros centros de procesamiento y almacenamiento dependientes del Poder Ejecutivo que no se encuentran bajo la órbita de control de ASInf. La Agencia de Sistemas de información, como órgano de control, debe gestionar y asegurar el cumplimiento del Marco Normativo de Tecnología de Información vigente para la totalidad de los sistemas utilizados por el GCABA.

Alcance limitado de la seguridad en los sistemas no gestionados por ASInf

La falta de administración en los sistemas o el control parcial, no permite la gestión de la identidad y la cuenta de usuario. Por tal motivo, imposibilita el adecuado control del acceso y la correcta asignación a los recursos de TI autorizados.

Carencia de un proceso de gestión de vulnerabilidades en los sistemas

Para consolidar la seguridad de los sistemas debe llevarse a cabo un proceso con el objetivo de minimizar el impacto de las vulnerabilidades y los incidentes de seguridad. Es conveniente establecer un proceso de identificación y

tipificación de las vulnerabilidades tecnológicas que impactan en los sistemas, definir los tiempos necesarios para su solución y asignar a los responsables afectados. La falta de un proceso de gestión de vulnerabilidades permite que los sistemas sean susceptibles a amenazas, comprometiendo la confidencialidad, integridad y disponibilidad de la información contenida.

Aceptación del Marco Normativo de Tecnología de Información

La publicación de las políticas tecnológicas en el boletín oficial no garantiza el conocimiento ni la aceptación de las mismas por parte de cada agente. Es conveniente documentar el conocimiento, la adhesión y responsabilidad del agente según su función en TI.

Limitación en la seguridad de la infraestructura por sistemas no gestionados

Los sistemas no gestionados o parcialmente gestionados por ASInf utilizan la totalidad o parte de la estructura tecnológica perteneciente al GCABA. Las vulnerabilidades no controladas en los mencionados sistemas permiten materializar las amenazas a través de ataques a la infraestructura de TI del organismo que impactan en la continuidad de sus servicios.

Limitación en la firma digital

La firma digital, simplifica procesos, minimiza los costos y suministra seguridad durante el intercambio de la información digital. Utilizado en el envío de correos electrónicos, documentos de texto, imágenes, planillas y mayormente para formatos PDF. El auditado declara que la tecnología usada actualmente en firma digital posee limitaciones en los procesos de obtención de nuevos certificados al igual que para agregar nuevos procedimientos.

Las limitaciones tecnológicas en los procesos de firma digital pueden generar intercambios de información poco seguros a través de otros medios electrónicos o regresar al formato papel que, además, incrementaría los costos de dichos procesos.

Herramientas de monitoreo y prevención limitadas

La frecuencia, complejidad y diversidad de las amenazas que se presentan en la red, requiere de la vigilancia constante y actualización de las herramientas utilizadas para monitorear, detectar y prevenir los ataques cibernéticos. La utilización de herramientas básicas o saturadas para anticipar los intentos de daños informáticos no garantiza la continuidad de las operaciones informáticas ni la conservación y protección de la información.

Saturación de registros (log´s)

Los registros informáticos o log´s, almacenan información de los eventos que afectan a un sistema o proceso particular en forma secuencial. Los datos guardados son una fuente primordial para el análisis de los errores del sistema y sirven como evidencia para diagnosticar los problemas generados e implementar acciones correctivas. La saturación de los registros impide conocer y analizar los eventos ocurridos.

Carencia de grupos electrógenos en ciertos nodos de la red

Es necesario dar cobertura a las fallas provocadas por la falta de energía en los nodos que conforman la red que transmite información del GCABA. Ciertos nodos Core, como el ubicado en el edificio de Tránsito y otros nodos Borde tales como el Hospital Santojanni, Hospital Zubizarreta, Defensa Civil, los centros de Gestión y participación 12 y 13, entre otros, no poseen conexión a grupo electrógeno. La falta de cobertura de energía alternativa puede ocasionar fallas en la continuidad de los servicios por interrupción en el acceso a la red de datos del GCABA.

VII. CONCLUSIONES

La Dirección General Seguridad Informática de la Agencia de Sistemas de Información provee al GCABA servicios tales como el correo institucional, evaluación de aplicaciones, prevención y monitoreo de alertas tempranas y atención de incidentes de seguridad informática, entre otros.

Gestiona un inventario de activos de información, el cual se encuentra clasificado en una tabla mediante registros con campos que contienen su descripción.

