Marco Normativo de IT

PO0001 - Política Catálogo General

Gobierno de la Ciudad Autónoma de Buenos Aires

Política Catálogo General

1. Introducción

Un catálogo general tiene por finalidad, registrar, describir y ordenar una serie de temas que tienen algún punto en común. La presente política tiene como propósito, catalogar los documentos que conforman el Marco Normativo de TI, enumerando cada uno de ellos y exponiendo de manera concisa el contenido y codificación de los mismos.

2. Objetivo

Establecer la estructura, contenido y codificación de los documentos (política, procesos, procedimientos y estándares) que conforman el Marco Normativo de TI vigente en el GCABA.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

La *Política catálogo general* describe de forma sucinta cada una de las políticas que conforman el Marco Normativo de TI del GCABA y a partir del cual se irán actualizando e incorporando nuevos documentos a dicho marco.

El proceso de codificación y elaboración de nuevos documentos que pertenezcan al Marco Normativo de TI queda excluido de la presente política y deberá ajustarse a lo establecido en la *Política reguladora del marco normativo.*

Marco Normativo de TI

A continuación se resumen los documentos que conforman el Marco Normativo de TI, ordenados por dominio, exponiendo una breve descripción de su contenido y codificación:

0. Índice referencial

PO0001-Política catálogo general (pág. 1)
Descripción y codificación de cada uno de los documentos que forman parte del Marco Normativo de TI.

1. Política de seguridad de la información

Administrar la seguridad de la información dentro de la organización, estableciendo una estrategia y un marco gerencial para controlar su implementación.

PO0101-Política externa reguladora (pág. 9)
Exposición de criterios y lineamientos básicos a cumplir para la elaboración, codificación y contenido de los documentos que conformarán el Marco Normativo de TI.

PO0102-Política general de seguridad informática (pág. 14)
Documento de máxima relevancia que establece un marco general para instituir y mantener las políticas, procesos, procedimientos y estándares que definen las medidas de seguridad de la información a aplicar, de acuerdo con la normativa vigente.

2. Evaluación y tratamiento de riesgos

Identificar, cuantificar, y priorizar los riesgos de seguridad a los que se encuentra sometido el GCABA, definiendo cuáles deben ser las vías para determinar si serán aceptados, transferidos o mitigados.

PO0201-Política análisis de riesgos tecnológicos (pág. 20)
Definir y establecer los requisitos para la realización de evaluaciones de riesgos tecnológicos y la administración de los mismos dentro del ámbito del GCABA.

3. Organización de la seguridad

Administrar la seguridad de la información dentro de la organización, estableciendo una estrategia y un marco gerencial para controlar su implementación.

PO0301-Política de contratación de proveedores de TI (pág. 24)
Establecer las pautas que deben ser consideradas para toda adquisición de equipamiento, software, servicios, comunicaciones, telecomunicaciones y sistemas de información, debiendo garantizar su estandarización, interoperabilidad y seguridad.

4. Gestión de activos de Información

Alcanzar y mantener una adecuada protección de los activos, estableciendo roles y responsabilidades para la clasificación y tratamiento de los mismos. Cada Organismo clasificará la información de acuerdo a los criterios que establece el GCABA en sus políticas, contando para ello con la asistencia del Área de Seguridad Informática.

PO0401-Política de responsabilidades sobre la información (pág. 28)
Establecer los roles y responsabilidades de actuación, los actores que custodian, administran y salvaguardan de la información, así como los que autorizan el acceso; a través de una correcta asignación y una adecuada segregación de funciones.

PO0402-Política de clasificación de la información (pág. 34)
Establecer los criterios que se deben considerar para clasificar la información a fin de poder definir el nivel de criticidad de la misma y adoptar las medidas de protección y tratamiento adecuadas.

5. Seguridad de los recursos humanos

Asegurar que el personal de planta, personal con contrato de locación de servicio y proveedores, entiendan sus responsabilidades, sean adecuados a sus roles asignados y estén preparados para respaldar la Política General de Seguridad Informática.

A la fecha, el presente dominio no posee documentos asociados.

6. Seguridad física y del entorno

Impedir accesos físicos no autorizados, daños e interferencia a las instalaciones e información del GCABA.

PO0601-Política de seguridad física (pág. 40)
Definir las pautas generales de seguridad física que permitan asegurar la integridad de los recursos informáticos utilizados para el procesamiento, transmisión y resguardo de la información.

7. Gestión de las comunicaciones y operaciones

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, implementando y manteniendo un nivel de seguridad adecuado en la provisión de servicios y detectando las actividades de procesamiento de información no autorizadas.

PO0701-Política de copias de resguardo y recuperación (pág. 47)
Establecer los lineamientos para la generación, prueba y administración de copias de resguardo periódicas de la información, como así también los criterios básicos para su recuperación.

PO0702-Política de seguridad de las comunicaciones (pág. 54)

Asegurar una adecuada protección en los procesos de intercambio de información y de las comunicaciones del GCABA.

PO0703-Política de seguridad en redes (pág. 64)
Asegurar una adecuada protección de la información procesada en la red de datos del GCABA.

PO0704-Política de prevención de software malicioso (pág. 74)
Establecer los requerimientos que deben cumplir todos los equipos de procesamiento centralizado y estaciones de trabajo conectados a la red de comunicaciones del GCABA, de forma de garantizar la detección y eliminación de software malicioso (virus informáticos, troyanos, gusanos, malware en general; incluyendo código móvil), minimizando el riesgo de infección y propagación de los mismos.

PO0705-Política de instalación de estaciones de trabajo (pág. 79)
Establecer los lineamientos necesarios para regular el uso de las estaciones de trabajo, la instalación de software, hardware y responsabilidades de los agentes, cualquiera sea su función asignada.

PO0706-Política de uso de correo electrónico (pág. 84)
Establecer las pautas de comportamiento referidas a la utilización del servicio de Cuenta de Correo Electrónico Gubernamental (CCEG) por parte de los usuarios, de forma de garantizar una adecuada protección de la información y los recursos informáticos y prevenir el tráfico de spam en la red de comunicaciones del GCABA.

PO0707-Política de uso de Internet (pág. 88)
Establecer las pautas de comportamiento referidas a la utilización de Internet para un uso debido por parte de los usuarios conectados a la red de comunicaciones del GCABA, de forma de garantizar una adecuada protección de la información.

8. Control de accesos

Controlar los accesos a la información sobre la base de los requerimientos de seguridad y de los objetivos definidos por el GCABA. Los accesos serán otorgados sobre los principios de "mínimo privilegio" y "necesidad de conocer", aplicables a cada usuario.

PO0801-Política de uso de equipos portátiles (pág. 93)
Establecer los lineamientos de seguridad a implementar para el tratamiento de los equipos portátiles que procesan, almacenan información o requieran conexión a la red de comunicaciones del GCABA.

PO0802-Política de seguridad en dispositivos móviles (pág. 99)
Asegurar una adecuada protección de la información en los dispositivos móviles que se conectan a la red de comunicaciones, procesen o almacenen información del GCABA.

PO0803-Política de registro de eventos en servicios de TI (pág. 103)
Definir las pautas generales para asegurar una adecuada registración de eventos relacionados con los servicios de TI del GCABA, maximizando la trazabilidad de los mismos.

PO0804-Política de control de eventos en servicios de TI (pág. 108)
Definir las pautas generales para asegurar una adecuada identificación y seguimiento de los eventos en los servicios de TI registrados en los sistemas del GCABA. Asegurar que se registren y se evalúen todos los eventos significativos para la seguridad de accesos

PO0805-Política de administración de usuarios GCABA (pág. 113)
Establecer los lineamientos que permitan asegurar una adecuada administración de los usuarios del GCABA.

PO0806-Política de administración de usuarios en custodia (pág. 120)
Establecer las medidas de control para la utilización de usuarios en custodia, de manera que los mismos sean utilizados solo en situaciones de emergencia que lo ameriten.

PO0807-Política de administración de contraseñas (pág. 125)
Asegurar una adecuada administración (generación, modificación, utilización y almacenamiento) de las contraseñas de los usuarios del GCABA.

PO0808-Política de administración de accesos a software de aplicación (pág. 131)
Establecer los lineamientos que permitan asegurar una adecuada administración de los accesos de usuarios al software de aplicación del GCABA.

PO0809-Política de administración de accesos a recursos de infraestructura de TI (pág. 136)
Establecer los lineamientos que permitan asegurar una adecuada administración de los accesos de usuarios a los recursos de infraestructura de TI del GCABA.

PO0810-Política de accesos remotos (pág. 141)
Establecer los aspectos de seguridad y reglas a cumplir al acceder a la red de comunicaciones del GCABA de forma, a fin de garantizar una adecuada protección de la información y los recursos informáticos de la misma.

9. Adquisición, desarrollo y mantenimiento de sistemas de información

Garantizar que la seguridad sea una parte integral del ciclo de vida de los sistemas de información, previniendo errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

PO0901-Política de separación de ambientes de TI (pág. 145)
Establecer los lineamientos y las pautas generales para garantizar una adecuada separación de ambientes de procesamiento de la información del GCABA, definiendo las características de los ambientes y asegurando una apropiada segregación de funciones y limitaciones de acceso.

PO0902-Política de control de cambios (pág. 152)
Establecer los controles que deberán realizarse en el proceso de cambios de software de aplicación, software de base, información e infraestructura tecnológica de los ambientes, de manera de

asegurar su integridad y minimizar el riesgo de pérdida de información, accesos no autorizados o falta de disponibilidad del servicio.

10. Gestión de incidentes de seguridad de la información

Asegurar que se aplique un proceso de mejora continua para la gestión de los incidentes de seguridad de la información, garantizando que los eventos sean registrados y comunicados de forma correcta y oportuna.

PO1001-Política de respuesta ante incidentes de TI (pág. 158)
Establecer lineamientos que permitan corregir con la máxima celeridad posible, las consecuencias y efectos negativos de los incidentes de los servicios de TI, a fin de minimizar su impacto.

11. Gestión de la continuidad de las actividades

Desarrollar e implementar planes de continuidad que aseguren la reanudación oportuna de las operaciones esenciales. Contrarrestar las interrupciones de las operaciones y proteger los procesos críticos del GCABA.

A la fecha, el presente dominio no posee documentos asociados.

12. Cumplimiento

Impedir infracciones y violaciones a cualquier obligación legal, reglamentaria, reguladora o contractual, así como a cualquier requerimiento de seguridad. Garantizar el cumplimiento de las políticas, procesos, procedimientos y estándares de seguridad del GCABA.

PO1201-Política de licencias y legalidad de software (pág. 162)
Establecer los lineamientos necesarios para asegurar que todo software que sea utilizado por el personal del GCABA en el desarrollo de sus tareas (tanto adquirido como desarrollado internamente) tenga la licencia de uso legal correspondiente.

13. Glosario

PO1301-Política glosario de términos y definiciones (pág. 166)
Términos empleados en la redacción dentro del contexto del marco normativo de TI.

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a la *información digital* sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0101 - Política Externa Reguladora

Gobierno de la Ciudad Autónoma de Buenos Aires

Política Externa Reguladora del Marco de TI

1. Introducción

Los criterios de elaboración de los documentos que conforman el Marco Normativo de TI se basan en el establecimiento de unas reglas claras considerando su tipología y el ciclo de vida de dichos documentos.

2. Objetivo

La presente política tiene por objeto establecer la codificación y los criterios que se utilizarán para elaborar las Políticas, Procesos, Procedimientos y Estándares que conforman el Marco Normativo de TI vigente en el GCABA.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

A continuación se resumen los criterios a adoptar para la redacción del los documentos que conformarán el Marco Normativo de TI vigente en el GCABA:

a. Tipología de los documentos

Política General

Documento de máxima relevancia que define las competencias y actuaciones, cumpliendo una función coordinadora, orientadora y reguladora. Por su carácter estratégico y como medio para proteger la información, posee un interés prioritario y el máximo apoyo por parte de la ASI, estableciendo los controles necesarios a fin de garantizar la seguridad de la información que genera, procesa y almacena el GCABA.

