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.