De acuerdo con la Resolución 177/ASInf/2013[1], gestiona la clasificación de los activos de información mediante niveles de confidencialidad, integridad y disponibilidad de la información. Asimismo, define la criticidad de la información como baja, media y alta.

Identifica los activos de información con los responsables de las aplicaciones de las diversas áreas de GCABA. La lista de activos de información obtenida, mediante un vector en tres dimensiones, es utilizada para determinar la clasificación definitiva.

De acuerdo con el marco normativo de tecnología vigente en el GCABA, ASInf gestiona el tratamiento de activos, el cual tiene como objetivo la protección del inventario tecnológico existente bajo la custodia del organismo. La asignación de las responsabilidades está clasificada como usuario, custodio o propietario.

ASInf administra el control y los accesos a las áreas críticas, centros de datos, procesamiento y almacenamiento de copias de resguardo.

La Dirección de Seguridad Informática de la Agencia de Sistemas de Información tiene dependencia jerárquica funcional de la Dirección Ejecutiva. Esta configuración en la estructura organizativa debilita el ambiente de control interno. Se destaca la conveniencia que la Dirección de Seguridad Informática dependa jerárquicamente de un nivel superior.

Los controles de seguridad de la información están limitados ya que ASInf no administra la totalidad de los sistemas usados por el GCABA. Es necesario centralizar la gestión de los servicios con la finalidad de asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información. De esta manera se evita la duplicación de los datos existentes en el GCABA.

Sería aconsejable que el personal de ASInf incremente el apoyo y brinde capacitación a los recursos humanos de los organismos del GCABA, teniendo en cuenta que, según el tamaño y complejidad, no siempre poseen personal idóneo en seguridad. Las cuentas de usuarios en sistemas que no dependen directamente de ASInf, conllevan un alcance limitado en cuanto a la verificación de la identidad.

También sería adecuado establecer un proceso de identificación y tipificación de las vulnerabilidades tecnológicas que impactan en los sistemas.

En cuanto a la seguridad y aceptación del marco normativo indicado por ASInf, sería apropiado que la misma sea formalizada, tomada conocimiento por los diferentes sectores de sistemas de los organismos del GCABA.

Por otro lado, es importante incrementar la capacidad para evitar la saturación de los registros (log´s), almacenar la totalidad de los eventos ocurridos en los sistemas y el posterior análisis e implementación de las acciones correctivas necesarias.