La Política General define una serie de interrogantes, que necesariamente deben estar incluidos en su enunciado:

Qué es lo que se pretende proteger (objetivo).

Alcance e impacto (a quiénes aplica).

Sobre quiénes recae su ejecución (responsabilidades).

ANEXO I

Política

Disposiciones que soportan los objetivos recogidos en la Política General y concretan las orientaciones, competencias y regulaciones específicas indicadas en la misma. Las Políticas abarcan la definición de los roles y responsabilidades de actuación en la gestión de TI y seguridad de la información, tanto para el personal interno como externo al GCABA.

Proceso

Conjunto estructurado de actividades diseñado para la consecución de un objetivo determinado. Los Procesos requieren de una o más entradas y producen una serie de salidas, ambas previamente definidas. Un Proceso suele incorporar la definición de los roles que intervienen, las responsabilidades, herramientas, regulaciones y controles de gestión necesarios para obtener las salidas de forma eficaz. El Proceso podrá definir las Políticas, Procedimientos, Estándares, así como las actividades y las instrucciones de trabajo que fueran necesarias.

Procedimientos

Los procedimientos establecen en detalle, los pasos necesarios a seguir a efectos de realizar una determinada tarea y así cumplir con uno o varios objetivos de control. Los procedimientos:

Deben referenciar a una política.

Deben ser auditables, es decir, deben dejar evidencias de cumplimiento.

Deben ser ejecutados por personas, identificando responsables.

Pueden referenciar a otros procedimientos (procedimientos anidados).

Pueden referenciar a un estándar.

Estándares

Los estándares definen un conjunto de criterios y/o especificaciones orientados a cumplimentar los objetivos de control del marco normativo en un ámbito de aplicación concreto. Los estándares:

Constituyen un marco de referencia dentro del ámbito de aplicación.

Son de obligado cumplimiento.

Si son tecnológicos no deben corresponderse con un fabricante específico.

Ciclo de vida de los documentos

ANEXO I

b. Ciclo de vida de la documentación

Las responsabilidades que a continuación se describen se refieren específicamente al ciclo de vida de toda la documentación que formará parte del Marco Normativo de TI del GCABA.

Elaboración

Corresponde a las *Direcciones Generales* y a las *Gerencias Operativas* dependientes de la ASI, velar por la seguridad de la información, proponiendo, elaborando, revisando y manteniendo de forma estricta el Marco Normativo de TI, con el objeto de garantizar el cumplimiento de dicha premisa en el ámbito del GCABA.

Publicación, distribución y custodia

La *ASI* será la encargada de promover la publicación y distribución del Marco Normativo de TI aprobado, a todo el personal afectado. Una vez publicado y distribuido cada documento, quedará bajo la custodia de las *Direcciones Generales* y las *Gerencias Operativas* que corresponda.

Control del cumplimiento

Cada *dependencia* será responsable de controlar el cumplimiento del Marco Normativo de TI dentro de su ámbito.

Corresponde a la *Gerencia Operativa de Seguridad Informática o Equivalente* monitorear el cumplimiento del Marco Normativo de TI, de acuerdo con sus objetivos de control en materia de seguridad de la información.

Corresponde a *Sindicatura General* verificar el cumplimiento de la Normativa vigente, detectando, reportando y proponiendo mejoras en su contenido, fruto de las auditorías realizadas.

Actualización

Toda la documentación podrá revisarse y actualizarse cuando se considere necesario. Dicha revisión se planificará en función de su antigüedad, grado de obsolescencia, acciones correctivas en curso y observaciones recibidas. Se evitará mantener en vigor documentos no revisados de más de tres años de antigüedad. El deber de dicha actualización recaerá en la *ASI*.

Será responsabilidad de cada dependencia, mantener actualizados en todo momento aquellos Procedimientos y Estándares alineados con el Marco Normativo de TI de la ASI.

ANEXO I

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a la *información digital* sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0102 - Política General de Seguridad Informática

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política General de Seguridad Informática

1. Introducción

La información hoy en día, es un bien valioso que brinda grandes beneficios en términos de intereses políticos, objetivos de gestión y ayuda en la toma de decisiones.

La información digital puede presentarse de diversas formas y en diferentes contextos como es la información almacenada en soportes electrónicos, transmitida por correo o publicada en redes sociales, representada en imágenes, o expuesta en una conversación telefónica. En este sentido, cualquiera sea el modo en el que se manifieste, almacene o comunique, debe ser debidamente protegida, dado que representa un patrimonio para el Poder Ejecutivo del GCABA (en adelante GCABA).

La seguridad protege a la información de una amplia variedad de amenazas, con el objeto de asegurar la continuidad de las actividades, minimizar los riesgos y maximizar la calidad en la entrega de los servicios de tecnología informática.

Esto se logra implementando un conjunto adecuado de controles, que incluye políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware, los cuales se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, a fin de garantizar que se alcancen los objetivos del GCABA.

Es importante que los principios de la Política General de Seguridad Informática formen parte de la cultura organizacional, a fin de facilitar su efectivo cumplimiento.

2. Objetivo

La presente Política General de Seguridad Informática tiene por objetivo constituir un marco general para establecer y mantener las políticas, procesos, procedimientos y estándares que definen las medidas de seguridad informática a aplicar en el GCABA, de acuerdo con la normativa vigente.

3. Ámbito de aplicación

La Política General de Seguridad Informática, así como el resto de políticas enmarcadas dentro de la normativa vigente, se aplica con carácter obligatorio a todo al ámbito del GCABA, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la organización a través de contratos o acuerdos con terceros. Abarca toda la información digital utilizada por el GCABA para el desarrollo de sus actividades y los sistemas de información que la soportan.

4. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

ANEXO I

5. Contenido

Principios Fundamentales

La Política General de Seguridad Informática vela por la seguridad de todos sus procesos, siendo ésta de aplicación en todas las fases de su ciclo de vida: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción, así como de los sistemas que los soportan: análisis, diseño, desarrollo, pruebas, homologación, producción; operación y mantenimiento.

La ASI adoptará acciones tendientes a preservar en cada momento las tres componentes básicas de la seguridad de la información:

- CONFIDENCIALIDAD: garantizar que a la información y a los sistemas de información solo accedan personas debidamente autorizadas.
- INTEGRIDAD: garantizar la exactitud de la información y de los sistemas de información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- DISPONIBILIDAD: garantizar que la información y los sistemas de información pueden ser utilizados en la forma y tiempo requeridos.

Sobre estos tres pilares, el GCABA cimienta su Política General en materia de Seguridad Informática, dado que son vitales para la gestión de gobierno, la imagen social y la calidad en la atención de los ciudadanos.

Adicionalmente, se adoptarán conductas destinadas a garantizar el cumplimiento de los principios que se detallan a continuación:

- AUTENTICACIÓN: Establecer la identidad del usuario y asegurar que éste sea quién dice ser.
- TRAZABILIDAD: Asegurar que cualquier acción o transacción pueda ser relacionada unívocamente asegurando el cumplimiento de controles claves establecidos en las correspondientes políticas, así como el almacenamiento en un histórico para posibles inspecciones legales.
- LEGALIDAD: Garantía de que la información organizacional cumple con las leyes, reglamentaciones y disposiciones vigentes.

Implementación del Marco Normativo de IT

El conjunto de documentos incluidos en el Marco Normativo de IT se definen e implementan en base a diferentes dominios de seguridad, sobre los cuales también se funda la presente Política General de Seguridad Informática:

ANEXO I

a. Organización de la seguridad

Administrar la seguridad de la información dentro de la organización, estableciendo una estrategia y un marco gerencial para controlar su implementación.

Corresponden a este dominio los siguientes documentos: *Política de contratación de proveedores de TI.*

b. Evaluación y tratamiento de riesgos

Identificar, cuantificar, y priorizar los riesgos de seguridad a los que se encuentra sometido el GCABA, definiendo cuáles deben ser las vías para determinar si serán aceptados, transferidos o mitigados.

c. Gestión de activos de Información

Alcanzar y mantener una adecuada protección de los activos, estableciendo roles y responsabilidades para la clasificación y tratamiento de los mismos. Cada Organismo clasificará la información de acuerdo a los criterios que establece el GCABA en sus políticas, contando para ello con la asistencia del Área de Seguridad Informática.

Corresponden a este dominio los siguientes documentos: *Política de responsabilidades sobre la información, Política de clasificación de la información y Procedimiento de clasificación de la información.*

d. Seguridad de los recursos humanos

Asegurar que el personal de planta, personal con contrato de locación de servicio y proveedores, entiendan sus responsabilidades, sean adecuados a sus roles asignados y estén preparados para respaldar la Política General de Seguridad Informática.

e. Seguridad física y del entorno

Impedir accesos físicos no autorizados, daños e interferencia a las instalaciones e información del GCABA.

Corresponden a este dominio los siguientes documentos: *Política de seguridad física.*

f. Gestión de las comunicaciones y operaciones

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, implementando y manteniendo un nivel de seguridad adecuado en la provisión de servicios y detectando las actividades de procesamiento de información no autorizadas.

ANEXO I

Corresponden a este dominio los siguientes documentos: *Política de copias de resguardo y recuperación, Política de seguridad de las comunicaciones, Política de seguridad en redes, Política de prevención de software malicioso, Política de instalación de estaciones de trabajo, Política de uso de correo electrónico y Política de uso de Internet.*

g. Control de accesos

Controlar los accesos a la información sobre la base de los requerimientos de seguridad y de los objetivos definidos por el GCABA. Los accesos serán otorgados sobre los principios de "mínimo privilegio" y "necesidad de conocer", aplicables a cada usuario.

Corresponden a este dominio los siguientes documentos: *Política de administración de portátiles, Política de seguridad en dispositivos móviles, Política de registro de eventos de TI, Política de control de eventos de TI, Política de administración de usuarios GCABA, Política de administración de usuarios en custodia, Política de administración de contraseñas, Política de administración de accesos a software de aplicación, Política de administración de accesos a infraestructura de TI y Política de accesos remotos.*

h. Adquisición, desarrollo y mantenimiento de sistemas de información

Garantizar que la seguridad sea una parte integral del ciclo de vida de los sistemas de información, previniendo errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

Corresponden a este dominio los siguientes documentos: *Política de separación de ambientes y Política de control de cambios en homologación y producción.*

i. Gestión de incidentes de seguridad de la información

Asegurar que se aplique un proceso de mejora continua para la gestión de los incidentes de seguridad de la información, garantizando que los eventos sean registrados y comunicados de forma correcta y oportuna.

Corresponden a este dominio los siguientes documentos: *Política de respuesta ante incidentes de TI.*

j. Gestión de la continuidad de las actividades

Desarrollar e implementar planes de continuidad que aseguren la reanudación oportuna de las operaciones esenciales. Contrarrestar las interrupciones de las operaciones y proteger los procesos críticos del GCABA.

ANEXO I

k. Cumplimiento

Impedir infracciones y violaciones a cualquier obligación legal, reglamentaria, reguladora o contractual, así como a cualquier requerimiento de seguridad. Garantizar el cumplimiento de las políticas, procesos, procedimientos y estándares de seguridad del GCABA.

Corresponden a este dominio los siguientes documentos: *Política de licencias y legalidad de software.*

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0201 - Política de Análisis de Riesgos Tecnológicos

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Análisis de Riesgos Tecnológicos

1. Introducción

La *información* es un recurso de vital importancia para el funcionamiento del Poder Ejecutivo del GCABA (en adelante GCABA) y por consiguiente debe ser debidamente protegida a través de mecanismos de seguridad (lógica y física). Dichos mecanismos se establecen adecuadamente a partir de un análisis de riesgos.