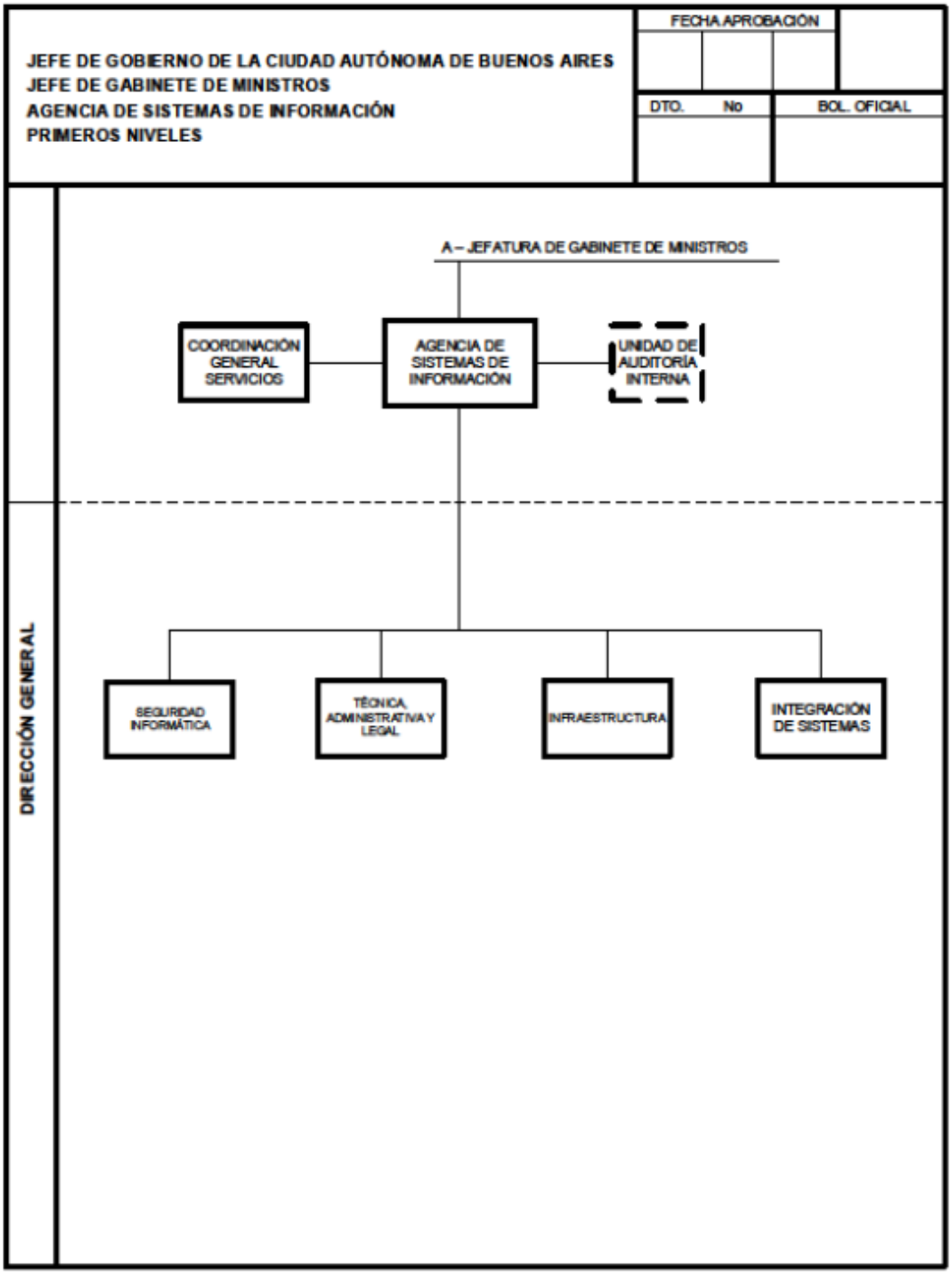
El auditado destaca que se encuentra aprobado el presupuesto y en proceso de implementación, el recambio tecnológico del SOC (Centro de Operaciones de Seguridad), a los fines de garantizar la continuidad de las operaciones informáticas y la conservación y protección de la información. Con dicho proyecto se lograría una mayor capacidad y velocidad en la prevención de ataques.

Para asegurar la continuidad de los servicios, es ventajoso contar con grupos electrógenos que provean energía eléctrica a todos los nodos de la red.

Por último, sería beneficiosa la implementación de los dos equipos Criptográficos HSM (Hardware Security Modules) adquiridos en el año 2020 con el objetivo de garantizar la seguridad en el intercambio de información. Así también, la existencia de un mayor número de herramientas de monitoreo con el propósito de mitigar y minimizar las amenazas informáticas.

ANEXO I

Organigrama 2020



Nómina del personal de la Sede Independencia

Situación de Revista	Función	Título alcanzado	Antigüedad laboral
DG	Director General de Seguridad Informática	Universitario	4
GO	GO Seguridad de la Información	Terciario	3
SGO	SGO Accesos, Investigación y Administración de la Identidad	Secundario	7
SGO (PP)	SGO Monitoreo, Prevención y Detección	Terciario	31
Planta Permanente	Auxiliar administrativo	Secundario	4
	Auxiliar de apoyo informático	Universitario	5
	Asistente de accesos	Secundario	33
	Auxiliar administrativo	Secundario	4
Planta Transitoria	Monitoreo, Prevención y Detección	Secundario	3
Locación de Servicios	Seguridad Informática	Terciario	13
	Analista de Seguridad Informática	Secundario	3
	Operador de Seguridad Informática Nivel 2	Secundario	3
	Operador de Seguridad Informática	Secundario	4
	Seguridad Informática	Secundario	2
	Asesor Legal en Ciberseguridad	Secundario	2

Situación de Revista	Función	Título alcanzado	Antigüedad laboral
	Diseñadora multimedia	Secundario	2
	Sitio web de radio frecuencia	Secundario	2
	Administrador de seguridad informática BACSIRT	Secundario	3
Planta Técnica	Líder de Seguridad Informática	Universitario	2
	Analista Seguridad Informática Nivel 2	Terciario	3
	Administrador Seguridad Informática Nivel 2	Terciario	13
	Administrador Seguridad Informática Nivel 1	Secundario	3
	Analista Seguridad Informática Nivel 2	Terciario	3
	Analista Seguridad Informática Nivel 1	Terciario	3
	Analista Seguridad Informática Nivel 2	Universitario	2
	Analista Seguridad Informática Nivel 1	Secundario	3
	Analista Seguridad Informática Nivel 2	Universitario	12
	Analista Seguridad Informática Nivel 1	Terciario	3
	Líder de Seguridad Informática	Secundario	3
	Administrador Seguridad Informática Nivel 2	Universitario	3
	Administrador Seguridad Informática Nivel 2	Universitario	3
	Líder de Seguridad Informática	Universitario	3
	Líder de Seguridad Informática	Universitario	1
	Líder de Seguridad Informática	Universitario	4
	Operador de Seguridad Informática Nivel 2	Universitario	0