2. Objetivo

Definir y establecer los requisitos para la realización de evaluaciones de riesgos tecnológicos y la administración de los mismos dentro del ámbito del GCABA.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

La ASI tiene como objetivo organizar y coordinar la infraestructura tecnológica y los sistemas de información que se utilizan en la administración pública del GCABA. Para cumplir con esta premisa, la ASI podrá realizar evaluaciones de riesgos cuando lo considere necesario, estableciendo las siguientes pautas:

Roles y Responsabilidades

La ASI podrá solicitar revisiones periódicas de los riesgos de seguridad y de las salvaguardas implementadas a fin de:

a. reflejar los cambios en los requerimientos y prioridades del GCABA;
b. considerar nuevas amenazas y vulnerabilidades;
c. corroborar que las salvaguardas siguen siendo eficaces y apropiadas.

Las revisiones podrán llevarse a cabo con diferentes niveles de profundidad según los resultados de evaluaciones anteriores y los niveles variables de riesgo que la ASI está dispuesta a aceptar.

La Gerencia Operativa de Seguridad Informática o Equivalente será la responsable de establecer los controles o mecanismos de salvaguarda, de acuerdo al grado de exposición a potenciales riesgos de los

procesos, activos de información, aplicaciones, software base, equipamiento, redes de comunicaciones e instalaciones dentro del ámbito del GCABA.

Asimismo, la Gerencia Operativa de Seguridad Informática o Equivalente será la responsable de realizar la ejecución de dichos análisis de riesgos y reportar los resultados a la Dirección Ejecutiva de la ASI.

Metodología

La metodología de evaluación de riesgos adoptada por la ASI es una consideración sistemática de los siguientes puntos:

a. Establecimiento de un *inventario o árbol de activos tecnológicos*. El mismo será actualizado ante cualquier modificación de la información registrada.
b. Valoración cualitativa de los *activos* de dicho *inventario tecnológico*.
c. Impacto potencial de una falla de seguridad en la administración de los recursos del GCABA, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información;
d. Probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominantes, la posibilidad de propagación de dichas amenazas sobre los recursos del GCABA y los controles actualmente implementados.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la implementación de los controles o salvaguardas seleccionadas a fin de brindar protección contra dichos riesgos.

Los controles o salvaguardas se seleccionarán teniendo en cuenta el costo de implementación en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad. Asimismo la ASI podrá considerar otros factores no monetarios, como el daño en la reputación o en la imagen del GCABA.

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a la información digital sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se

resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0301 - Política de Contratación de Proveedores de TI

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Contratación de Proveedores de TI

1. Introducción

Las compras y contrataciones de TI constituyen un factor clave para que los organismos del GCABA puedan cumplir con sus misiones. Por esta razón, y dada la gran incidencia que las adquisiciones de TI tienen en el GCABA, resulta crucial que se promueva la transparencia en esos procedimientos, no sólo para resguardar los activos de información y asegurar la confidencialidad sobre la información del GCABA, sino también optimizar el gasto y utilizar más eficientemente los recursos informáticos.

En este contexto, la ASI interviene en procedimientos de adquisiciones y propone lineamientos generales para mejorar la transparencia en los procesos de compras y contrataciones públicas de proveedores de TI, en concordancia con la normativa vigente y sus decretos relacionados.

2. Objetivo

Establecer las pautas que deben ser considerados para toda adquisición de equipamiento, software, servicios, comunicaciones, telecomunicaciones y sistemas de información, debiendo garantizar su estandarización, interoperabilidad y seguridad.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Contrataciones que deben ser aprobadas por la ASI

Se deberá contar con la conformidad expresa de la ASI, para:

a. La adquisición de bienes y servicios informáticos que superan los montos establecidos en el decreto 1036/GCBA/08, en la resolución 44/ASINF/08 y sus modificatorias.

b. La contratación de servicios de transmisión de datos, por medios tales como enlaces punto a punto, internet, banda ancha, fibra óptica, 3G, ADSL y/o cualquier otro que se emplee con dicha finalidad.

ANEXO I

Contrataciones de los organismos del GCABA gestionadas por la ASI

La ASI podrá gestionar las contrataciones que sean requeridas por los Organismos del GCABA. A fin de permitir la correcta elaboración de las especificaciones técnicas, el Organismo solicitante deberá informar a la ASI en forma clara, lo siguiente:

a. Características del servicio;

b. Si los elementos deben ser nuevos, usados o reacondicionados;

c. Si se aceptarán tolerancias, y en su caso, en qué medida;

d. La calidad exigida, y en su caso, las normas de calidad que deben cumplir los bienes o servicios a satisfacer por los proveedores;

e. La exigencia de marca, debidamente justificadas, si corresponde.

Ante cualquier compra requerida a la ASI, esta podrá solicitar una transferencia presupuestaria del organismo solicitante.

Contrataciones gestionadas por los Organismos

La ASI pondrá a disposición de los Organismos los modelos para la elaboración de los pliegos de Especificaciones Técnicas, los cuales deberán ser enviados para la evaluación y autorización de la ASI.

Las especificaciones técnicas podrán formularse en términos de rendimiento o de requisitos funcionales que permitan acuerdos por niveles de servicio. Tales requisitos deberán ser lo suficientemente precisos para permitir a los oferentes determinar el objeto del contrato.

Condiciones generales para la contratación

Sin prejuicio de las obligaciones previstas por las normativas vigentes y sus decretos relacionados con compras y contrataciones, toda documentación contractual deberá contemplar:

a. La definición los niveles de servicio, indicando la disponibilidad del servicio prestado, y los tiempos de respuesta esperados.

   Deberán contar con planes de contingencias para asegurar la continuidad del servicio que presta, y comprometerse a la entrega de documentación de respaldo de los mismos a requerimiento de la ASI.

b. Para el software desarrollado o modificado específicamente para el *GCABA* por un proveedor, la ASI deberá mantener en su poder una copia actualizada del programa en código fuente.

c. El plazo de preaviso de rescisión de contratos por parte del proveedor, debe estar en concordancia con el tiempo estipulado por la normativa vigente del GCABA.

d. La confidencialidad de la información y datos inherentes a la tarea que desarrolla, tanto durante la vigencia del contrato como después, obligándose a no divulgar, revelar ni transmitir a terceros a la contratación.

e. La garantía técnica de funcionamiento y mantenimiento correctivo integral, por el término definido por la ASI y establecido según el caso particular, la que debe cubrir cada componente o adaptación solicitada e implementada en producción.

f. La obligación del proveedor a responder por el personal que afecte al trabajo, servicio u obra, como así también por el personal que afecte el subcontratista con quien el adjudicatario contrata la realización de cualquier tarea.

La ASI, en su carácter de órgano rector en materia de tecnología y comunicaciones podrá realizar un análisis de riesgo previo a la asignación de actividades al tercero, que evidencie los expuestos a los que se verá sometido el GCABA e identifique las medidas requeridas para minimizarlos.

El proveedor que va a prestar un servicio de TI al GCABA debe estar en conocimiento de las políticas, estándares y procedimientos definidos por la ASI y realizar sus tareas en cumplimiento de las mismas.

Generalidades

La ASI podrá determinar las acciones a tomar en el caso de incumplimiento a los puntos de la presente política una vez evaluadas las consecuencias, que sobre los recursos y servicios informáticos del *GCABA* se haya podido ocasionar. Todo ello sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas presuntamente implicadas en dicho incumplimiento.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe y de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0401 - Política de Responsabilidades sobre la Información

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Responsabilidades sobre la Información

1. Introducción

La *información* es un recurso de vital importancia para el funcionamiento del Poder Ejecutivo del GCABA (en adelante GCABA) y por consiguiente debe ser debidamente protegida a través de mecanismos de administración y control de seguridad (lógica y física). Por esta razón deben establecerse las diversas responsabilidades que permitan brindar una adecuada protección a la misma.

2. Objetivo

Asegurar adecuadamente la custodia y salvaguarda de la *información*, así como también la administración de la seguridad de los accesos a los recursos que la contienen, a través de una correcta asignación de responsabilidades y teniendo en cuenta una adecuada segregación de funciones.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Para una adecuada protección de la *información* del *GCABA* se establecen las responsabilidades que se detallan a continuación:

Roles Funcionales Relacionados con el Acceso a la Información

a. Propietario

Son funcionarios a los que se les ha asignado la responsabilidad de la gestión y utilización de una *información* en particular.

Los *Propietarios* serán los funcionarios a cargo de las diferentes unidades organizacionales de cada Organismo, actuando conjuntamente con sus respectivas gerencias operativas (*Referentes de la Información*). Estas responsabilidades no pueden ser delegadas en proveedores externos al GCABA.

El Propietario tendrá a su cargo lo siguiente:

- Conocer como se usa la información bajo su responsabilidad, dentro y fuera del Organismo; entendiendo también los riesgos y problemas potenciales a los que está expuesta la información y actuando en consecuencia para minimizar el grado de exposición de la misma.
- Clasificar la información basándose en su criticidad. Las escalas de criticidad no son desarrolladas por el *Propietario*, sino por la *Gerencia Operativa de Seguridad Informática o Equivalente* de acuerdo con la *Política de Clasificación de la Información*.
- Documentar y actualizar periódicamente la clasificación de la información efectuada.
- Aprobar todos los requisitos de acceso a la información de la que ha sido designado el Propietario, según el criterio de clasificación; garantizando que sólo puedan acceder los *Agentes del GCABA* autorizados o externos al GCABA, según sea el caso.
- Autorizar toda acción relacionada con el ciclo de vida de la información que le ha sido designada bajo su responsabilidad.
- Velar por la integridad de la información de la cual es responsable.
- Mantener un adecuado registro de los *Agentes del GCABA* con permisos para acceder a su información.
- Garantizar el cumplimiento irrestricto de lo dispuesto por las Leyes N° 1845 y N° 104.
- Tomar conocimiento y participar activamente en la investigación de los incidentes relativos a la seguridad de la información bajo su responsabilidad.
- Solicitar la baja inmediata del acceso a la información cuando la misma ya no deba ser accedida, se sospeche de una violación de seguridad o deje de ser relevante.

Los *Propietarios* podrán asignar un *usuario* colaborador idóneo a su cargo (*Referente de la Información*) para la administración de sus funciones. Sin embargo la responsabilidad del cumplimiento de las mismas será siempre del *Propietario*. La asignación de tareas de administración por parte de los *Propietarios* a los Referentes deberá ser documentada y expresamente comunicada a la *ASI.*

b. Custodio

Tiene la posesión de la información y administra técnicamente los sistemas que utilizan esta información. Este rol comúnmente es asignado a los Administradores de Sistemas, Administradores de Bases de Datos, Personal de Microinformática, Personal de Centros de Procesamiento de Datos y Centros de Almacenamiento de Copias de Resguardo, entre otros.

El Custodio de la Información será responsable de:

- Salvaguardar el almacenamiento y procesamiento seguro de la información, como puede ser el resguardo diario de la información y la administración de los sistemas de control de accesos.
- Cumplir las instrucciones del Propietario y los requisitos de la Política General de Seguridad Informática.
- Gestionar diariamente la información que le ha sido encomendada, incluyendo el soporte técnico.
- Informar periódicamente al Propietario sobre todos los accesos a la información en cuestión.
- Proveer asesoramiento técnico sobre las mejores formas de proteger la confidencialidad, integridad y disponibilidad de la información.
- Informar de forma inmediata al *Propietario* y a la *Gerencia Operativa de Seguridad Informática o Equivalente,* cualquier incidente o sospecha de violación de acceso a la información.

c. Usuario

El usuario es toda persona que tiene acceso a la información y/o sistemas del GCABA. Podrá ser personal de planta, personal con contrato de locación de servicio o proveedor. Sus privilegios deberán ser revocados cuando cambie o se acabe la necesidad de contar con dichos accesos.

Es Usuario será responsable de:

- Solicitar al correspondiente Propietario los accesos a información y sistemas.
- Abstenerse de transferir o usar la información del GCABA para cualquier otro propósito que el autorizado por parte del Propietario o por su superior inmediato.
- Manejar de forma segura la información en su posesión, incluyendo el hecho de mantener en secreto sus claves de acceso, manipular de forma segura la información sensible de copias de papel, información en medios extraíbles, información transmitida verbalmente, etc.
- Informar, al Propietario, los errores o anomalías en la información a la cual tienen acceso. Será considerado una falta grave, el intentar aprovecharse de errores, anomalías o vulnerabilidades para ganar acceso a sistemas.

Responsabilidades Relacionadas con la Estructura Organizativa

a. Agencia de Sistemas de Información (ASI)

La *ASI* tiene como objetivo organizar y coordinar la infraestructura informática de telecomunicaciones y los sistemas informáticos que se utilizan en la administración pública del *GCABA*.

ANEXO I

Se definen las principales funciones que desempeña la *ASI* relacionadas con la protección de la *información* del *GCABA*:

a. Verificar el cumplimiento de las políticas, procedimientos y controles establecidos.

b. Definir procedimientos para el control de cambios a los *sistemas informáticos* y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

c. Establecer criterios de aprobación para nuevos *sistemas informáticos*, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva.

d. Definir procedimientos para el manejo de *incidentes* de seguridad y para la administración de los medios de almacenamiento.

e. Desarrollar procedimientos de concientización para los *Agentes* del *GCABA* en materia de seguridad, controles de acceso a los *sistemas informáticos* y administración de cambios.

f. Controlar los mecanismos de distribución y difusión de *información* dentro del *GCABA*.

g. Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra *software malicioso* y para garantizar la seguridad de los datos y los *servicios* conectados en la red de comunicaciones del *GCABA*.

h. Implementar las medidas de seguridad física definidas para la protección de la *información* del *GCABA*.

i. Disponer la efectiva custodia de las claves de mayor riesgo de los equipos/ *servicios*/ *software de aplicación*.

j. Efectuar el control de los principales eventos que afecten la seguridad de la *información* y la posterior comunicación y asistencia a los *Propietarios* mediante:

    - La identificación del problema,
    - El análisis de las consecuencias,
    - Las medidas a considerar para su resolución.

La *ASI* podrá asistir a los *Agentes* de los *Organismos* en materia de seguridad de la *información*. Asimismo, junto con los *Propietarios*, analizará el riesgo de los accesos de terceros a la *información* y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma**.**

ANEXO I

b. Control Interno

La Sindicatura General del GCABA y las Unidades de Auditoría Interna de cada jurisdicción, actuando como órganos del sistema de Control Interno del GCABA, serán responsables por la fiscalización de las políticas establecidas por la ASI. Todo esto se realizará respetando las competencias que le son propias, según la normativa vigente.

c. Agentes del GCABA

Los *Agentes* del *GCABA,* son responsab*les de cono*cer, cumplir y hacer cumplir las políticas, procedimientos y estándares vigentes relacionados con la seguridad de la *información*.

Se definen las principales responsabilidades de los *agentes* respecto a la protección de la información:

a. Velar por la confidencialidad, operatividad, integridad y exactitud de todo soporte físico y/o de salvaguarda de *información*, *software de aplicación, software utilitario* y/o *software de base* que utilizan para la realización de sus tareas diarias.

b. Informar a la *ASI* sobre toda exposición no autorizada de *información digital* del *GCABA*.

c. No introducir ni extraer *información* de los *sistemas informáticos* del *GCABA* por vías no autorizadas, esto incluye todo tipo de *software* ilegal o copias no autorizadas de *software* legal.

d. Participar en las pruebas de los nuevos *sistemas informáticos* y/o modificaciones sobre los sistemas vigentes.

e. Respetar el Compromiso de Confidencialidad de la *información* asumido por el *Organismo* en el cual se desempeña.

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a la información digital sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0402 - Política de Clasificación de la Información

Gobierno de la Ciudad Autónoma de Buenos Aires

Política de Clasificación de la Información

1. Introducción

La *información* adopta muchas formas, tanto en los *sistemas informáticos* como fuera de ellos. Puede ser almacenada, transmitida e impresa o escrita en papel. Para todas estas formas deben contemplarse las medidas necesarias para alcanzar un grado razonable de protección Para ello se realiza la clasificación de la información desde el punto de vista de la confidencialidad, integridad y disponibilidad, a fin de obtener una serie de valores que permitirán justificar cuáles serán las medidas de tratamiento a aplicar para garantizar una adecuada protección, como por ejemplo preservar la confidencialidad de aquella información que está fuera del alcance público, mediante mecanismos de cifrado.

2. Objetivo

Establecer los criterios que se deben considerar para clasificar la *información* del *GCABA* a fin de poder definir el nivel de criticidad de la misma y adoptar las medidas de protección y tratamiento adecuadas.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Los *Propietarios,* o quienes éstos designen, son los encargados de clasificar la *información* de acuerdo con su nivel de criticidad (en términos de confidencialidad, integridad y disponibilidad), de documentar y mantener actualizada la clasificación efectuada y establecer los permisos de acceso en función de los niveles establecidos.

La *ASI* establece los lineamientos para que los *activos de información* utilizados contemplen los requerimientos de seguridad establecidos según la criticidad de la *información* que procesan.

El proceso de clasificación de la *información* deberá ser cumplimentado de acuerdo a lo establecido en la presente Política.

ANEXO I

Inventario de activos

El *Propietario* identificará los *Activos de Información* que pertenecen a su dominio, su respectivo código, tipología, administrador, etc., para luego elaborar un inventario básico con dicha información. El mismo será actualizado ante cualquier modificación de la información registrada.

Para el inventario de activos se deberá considerar como mínimo los atributos básicos del activo, pudiendo incorporar si fuese necesario atributos extendidos, de acuerdo al tipo de activo (Ej. ubicación física, licencia, subtipo, etc.).

Los atributos básicos para la confección del inventario de activos son los siguientes:

a. Código de Identificación del Activo (código alfanumérico asignado).

b. Tipo de Activo (*información, sistema de información, funcionalidad, intangible, entorno*).

c. Organismo o Dependencia del Activo (datos para su gestión interna).

d. Responsable del Activo (nombre o cargo de quién cumple el rol).

e. Administrador del Activo (nombre o cargo de quién cumple el rol).

f. Estado (*prueba, producción, eliminable, etc.*)

Tipología de Activos

A continuación se describen los tipos de *Activos* que se pueden encontrar dentro del GCABA:

a. *Información: Abarca datos, meta-información y soportes.* Ej.: Datos capturados, datos informatizados, datos resultantes, otros datos, documentación de desarrollo, documentación de sistemas, claves de cifrado, código fuente, estructuras de datos, formatos de datos, modelos de datos, documentación en general, soportes de información.

b. *Sistema de información: Abarca comunicaciones, hardware y software.* Ej.: Componentes de conexión, redes propias, servicios de comunicaciones, otro comunicaciones, hardware de almacenamiento, dispositivos móviles, hardware de procesamiento, otro hardware, servidores, servidor de red, aplicaciones propias, aplicaciones adquiridas, paquetes de software, software de base, sistema gestor de Base de Datos.

c. *Funcionalidad: Usuarios y terceros, estrategia, gestión de IT, gestión de seguridad, políticas, normativas, procedimientos, productos y administración.* Ej.: Usuarios, procesos de gestión del organismo, gestión de tecnología, gestión de operaciones, estrategia de IT, control de cambios, gestión de accesos, gestión de desarrollo, gestión de seguridad de la información, política de

seguridad, marco normativo de seguridad, plan de continuidad de las operaciones, plan de contingencia, bienes, servicios, gestión de RRHH.

d. *Intangible: Aspectos legales y regulatorios, imagen, integridad, intimidad, conocimiento, independencia.* Ej.: Cumplimiento de leyes y regulaciones, contratos o acuerdos, credibilidad ética, credibilidad jurídica, imagen, integridad física de personas, intimidad de personas, conocimiento acumulado, independencia de actuación, independencia de criterio.

e. *Entorno: Abarca equipamientos, suministros, otros tangibles y personal.* Ej.: climatización, energía, medios de comunicación, edificaciones, instalaciones físicas, mobiliario informático, personal de desarrollo, personal de dirección, personal de operación, otro personal.

Podrán declararse dependencias funcionales entre activos (árbol de activos), dado que no todos los activos poseen la misma jerarquía dentro del inventario (Ej. información procesada en un servidor, que a su vez contiene una aplicación que depende de una o varias bases de datos para funcionar).

La declaración explícita de las relaciones que existen entre los activos del inventario, se establece mediante dependencias del tipo "padre – hijo" donde el hijo da servicios al padre, o el padre depende del hijo para poder funcionar.

Clasificación de la Información

La clasificación de la *información* se realizará mediante el empleo de un método cualitativo que permite establecer valores normalizados (0, 1, 2, 3).

Los *activos de información* se clasificarán de acuerdo con lo siguiente esquema:

a. Nivel de Confidencialidad: La confidencialidad previene la divulgación no autorizada de información.

    0. PUBLICA: *Información* que puede ser conocida y utilizada sin autorización por cualquier persona.

    1. USO INTERNO: *Información* que puede ser conocida y utilizada por todos los *Agentes* del *GCABA* y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar pérdidas leves o impacto a nivel operativo en el *GCABA*.

    2. CONFIDENCIAL: *Información* que sólo puede ser conocida y utilizada por un grupo de *Agentes* del *GCABA*, siendo esta necesaria para sus funciones y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas o impacto a nivel directivo en el *GCABA*.

3. SECRETA: *Información* que sólo puede ser conocida y utilizada por un grupo muy reducido de *Agentes* del *GCABA*, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves o impacto a nivel estratégico en el *GCABA*.

b. Nivel de Integridad: La integridad previene la degradación de la calidad de la información.

0. REEMPLAZABLE: *Información* cuya modificación no autorizada, no afecta la operatoria o imagen pública del *GCABA*.

1. BAJA: *Información* que es posible reobtener fácilmente. Su modificación no autorizada podría ocasionar pérdidas menores, impacto a nivel operativo o afectar de forma menor la imagen pública del *GCABA*.

2. ALTA: *Información* que su reobtención o restitución es compleja. Su modificación no autorizada podría ocasionar pérdidas significativas, impacto a nivel directivo o afectar la imagen pública del *GCABA*.

3. CRUCIAL: *Información* irremplazable. Su modificación no autorizada podría ocasionar pérdidas graves, impacto a nivel estratégico o afectar gravemente la imagen pública del *GCABA*.

c. Nivel de Disponibilidad: La disponibilidad previene la denegación no autorizada de la información.

0. ESTANDAR: *Información* cuya inaccesibilidad no afecta la operatoria del GCABA.

1. RELEVANTE: *Información* cuya inaccesibilidad permanente durante una semana o más, podría ocasionar pérdidas no significativas o impacto a nivel operativo en el *GCABA*.

2. DELICADA: *Información* cuya inaccesibilidad permanente durante un día o más, podría ocasionar pérdidas significativas o impacto a nivel directivo en el *GCABA*.

3. VITAL: *Información* cuya inaccesibilidad permanente durante unas horas podría ocasionar pérdidas graves o impacto a nivel estratégico en el *GCABA*.

Criticidad de la Información

Una vez obtenidos los valores de clasificación (*confidencialidad, integridad y disponibilidad*), se procederá a determinar la criticidad de la información de acuerdo con la siguiente escala:

ANEXO I

a. CRITICIDAD BAJA: ninguno de los valores asignados superan el nivel 1 **(Ej.: C0, I0, D1)**

b. CRITICIDAD MEDIA: alguno de los valores asignados alcanza el nivel 2 **(Ej. C1, I2, D2)**

c. CRITICIDAD ALTA: algunos de los valores asignados alcanza el nivel 3 **(Ej. C2, I0, D3)**

Tratamiento de la Información

Las medidas de tratamiento de la información serán aplicables una vez finalizada la fase de clasificación. La ASI determinará - en función de los resultados obtenidos- cuáles serán las medidas de tratamiento más adecuadas para garantizar una protección efectiva de la información del GCABA.

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a la *información digital* sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0601 - Política de seguridad física

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Seguridad Física

1. Introducción

A fin de proteger la información almacenada en formato digital del GCABA, es fundamental proveer medidas de Seguridad Física a los recursos informáticos que almacenan, transmiten y procesan dicha información. Esto deberá realizarse mediante la aplicación de barreras físicas, procedimientos de control, medidas de prevención y contramedidas para proteger el equipamiento ante amenazas ambientales y de seguridad.