Situación de Revista	Función	Título alcanzado	Antigüedad laboral
	Administrador Seguridad Informática Nivel 1	Secundario	2
	Administrador Seguridad Informática Nivel 2	Secundario	4
	Administrador Seguridad Informática Nivel 2	Terciario	1
	Administrador Seguridad Informática Nivel 2	Universitario	1
	Administrador Seguridad Informática Nivel 2	Universitario	1
	Analista Seguridad Informática Nivel 1	Secundario	3

ANEXO II

Presupuesto 2019 - Distribución de Créditos - Agencia de Sistemas de Información

Presupuesto 2019 - Distribución de Créditos

Jur	SubJur.	Entidad	Descripción	Credito Sanción
21	0	270	AGENCIA SISTEMAS DE INFORMACION	1.345.344.758

ANEXO III

Presupuesto 2019 - Distribución de Créditos - Seguridad Informática

Presupuesto 2019 - Distribución de Créditos

Jur	SubJur.	Entidad	UE	Progra	SubProgr	Proyect	Actividad	Obra	Finalida	Fun	Descripción	Credito Sanción
21	0	270	8056	7	0	0	11000				SEGURIDAD INFORMÁTICA.	62.657.427
21	0	270	8056	7	0	0	11000	0	1		Administración Gubernamental	62.657.427
21	0	270	8056	7	0	0	11000	0	1	3	Direcoción ejecutiva	62.657.427

ANEXO IV

Presupuesto 2019 - Organismos Descentralizados, Entes Autárquicos, y Órganos de Control - Composición del Gasto por Jurisdicción, y Objeto del Gasto

Organismos Descentralizados, Entes Autarquicos y Organos de Control
Composición del Gasto por Jurisdicción, y Objeto del Gasto
(En Pesos)

INCISOS / JURISDICCION / ENTIDAD	PERSONAL	BIENES DE CONSUMO	SERV. NO PERSONALES	BIENES DE USO	TRANSFERENCIAS	ACTIVOS FINANCIEROS	SERVICIO DE LA DEUDA	OTROS GASTOS	EROGACIONES FIGURATIVAS	TOTAL GENERAL
AGENCIA SISTEMAS DE INFORMACION	271.432.566	3.962.880	903.014.056	166.935.256	0	0	0	0	0	1.345.344.758

ANEXO V

Presupuesto 2019 - Organismos Descentralizados, Entes Autárquicos, y Órganos de Control - Composición del Gasto por Finalidad y Función, y Entidad

Organismos Descentralizados, Entes Autarquicos y Organos de Control
Composición del Gasto por Finalidad y Función, y Entidad
(En Pesos)

ENTIDAD / FINALIDAD-FUNCION		AGENCIA SISTEMAS DE INFORMACION
Administración Gubernamental		**1.345.344.758**
Judicial		0
Dirección ejecutiva		1.338.081.742
Administración fiscal		0
Control de la gestión		7.263.016
Servicios de Seguridad		**0**
Seguridad pública		0
Servicios Sociales		**0**
Promoción y acción social		0
Educación		0
Cultura		0
Vivienda		0
Servicios Económicos		**0**
Ecología		0
Turismo		0
Servicios urbanos		0
TOTAL		**1.345.344.758**

ANEXO VI

Plan Plurianual de Inversiones Públicas 2019 - 2021

ADMINISTRACION DEL GOBIERNO DE LA CIUDAD DE BUENOS AIRES
PLAN PLURIANUAL DE INVERSIONES PUBLICAS 2019-2021
RESUMEN GENERAL
(en pesos)

Jur	Og	FF	Descripción	Inversión Total	Inversiones				Posteriores
					Anteriores	2019	2020	2021	
	270		AGENCIA SISTEMAS DE INFORMACION	1.326.773.433	755.144.990	571.628.443	0	0	0