2. Objetivo

Definir las pautas generales de seguridad física que permitan asegurar la integridad de los recursos informáticos utilizados para el procesamiento, transmisión y resguardo de la información del GCABA.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Para una adecuada protección física de los *recursos informáticos* que contienen *información* del *GCABA* la *ASI* establece que deben cubrirse, como mínimo, los siguientes aspectos:

a. Seguridad perimetral

   Conjunto de medidas tendientes a controlar y restringir el acceso físico a las *áreas críticas* a todo el personal no autorizado por la *ASI*, para reducir el riesgo de accidentes y/o actividades fraudulentas.

b. Autorización, registro e identificación de visitantes

Conjunto de mecanismos destinados a asegurar que todos los individuos que ingresen a *áreas críticas* se identifiquen, sean autenticados y autorizados a permanecer en las instalaciones durante los horarios de acceso permitidos.

c. Sistemas Preventivos, Correctivos y de Detección en las *áreas críticas*

Conjunto de mecanismos destinados a:

- Minimizar las amenazas de tipo natural, humana o técnica (sistemas de control de temperatura, humedad, polvo, etc.).
- Asegurar la continuidad operativa (*unidades de suministro continúo de energía*, generadores, etc.).
- Generar acciones correctivas (sistemas de extinción de incendios, evacuación, etc.).

Áreas Críticas

Las *áreas críticas* deben estar ubicadas en áreas seguras. Las mismas deben estar protegidas y resguardadas por un perímetro de seguridad físico definido, con controles de acceso apropiados. Deben estar protegidas contra accesos físicos no autorizados, daños e intrusiones.

La protección física puede llevarse a cabo mediante la creación de diversas barreras físicas alrededor del área segura, donde cada barrera establece un perímetro de seguridad, cada uno de los cuales incrementa la protección total provista.

Se debe minimizar el número de puertas de acceso a las *áreas críticas* para reforzar el control físico del personal que ingresa. El acceso a las áreas críticas sólo debe realizarse a través de las puertas controladas, por lo que el resto de las aberturas deben poseer los recaudos físicos para que esto último se cumpla.

Las *áreas críticas* deben contar con puertas ignífugas con apertura hacia el lado de afuera. Las puertas de acceso no deben permanecer abiertas bajo ninguna circunstancia. Adicionalmente, deben contar con puertas de emergencia ubicadas en distintos puntos de las instalaciones, con cerradura antipánico de accionamiento sólo desde el interior.

Para el acceso físico a las *áreas críticas* se deben utilizar dispositivos automáticos con claves de acceso, combinaciones de cerraduras, tarjetas magnéticas, tecnología biométrica ó claves personales. Adicionalmente se recomienda utilizar CCTV (circuitos cerrados de TV) y/o similares, que permitan monitorear de manera permanente, al menos, los puntos de acceso.

ANEXO I

La *ASI* establecerá las medidas necesarias a realizar ante pérdidas de llaves de acceso (electrónicas o mecánicas), a fin de evitar que las mismas sean utilizadas por personal no autorizado.

No deben ubicarse, dentro de las *áreas críticas*, recursos de uso habitual por parte del personal (tales como impresoras descentralizadas, *insumos informáticos*, documentación en papel, mobiliario que no corresponda al que contiene los recursos informáticos).

Acceso a las *áreas críticas*

El acceso físico a las *áreas críticas* (propias y tercerizadas) se encuentra restringido tanto a personas externas como a todo el personal del *GCABA* que no se encuentre debidamente autorizado por la *ASI*.

Deben existir listas explícitas de las personas autorizadas a acceder a las *áreas críticas*, las cuales mantendrá actualizadas la *ASI*.

Debe registrarse el ingreso y egreso de todos los individuos autorizados a acceder y/o permanecer en las *áreas críticas*. Para el caso en que el control automatizado de acceso estuviera transitoriamente fuera de funcionamiento, deberá existir un "Libro de Registros" en el cual quede formalmente documentado el acceso.

Toda persona que excepcionalmente necesite ingresar a las *áreas críticas* deberá estar acompañada por personal autorizado y deberá registrarse el correspondiente acceso en el "Libro de Registros".

En el "Libro de Registros" deben asentarse, por lo menos, los siguientes datos:

a. Fecha

b. Hora de ingreso y egreso

c. Nombre y apellido del visitante

d. CUIL/T

e. Firma del visitante

f. Organismo/Repartición/Empresa al que pertenece

g. Motivo del ingreso

h. Nombre y Apellido del autorizante

i. Firma del agente autorizante

La *ASI* implementará mecanismos para monitorear en forma específica los ingresos de usuarios externos y/o internos del *GCABA* que no realicen tareas operativas habituales en las *áreas críticas*.

La *ASI* tendrá a disposición del *Organismo* competente que lo requiera, los registros generados por los *sistemas de control de accesos* y/o el "Libro de Registros".

No está permitido el ingreso a las *áreas críticas* con elementos que no sean necesarios para la función para la cual se registre su ingreso.

Se prohíbe el uso de cámaras fotográficas, cualquiera sea su tipo, todo dispositivo de captura de imágenes dentro de las *áreas críticas*, o ingresar con *equipos portátiles* o *dispositivos móviles*, salvo las excepciones debidamente autorizadas por la *ASI*.

Factores Ambientales

La *ASI* establece las siguientes medidas de higiene y condiciones ambientales básicas para evitar que se produzcan hechos que afecten el ambiente donde residen los *recursos informáticos*.

a. Efectuar la limpieza habitual.

b. Disponer la remoción inmediata de materiales que no se utilicen.

c. Evitar la concentración de elementos combustibles innecesarios.

d. Implementar un piso elevado antiestático.

e. Mantener una temperatura ambiente de acuerdo con los requerimientos específicos del equipamiento.

f. Establecer prohibiciones de comer, beber y fumar dentro de las áreas críticas.

Adicionalmente, las *áreas críticas* deben contar con sistemas automáticos de detección y respuesta ante condiciones ambientales que afecten el procesamiento de los equipos.

Instalaciones eléctricas

Los *recursos informáticos* donde se procesa, comunica y almacena información considerada de criticidad media/alta deben contar con *unidades de suministro continuo de energía (UPS)*, estabilizadores de tensión y grupos electrógenos fijos y/o móviles.

Debe realizarse en forma periódica el mantenimiento preventivo y correctivo del cableado, las cajas de conexión y los paneles de distribución de electricidad.

La instalación eléctrica de todas las *áreas críticas* debe ser independiente a la del resto del edificio.

ANEXO I

Las líneas de energía eléctrica y telecomunicaciones dentro de las *áreas críticas* deben estar ubicadas entre el piso y el piso técnico y/o entre el techo y falso techo, y deberán estar dentro de canaletas ignífugas y termo resistentes. El cableado de potencia debe estar claramente separado del cableado lógico, y debidamente identificados.

Detección/Extinción de incendios

a. Todas las *áreas críticas*, sin excepción, deben contar con detectores de calor y humo instalados en forma adecuada y en número suficiente como para detectar el más mínimo principio de incendio. Los mismos deben probarse periódicamente.

b. En la construcción de las *áreas críticas* deberán haberse contemplado barreras cortafuegos en cableados y conductos de comunicación y ventilación.

c. Los paneles eléctricos, en la medida de lo posible, deben estar cubiertos por cajas ignífugas.

d. Se debe contar con un sistema de extinción automática de incendios y, complementariamente, con cantidad suficiente de matafuegos habilitados que cumplan con las especificaciones para incendios en equipos eléctricos, con su correspondiente identificación que indique la vigencia y el tipo de carga que contienen. Deben estar instalados en lugares de fácil acceso y claramente indicados, visibles incluso ante ausencia de luz.

Detección/prevención de inundaciones

a. Las *áreas críticas* deben estar ubicadas a una altura superior al nivel de la calle, a fin de evitar inundaciones.

b. En las *áreas críticas* no deben pasar cañerías de líquidos por sus techos, ni ser contiguos a sectores húmedos (tales como torres de enfriamiento, baños, depósitos de líquidos, etc.).

c. Las bandejas portacables deben poseer perforaciones en un número y tamaño suficiente, a fin de que no sirvan como compartimentos estancos con la posibilidad de inundación de las mismas.

d. En los pisos deben existir detectores de humedad, y las pendientes de los pisos deben conducir hacia las bocas de desagüe.

e. Las cañerías de desagüe ubicadas en el piso deben poseer válvulas de retención, a fin de que no sirvan como bocas de inundación ante sobreflujos.

f. Los paneles eléctricos deberían, en la medida de lo posible, estar protegidos por aislantes anti humedad.

ANEXO I

Centros de almacenamiento de copias de resguardo

Las copias de resguardo deben almacenarse dentro de un lugar restringido en las instalaciones del *GCABA*, consideradas estas como *áreas críticas* a las que aplican todas las condiciones de seguridad física descritas en esta política.

Toda reforma que se realice a los *centros de almacenamiento de las copias de resguardo* (sean propios o de terceros) deberá ser comunicada a la *ASI*, a fin de que la misma evalúe las posibles consecuencias que se podrían ocasionar sobre la seguridad física establecida en la presente política.

Las copias de resguardo de información de criticidad media/alta deben conservarse en caja ignífuga y con un rótulo externo que permita su identificación.

Generalidades

La *ASI* podrá determinar las acciones a tomar en el caso de incumplimiento a los puntos de la presente política una vez evaluadas las consecuencias, que sobre los recursos y servicios informáticos del GCABA se haya podido ocasionar. Todo ello sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas presuntamente implicadas en dicho incumplimiento.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe y de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0701 - Política de copias de resguardo y recuperación

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Copias de Resguardo y Recuperación

1. Introducción

Es fundamental garantizar la seguridad y disponibilidad de la información almacenada en formato digital del *GCABA*. Todo organismo se encuentra expuesto al riesgo de pérdida de información debido a problemas de hardware, de software, por ataques relacionados con software malicioso, errores humanos, catástrofes, etc. Por esto, es necesario implementar un adecuado esquema de resguardo a fin de maximizar la posibilidad de recuperar la información y minimizar el tiempo y costo que conlleva la pérdida de la misma.

2. Objetivo

Establecer los lineamientos para la generación, prueba y administración de copias de resguardo periódicas de la información digital del *GCABA*, de forma que sea posible recuperar, en un tiempo aceptable, cualquier archivo y/o sistema que haya sido resguardado previamente y se haya perdido o dañado de forma accidental o intencional.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Requerimientos mínimos de resguardo

La *ASI* establecerá un cronograma ordenado y documentado de actividades de respaldo, que promueva la disponibilidad de aquella información que determine en acuerdo con cada *Propietario de la Información*. Se deberá considerar en el mismo la rotación de medios de resguardo, considerando su vida útil y las posibles fallas detectadas en estos.

Cuando un *Propietario de la Información* requiera un servicio de resguardo para un componente no considerado en el esquema actual, deberá solicitar su incorporación a la *ASI,* quien evaluará las necesidades técnicas del resguardo y, de acuerdo a la disponibilidad de la infraestructura existente, aprobará la incorporación de esta información al esquema de resguardo.

ANEXO I

El esquema de resguardo establecido por la *ASI* podrá ejecutarse manual o automáticamente y deberá contemplar además los siguientes criterios:

a. Periodicidad mínima: período mínimo para efectuar el proceso de resguardo de la información.

b. Almacenamiento externo: período mínimo para efectuar el envío a un sitio externo.

c. Conservación de soportes históricos: período mínimo de conservación de los medios donde se resguarda la información.

d. Tipo de resguardo:

- Completo: copia la totalidad de los datos.

- Diferencial: copia todos los datos que haya cambiado desde el anterior resguardo completo.

- Incremental: solo copia los datos que han variado desde la última operación de resguardo.

En el mismo, la *ASI* podrá establecer claramente la identificación de los equipos e información a resguardar, las frecuencias establecidas y los medios a utilizar. Mantendrá un inventario de medios de resguardo indicando además la fecha y hora en que se realizó el resguardo, el ciclo de rotación y el período de retención.

A partir de los criterios definidos para el esquema de resguardo se requiere que las copias realizadas sobre la *información digital* contenida en los *equipos de procesamiento y/o almacenamiento centralizados* cumplan como mínimo, con las siguientes pautas:

- Las copias de resguardo iniciales deberán ser de tipo completo.

- Anualmente se deberá realizar un resguardo completo y conservarse de forma permanente.

- Mensualmente se deberá realizar un resguardo completo y rotarse cada dos años.

- Semanalmente se deberá realizar un resguardo completo, con rotación mensual.

- Diariamente se deberá realizar un resguardo incremental, diferencial o completo, en medios separados, con rotación mensual.

- Se conservará en un sitio externo al *centro de almacenamiento de datos,* una copia del resguardo inicial, una copia del resguardo anual y una copia del resguardo realizado para cada mes. Dichas copias se conservarán de forma permanente. El sitio externo deberá ser el autorizado por la *ASI*.

Para aquellos casos que correspondan a software de aplicación, software de base y/o archivos de configuraciones, las copias realizadas deben cumplir como mínimo, las siguientes pautas:

- Realizar una copia de resguardo inicial, las que deberán ser de tipo completo.

- Realizar un resguardo de tipo diferencial cada vez que se efectúen cambios. Estos resguardos estarán disponibles para su uso en procedimientos de restauración en caso de que ocurra un problema con los cambios realizados.

Requerimientos para resguardos especiales

Para aquellos requerimientos especiales de resguardo la *ASI* establecerá el esquema de acuerdo a la disponibilidad de la infraestructura tecnológica existente. Salvaguardando en todos los casos el resguardo correspondiente.

Resguardo de los registros de auditoría

Los reportes correspondientes a registros de auditoría de seguridad deben ser resguardados en forma independiente a la información de producción y los registros de auditoría transaccional, en medios no reutilizables o modificables.

La definición de los registros de auditoría se realizará de acuerdo a lo establecido por la *ASI*. Quien definirá sobre estos registros de auditoría el resguardado necesario y la periodicidad de los mismos.

Soportes físicos

La *ASI* definirá los soportes más adecuados sobre los que se deben efectuar las copias de resguardo, como ser unidades ópticas, discos ópticos, cintas y/o similares.

Asimismo, el envío a sitios de almacenamiento externo tendrá que efectuarse por un medio de transporte seguro que garantice un adecuado resguardo de las copias, las cuales, deben ser transportadas, utilizando medios que eviten el acceso no autorizado a la información, asegurando su confidencialidad e inalterabilidad.

Rótulos internos

Las copias de resguardo deben contar con un rótulo interno almacenado dentro del medio magnético que permita su correcta identificación.

ANEXO I

Horario de los procesos de resguardo

Los procesos de generación de copias de resguardo deben efectuarse en horarios que minimicen el impacto en el rendimiento, tiempo de respuesta y disponibilidad de los servicios de los equipos de procesamiento centralizados.

Rotación de soportes físicos

Se conservarán los soportes físicos por un período establecido según el esquema de resguardo, luego de el cual podrán ser reutilizados. El esquema de rotación deberá contemplar medios de borrado seguro y factores de desgaste para maximizar la vida útil de los mismos.

Inventario de las copias de resguardo

La *ASI* establecerá y mantendrá un inventario de los soportes existentes, su contenido y el lugar donde se encuentran almacenados.

El mencionado inventario debe contener, como mínimo, la siguiente información respecto de lo respaldado:

a. Clara identificación de la denominación nemotécnica (rótulo interno).

b. El tipo de contenido.

c. La fecha de resguardo.

d. Los ciclos de rotación.

e. Períodos de retención.

f. Cantidad de usos del medio.

g. Fecha esperada de destrucción.

h. Responsable del resguardo.

i. Fecha de la última prueba del resguardo.

j. Responsable de la prueba.

Restauración de *información digital*

a. Solicitud de restauración de la *información digital.*

ANEXO I

Los *Responsables de la Información* pueden solicitar la restauración de la información a su cargo, sobre los *equipos de procesamiento centralizado* a través de un *Referente de Información* previamente autorizado.

La *ASI* registrará y documentará las tareas realizadas, los resultados obtenidos y la conformidad del *Propietario de la Información* que solicitó la restauración.

b. Pruebas periódicas de recuperación de *información digital*

La *ASI* podrá efectuar las pruebas de restauración desde los soportes almacenados que considere necesarias, con el fin de garantizar la integridad y disponibilidad de la *información digital*.

Estas pruebas incluyen la revisión periódica de las copias de resguardo, pruebas de recuperación, e integridad de la *información* resguardada y la seguridad física aplicada. Dichas pruebas quedarán debidamente registradas y documentadas.

En la ejecución de las pruebas se considerará la restauración de resguardos actuales e históricos, y se documentarán como resultado la siguiente información:

a. La antigüedad y el medio de almacenamiento utilizado.

b. El resultado final de las pruebas.

c. Constancia de conformidad por los resultados obtenidos por parte de los *Responsables de la Información* que correspondan.

Situaciones de emergencia

La *ASI* establecerá los mecanismos de recuperación adecuados ante situaciones de emergencia durante los procesos de generación y/o de restauración de las copias de resguardo. En dichos procesos, se deberán identificar: responsables autorizados, pasos a seguir, evidencias sobre las cuales dejar constancia, puntos de control del proceso y otros aspectos relacionados.

Dichas acciones a contemplar abarcarán desde interrupciones habituales en el uso de la tecnología hasta desastres de mayor magnitud que impliquen la inoperatividad de los Sitios de Procesamiento de Datos.

Proveedores Externos

Toda tercerización con un proveedor, en cualquiera de las etapas del proceso de resguardo de la información, deberá estar amparada por acuerdos de confidencialidad que deben cumplir con los requisitos formales estipulados por la *ASI*.

ANEXO I

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0702 - Política de seguridad en las comunicaciones

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Seguridad en Comunicaciones

1. Introducción

Los *sistemas de información* están comunicados entre sí, tanto entre *Organismos* como con terceros. La presente política establece los criterios de seguridad necesarios para la gestión de las comunicaciones, que garanticen la confidencialidad, integridad y disponibilidad de la *información* en los usos requeridos por los *agentes* del *GCABA*.

2. Objetivo

Asegurar una adecuada protección en los procesos de intercambio de *información* en las redes de comunicaciones del GCABA.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Controles en las comunicaciones

Las conexiones externas a la red de comunicaciones del GCABA se realizarán a través de puntos adecuadamente controlados y deben cumplir los lineamientos establecidos en las políticas de la ASI para tal fin.

Medios de acceso a la red de comunicaciones

La instalación y conexión de cualquier tipo de enlace para la transmisión y/o recepción de datos debe ser autorizada por la ASI. En caso de tratarse de una instalación ya realizada por agentes externos a la ASI,

se procederá a relevar y documentar la misma antes de autorizar la conexión a la red de comunicaciones del GCABA.

La ASI posee la facultad exclusiva de asignar y administrar las direcciones IP en todo el ámbito del GCABA.

A continuación se describen los distintos medios por los cuales se puede tener acceso a la red de comunicaciones del GCABA. La ASI es el organismo responsable de determinar el medio más adecuado para cada caso:

a) Conexiones de *Organismos* del *GCABA* a través de enlaces punto a punto contratados;
b) Conexiones de *Organismos* del *GCABA* a través de redes públicas;
c) Conexión de terceros por enlaces punto a punto contratados;
d) Conexiones de terceros a través de redes públicas;
e) Conexión de organismos del *GCABA* a través de enlaces propios (terrestres o inalámbricos).

a) Conexiones de *Organismos* del *GCABA* a través de enlaces punto a punto contratados

- La solución de conectividad para el organismo, es definida por la ASI teniendo en cuenta las características técnicas que se requieren y los recursos disponibles.

- La ASI es el organismo encargado de confeccionar las Condiciones Particulares y Especificaciones Técnicas.

- Sólo cuando la ASI haya aprobado la instalación, se dará de alta el servicio.

- La función de Administración en los equipos de ruteo del proveedor del servicio, en ambos extremos, es competencia de la ASI, como así también la implementación de las reglas y políticas de seguridad en los equipos de red para asegurar la disponibilidad de los servicios requeridos y seguridad de la red.

- Seis (6) meses antes de la finalización del contrato, el organismo responsable del pago mensual de los abonos informará este hecho a la ASI, a los efectos de iniciar el proceso licitatorio con la suficiente antelación.

b) Conexiones de Organismos del GCABA a través de redes públicas

- Es competencia de la ASI estimar la conveniencia de aplicar esta solución, dado que estos enlaces no garantizan alta disponibilidad.

- Los Organismos utilizarán el servicio de Internet que la ASI autorice expresamente. No podrán contratar servicios adicionales de terceros.

- Este tipo de comunicación se efectiviza a través de los mecanismos VPN gestionados por la ASI.

- La ASI es responsable de la puesta en marcha y de la administración del vínculo de comunicación (Ej.: VPN), así como de la implementación de las reglas y políticas de seguridad en los equipos de red, a fin de asegurar la disponibilidad de los servicios requeridos y la seguridad de la red.

- Las características técnicas del equipamiento con que deberá contar el usuario para establecer los mecanismos VPN, son definidas por la ASI.

- El equipo terminador en el extremo de la repartición, debe permanecer siempre encendido y conectado. Los organismos que utilicen este servicio deben informar a la ASI, los casos en los que se deba afectar su disponibilidad permanente, especificando el motivo y el tiempo de duración de la eventual salida de servicio.

- El equipo terminador debe estar ubicado en un sitio que cuente con las condiciones ambientales, seguridad física y alimentación eléctrica apropiados, siendo estas condiciones establecidas por la ASI.

- La gestión en su totalidad de los equipos terminadores de VPN en ambos extremos, es exclusiva competencia de la ASI.

- El uso de Internet, se realiza de acuerdo a las pautas definidas por la ASI para tal fin.

c) *Conexión de terceros por enlaces punto a punto contratados*

- Los organismos externos al GCABA coordinarán con la ASI los aspectos técnicos inherentes a la solución de conectividad a instalar.

- La función de administración en los equipos de ruteo del proveedor del servicio, en ambos extremos, es competencia de la ASI, como así también la implementación de las reglas y políticas de seguridad en los equipos de red para asegurar la disponibilidad de los servicios requeridos y la seguridad de la red. Por lo tanto este hecho debe ser tenido en cuenta en los acuerdos a establecer con el tercero, para la contratación y mantenimiento del servicio.

- Para cualquier tipo de conexión con independencia de su protocolo, todo el manejo de la conmutación lógica, administración de direccionamiento IP, etc., debe estar a cargo de la ASI (redes a nivel IP).

- Se debe entregar a la ASI, una copia del contrato o convenio celebrado con el proveedor del enlace.

- La ASI será responsable de establecer y revisar los acuerdos de nivel de servicio pudiendo monitorear en todo momento la calidad y/o la disponibilidad del enlace, a fin de hacer cumplir los lineamientos establecidos en dicho acuerdo.

- La detección de cualquier irregularidad en el tráfico de red es motivo suficiente para que la ASI proceda a la desconexión sin previo aviso.

- El tercero deberá informar a la ASI cuál es la solución de prevención de software malicioso que tiene implementada.

d) *Conexión de terceros* a través de redes públicas

- Este tipo de comunicación se efectiviza a través de mecanismos VPN. La ASI es responsable de la puesta en marcha y de la administración del mecanismo VPN.

- Las características técnicas del equipamiento con que deberá contar el usuario para establecer el mecanismo VPN, son definidas por la ASI.

- El organismo usuario es responsable de la contratación del servicio de acceso a Internet según las especificaciones técnicas emitidas por la ASI, debiendo luego informar a la ASI las características del servicio contratado.

- El equipo terminador en el extremo de la repartición, debe permanecer siempre encendido y conectado. Los organismos que utilicen este servicio deben informar a la ASI, los casos en los que se deba afectar su disponibilidad permanente, especificando el motivo y el tiempo de duración de la eventual salida de servicio

- La gestión de los equipos terminadores de VPN en ambos extremos, está a cargo de la ASI, así como también la implementación de las reglas y políticas de seguridad en los equipos de red para asegurar la disponibilidad de los servicios requeridos y la seguridad de la red.

- La ASI será responsable de establecer y revisar los acuerdos de nivel de servicio pudiendo monitorear en todo momento la calidad y/o la disponibilidad del enlace, a fin de hacer cumplir los lineamientos establecidos en dicho acuerdo.

- La detección de cualquier irregularidad en el tráfico de red es motivo suficiente para que la ASI proceda a la desconexión sin previo aviso.

- El tercero informará a la ASI cuál es la solución de prevención de software malicioso que tiene implementada.

e) *Conexión de organismos del GCABA a través de enlaces propios (terrestres o inalámbricos).*

- La solución de conectividad para el organismo, es definida por la ASI teniendo en cuenta las características técnicas que se requieren y los recursos disponibles.

- La función de administración en los equipos de ruteo y conmutación en ambos extremos es competencia de la ASI, como así también la implementación de las reglas y políticas de

seguridad en los equipos de red para asegurar la disponibilidad de los servicios requeridos y seguridad de la red.

- Cuando de la evaluación técnico-económica surja la conveniencia de instalar soluciones de conectividad de tipo inalámbrico, la comunicación entre nodos se realizará a través de los mecanismos VPN implementados y administrados por la ASI.

Dispositivos de red

Los equipos de red adquiridos y/o instalados por los organismos en la red de comunicaciones del GCABA deberán cumplir con las especificaciones técnicas establecidas por la *ASI*.

La ASI poseerá la administración completa y exclusiva de los equipos conectados a la red del GCABA.

Los equipos de red deben ser monitoreables; aquellos organismos que actualmente utilicen equipos que no cuenten con dicha condición, lo informarán a la ASI para acordar tiempo y forma de su sustitución.

Los equipos de red deben estar ubicados en sitios que cuenten con las condiciones ambientales, seguridad física y alimentación eléctrica apropiados, siendo estas condiciones establecidas por la ASI.

No deben utilizarse, ni tener instalados equipos de comunicación a redes externas (sean públicas o privadas), tales como módems, o equipos similares de comunicación; salvo autorización escrita de la ASI. Aquellos organismos que actualmente cuenten con equipos de estas características deben proceder a su desinstalación física. Todo equipo que no pueda ser removido físicamente y no tenga justificación de uso, deberá ser deshabilitada su funcionalidad a partir de las opciones de configuración de hardware suministradas por el fabricante.

No se permite la instalación de sistemas inalámbricos, salvo aprobación e intervención de la ASI.

La conexión de cualquier dispositivo cableado, deberá contar con la correspondiente autorización y será notificada al responsable de red local quien remitirá la información a la ASI.

Los usuarios que utilizan equipos portátiles, deberán tener instalado la solución corporativa de prevención de software malicioso provista por la ASI. Esta solución será instalada en modo *roamming* a efectos de que permanezca actualizado aún cuando (circunstancial o excepcionalmente) los equipos no se encuentren conectados a la red de comunicaciones de GCABA. La información del GCABA almacenada en estos equipos, deberá ser preservada, siendo su integridad y confidencialidad, responsabilidad de los usuarios. Por lo tanto, dichos usuarios deberán tomar los recaudos pertinentes cuando conecten los mismos a una red que no pertenezca al dominio del GCABA.

ANEXO I

Usos de la red de comunicaciones

La instalación de servidores o equipos similares que publiquen servicios en la red de comunicaciones debe contar previamente con la aprobación escrita de la ASI. La implementación de cualquier aplicación o servicio debe ser informado con la antelación suficiente a la ASI para determinar la clase de servicio que se le debe asignar.

Los servidores deben estar bajo la responsabilidad de personal con habilidad y experiencia para realizar las tareas de administración necesarias para mantener la seguridad del servicio que se brinda, como así también de la red de comunicaciones.

Sólo se permite la instalación de servidores de nombre de dominio (DNS) secundarios en un organismo conectado a la red de comunicaciones, si está debidamente autorizado por la ASI.

Sólo se permite la instalación de un servidor de asignación de direcciones dinámicas (DHCP) en un organismo conectado a la red de comunicaciones, si está debidamente autorizado por la ASI y configurado bajo las pautas establecidas por la ASI.

No se permite la instalación de dispositivos firewalls en las redes que se conectan a la red de comunicaciones GCABA, salvo expresa autorización por escrito e intervención de la ASI. La administración de los firewalls está a cargo de la ASI.

No se permite la instalación de firewalls personales salvo expresa autorización por escrito de la ASI. Todo equipo conectado a la red de comunicaciones podrá ser monitoreado por la ASI. Está prohibida la utilización de cualquier medio que permita ocultar la identidad del dispositivo de red o simule ser otro.

Todo usuario para tener acceso a los servicios brindados por la red de comunicaciones debe poseer un identificador personal (usuario y clave) y es el único responsable de las actividades que sean realizadas con dicho identificador. Cualquier intento por romper estos procedimientos de validación será considerado una falta grave a la seguridad de la red.

Toda estación de trabajo o equipo servidor del GCABA que esté conectado a la red de comunicaciones por cualquier medio, debe tener obligatoriamente instalado la solución corporativa de prevención de software malicioso proporcionada por la ASI; de lo contrario, el equipo será desconectado de la red sin previo aviso.

Toda estación de trabajo o equipo servidor del GCABA que esté conectado a la red de comunicaciones por cualquier medio, debe instrumentar los medios para aplicar las actualizaciones de seguridad correspondientes al sistema operativo instalado, de acuerdo a las pautas que dicte la ASI.

Circunstancialmente la ASI dará instrucciones respecto a la necesidad o no de instalar determinados parches. La ASI se reserva la decisión última sobre la necesidad o no de aplicar dichos parches.

Aquellos organismos externos al GCABA que por algún motivo ingresen a la red de comunicaciones, ya sea temporalmente o por un período prolongado, deben presentar y validar su solución de prevención de

software malicioso. La ASI evaluará si la misma es adecuada antes de conectar dicho organismo a la red de comunicaciones.

Queda prohibida la conexión de equipos de la red de comunicaciones a todo tipo de conexión externa a la misma, sea esta permanente o transitoria, salvo autorización escrita y supervisión de la ASI.

Toda conexión que tenga como origen una red externa a la red de comunicaciones debe estar autorizada, a través de los medios proporcionados por la ASI.

Queda prohibido el uso e instalación de cualquier software, programa, o servicio que no tenga un uso estrictamente laboral afín al cargo desempeñado en el ámbito del GCABA. Especialmente se prohíbe la instalación de software orientado a suplantar la identidad de otro usuario, penetrar o intentar penetrar las medidas de seguridad de los servicios brindados en la red de comunicaciones, así como de cualquier otra entidad externa; esto incluye el envío de correo masivo no deseado, denegación de servicio (DoS), mail-bombing o pirateo de software, entre otros.

Queda prohibido utilizar la red de comunicaciones para cualquier tipo de uso ilegal, emplear los servicios de la red de comunicaciones para transmitir y/o almacenar cualquier material que intencionalmente viole cualquier ley municipal, nacional o internacional o cualquier norma o regulación promulgada en un futuro. Esto incluye, material protegido por Copyright, marca registrada o cualquier otra ley de propiedad intelectual, entre otros.

Seguridad en las transmisiones

La ASI evaluará en función de la criticidad y sensibilidad de la información transmitida dentro y fuera del GCABA, la necesidad de utilizar métodos de cifrado para garantizar la confidencialidad, integridad y disponibilidad de los mismos.

La información clasificada por el *Propietario de la Información* deberá transmitirse cumpliendo con los controles de seguridad establecidos por la ASI dentro del marco normativo.

La ASI seleccionará las herramientas y algoritmos de cifrado que se utilizarán –cuando sea necesario- para garantizar la confidencialidad e integridad de la información digital transmitida.

La ASI proveerá a los usuarios las herramientas seleccionadas para realizar las transmisiones en forma segura. Adicionalmente, capacitará a los mismos sobre la forma de utilización de dichas herramientas a fin de garantizar su efectividad.

ANEXO I

Transmisiones inalámbricas

La ASI establece que se implementen las siguientes medidas de protección para la información transmitida y mecanismos de control de acceso y autenticación para la conexión inalámbrica de usuarios a la red de comunicaciones del GCABA:

- Toda transmisión inalámbrica debe realizarse en forma cifrada.

- Todo acceso a los recursos informáticos del GCABA a través de dispositivos inalámbricos deberá cumplir con los lineamientos de identificación y autenticación establecidos por la ASI. El proceso de autenticación deberá realizarse en forma cifrada.

Estos aspectos de seguridad deben considerarse para la evaluación de cualquier tipo de aplicación o sistema que se implemente sobre tecnologías inalámbricas.

En los casos en los que el GCABA ofrezca servicios gratuitos de conectividad inalámbrica en espacios públicos destinados a los ciudadanos, estos servicios deberán cumplir con las siguientes pautas:

- El establecimiento de la conexión deberá estar respaldado por una política de uso. Dicha política deberá contar con un mecanismo de aceptación de las condiciones que debe cumplir el usuario.

- La ASI es responsable de la puesta en marcha y de la administración del equipamiento WiFi.

- Las características técnicas con que deberá contar el equipamiento, son definidas por la ASI.

Documentación

La ASI establece la necesidad de documentar y mantener procedimientos operativos que registren los servicios, las características del tráfico y la política de comunicaciones implantada en la red del GCABA. Los procedimientos deberán ser tratados como documentos formales y los cambios deberán ser autorizados por la ASI, en todos los casos.

- Se deberán tipificar los servicios que se ofrecen en el entorno de la red GCABA, a través de un inventario, identificando para cada servicio, usuarios (quien accede), la exposición (desde donde se accede), la sensibilidad de los datos (clasificación de la información), la ubicación del servidor que lo alberga (dirección lógica) y la fase del ciclo de vida del software en la que se encuentre (desarrollo, pruebas, homologación, producción), etc.

- Se deberá recopilar y registrar toda la información referente a los perfiles de usuarios definidos y su ubicación dentro de la red GCABA. El objetivo es comprobar que cada usuario tiene las

credenciales y los permisos adecuados que limitan sus accesos exclusivamente a los entornos en los que tiene privilegios de acceso.

- Se deberá documentar toda la información referente a las comunicaciones del entorno, obteniendo el siguiente detalle:
    a. Mapas de red
    b. Topología de la red a nivel 2 y 3 del modelo OSI
    c. Inventario de redes
    d. Inventario de dispositivos de comunicaciones
    e. Inventario de dispositivos de seguridad
    f. Relaciones con los respectivos acuerdos de nivel de servicio (SLA)

- Así mismo deberá documentarse toda la información referente a la política de comunicaciones implantada en la red corporativa. Esta política posibilita identificar los flujos de tráfico permitidos y no permitidos de la red, así como los caminos utilizados para acceder de un entorno a otro. Se deberán identificar los protocolos de enrutamiento configurados en la red, el plan de direccionamiento implantado en el entorno de red especificado por la ASI y demás puntos que se consideren de utilidad para su registro y posterior análisis.

- Se deberán documentar las características del tráfico actual de la red, a fin de que sirvan de punto de comparación en futuras elecciones de soluciones tecnológicas. Se procederá a documentar:
    a. Identificación de puntos críticos
    b. Escuchas (sniffers) con fines estadísticos sobre los puntos críticos.
    c. Carga actual de los dispositivos de comunicaciones: firewalls, switches, routers, bridges y ocupación de las líneas de comunicaciones.

Generalidades

Queda prohibido el uso de dispositivos que permitan realizar "escuchas", alterar los datos, descifrarlos, desviarlos, entre otros, sobre los equipos o líneas de comunicaciones, salvo autorización expresa de la ASI para permitir diagnosticar o resolver algún inconveniente o mal funcionamiento puntual.

La detección de cualquier irregularidad en el tráfico de red es motivo suficiente para que la ASI proceda a la desconexión sin previo aviso.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0703 - Política de seguridad en redes

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Seguridad en Redes y Comunicaciones

1. Introducción

La presente política establece los criterios de seguridad necesarios para la gestión de redes que garanticen la confidencialidad, integridad y disponibilidad de la *información* en los usos requeridos por los *agentes* del *GCABA*.

2. Objetivo

Asegurar una adecuada protección de la *información* procesada en la red de datos del GCABA.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Seguridad en redes

Todos los accesos a la red del GCABA, tanto físicos como lógicos son autorizados, administrados y monitoreados por la ASI, quien tiene competencia exclusiva respecto al establecimiento de las políticas de seguridad correspondientes.

Para garantizar la seguridad en el procesamiento de sus datos, la ASI establece los criterios de seguridad que se tratan en adelante.

Controles de red

Se requiere un conjunto de controles para lograr y mantener la seguridad de las redes de datos. Se deben implementar controles para garantizar la seguridad de los datos y la protección de los servicios conectados contra el acceso no autorizado, En particular, la ASI establece los siguientes controles:

- Las responsabilidades de administración de las redes deben estar separadas de las de operaciones de equipos de usuario.

- Se deben establecer controles de tráfico en la administración del equipamiento perteneciente a los dominios Internet, Extranet e Intranet, así como los accesos remotos, accesos externos (confiables y no confiables).

- Deben establecerse controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y en especial para proteger las conexiones de los usuarios que realizan teletrabajo con información sensible. También pueden requerirse controles especiales para mantener la disponibilidad de los servicios de red y equipos conectados.

- Las actividades gerenciales deben estar estrechamente coordinadas, tanto para optimizar el negocio, como para garantizar que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

f) Segmentación de la Red Corporativa

Se debe diseñar una adecuada estructura de red implementando dominios lógicos separados, protegidos por un perímetro acotado de seguridad. Se definirán y crearán distintos dominios lógicos, realizando divisiones por servicios o grupos, sobre la base de los siguientes criterios que puntualiza la ASI:

- Definir los dominios de red a partir de un análisis de criticidad de cada una de las aplicaciones y de los datos que la componen, así como del perfil de los usuarios que acceden a dichas aplicaciones. Estos dominios deberán marcar la política de segmentación, puesto que establecen los puntos en los que será necesario incorporar controles, los diferentes segmentos de red que deben implementarse y las políticas generales de tráfico que se darán en la red.

- Cada red protegida deberá tener su perímetro de seguridad, y los distintos dominios se conectarán por medio de enlaces seguros entre dos redes distintas que filtren el tráfico entre los dominios.

- La segmentación se realizará dividiendo la red en dominios de seguridad lógicos con la finalidad de:

    a. Proteger el acceso a la información y los sistemas en función de su criticidad.

    b. Limitar el acceso de usuarios exclusivamente a los servicios que necesite para llevar a cabo sus funciones.

    c. Aislar los problemas en la red ante la presencia de software malicioso, errores, averías, intrusiones, etc.

    d. Facilitar la localización, gestión y administración de los activos conectados a la red.

- Todos los dominios deben estar identificados y separados física o lógicamente. Dentro de los propios dominios pueden existir componentes que no deban estar en el mismo segmento de red debido al compromiso de seguridad que supondría la conectividad plena entre ambos. Se establecerán entonces subdominios en base a criterios de segmentación concretos.

- La interconexión entre dominios se deberá realizar a través de dispositivos que permitan la segregación de tráfico permitido y no permitido y que mantengan un registro de las conexiones que se realizan.

- En los casos en que un mismo equipo pertenezca a varios dominios a la vez, se debe utilizar una interfaz para cada dominio, bien sea lógico o físico, y se debe deshabilitar el enrutado para que los servidores no actúen como 'puente' entre dominios.

- Deberán establecerse medidas que aseguren la disponibilidad de los segmentos de red, por lo que se estudiará la capacidad de tráfico soportada por los diferentes componentes de la red teniendo en cuenta el tráfico previsto en función de los usuarios que acceden y las operaciones que realicen. Dentro de las consideraciones técnicas que fija la ASI para implementar la segmentación de red, se pueden destacar:

    a. Implementar un segmento dedicado a los servidores con funciones de autenticación como son los de repositorio de usuarios, servidor de dominio, etc. que se ubicarán en el dominio de servidores.

    b. Comprobar que en el dominio de servidores, todas las bases de datos ubicadas en el mismo segmento contienen datos con el mismo nivel de criticidad y/o características de seguridad comunes para el negocio. En el caso contrario se recomienda crear otro segmento en el mismo dominio, separando los servidores críticos de los otros

    c. Mejorar la seguridad elevando el número de segmentos de red. Un mayor número redunda en una mayor seguridad, ya que la posibilidad de extensión de un ataque queda reducida a las máquinas directamente adyacentes a la atacada, a su vez que permite habilitar reglas de tráfico más sencillas y flexibles dando lugar a un acceso más selectivo a determinados servicios, considerando ésta una ventaja estratégica fundamental.

g) Política General de Flujo de Tráfico

Las políticas generales de flujos de tráfico pretenden dar las pautas de dirección de los flujos de datos entre dominios. Los controles generales de dirección de flujos de datos que fija la ASI son los que se exponen a continuación:

- El dominio de redes públicas sólo podrá realizar peticiones a equipos que se encuentren en el domino de extranet. En ningún caso deben realizar conexiones a equipos que se encuentren en dominios confiables distintos de la extranet.

ANEXO I

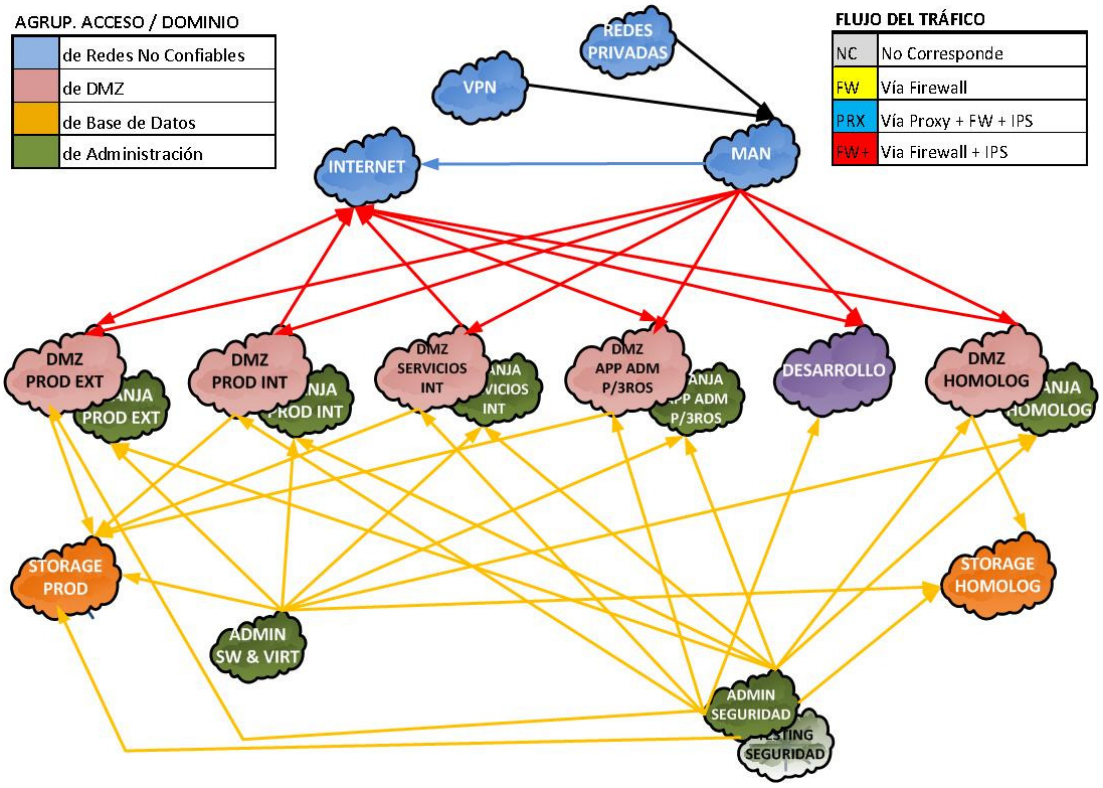
- Los servidores del dominio de extranet podrán realizar peticiones exclusivamente hacia los servidores del dominio de servidores que tengan sus bases de datos.

- Los servidores de pasarela (gateway) de la extranet tendrán privilegios especiales de acceso, pudiendo acceder a Internet (proxy de salida) y a la Intranet (dispositivos de VPN).

- El dominio de Intranet no podrá realizar conexiones hacia los dominios públicos. Para poder acceder a ellos deberán hacerlo a través de las pasarelas de acceso a Internet (proxy de salida).

- Los servidores del dominio de Servidores en ningún caso podrán realizar conexiones salientes hacia otros dominios. Podrán recibir conexiones del resto de dominios a través de la interfaz que corresponda

En la siguiente figura se representa gráficamente los diferentes flujos de datos permitidos entre los distintos dominios GCABA:



h) Administración de la Segmentación

ANEXO I

La administración de los segmentos de la Red Corporativa, deberá realizarse de acuerdo a los controles que a continuación dispone la ASI:

- Se establecerán reglas genéricas de acceso para favorecer en la medida de lo posible la administración de los dispositivos de seguridad.

- Se incluirán tiempos de vigencia en las reglas temporales de acceso

- Se definirán y documentarán los procesos de revisión de registros y las acciones a tomar en caso de detección de una incidencia.

- Se establecerán fechas periódicas de auditoría.

- Se centralizará la administración de las pasarelas (gateways), implementando las políticas de tráfico en la red corporativa, a fin de establecer un único punto de gestión, reduciendo el riesgo que puede provocar una inadecuada gestión de dichos dispositivos.

- Se deberán documentar y mantener procedimientos operativos que registren los servicios, las características del tráfico y la política de comunicaciones.

- Se definirán e implantarán herramientas que ayuden a establecer el flujo de autorización de las peticiones de modificación en la configuración de los dispositivos de seguridad.

Se mantendrán diagramas de red actualizados que permitirán identificar los protocolos utilizados, servicios existentes, direccionamiento utilizado, estrategias de enrutado, hardware y software, etc.

i) Administración del Tráfico de Red

Las conexiones de la red de datos se gestionan a nivel Corporativo. Debido a que el GCABA posee edificios localizados en diferentes áreas geográficas, el soporte de la red metropolitana (WAN) será un requerimiento básico, siendo necesaria una adecuada gestión de las rutas de tráfico. Cuando se compara el ancho de banda de la LAN con una WAN, se puede apreciar que es un recurso escaso y debe ser cuidadosamente manejado. A partir de esta premisa, la ASI dispone las siguientes medidas que se deberán aplicar a los dispositivos enrutadores:

- Filtrado de paquetes de red que brinde garantías de seguridad y control de los accesos en toda la Organización. Los accesos no autorizados pueden provocar pérdidas de negocio, fuga de datos sensibles, datos corruptos, además de reducir potenciales responsabilidades legales de los usuarios.

- Conexión de todas las oficinas ubicadas en las diferentes áreas geográficas, tomando en cuenta la tecnología existente en el mercado y los costos de uso, a fin de que el organismo pueda seleccionar la mejor opción desde el punto de vista económico y tecnológico.

- Compresión de paquetes a nivel enlace, a fin de reducir el tamaño del encabezado y los datos, garantizando de esta forma líneas de conexión de casi el doble de tráfico, respecto de las líneas sin compresión.

- Propiedades de reconocimiento de cada protocolo, permitiendo priorizar tráfico y soporte para protocolos sensibles a retardos de la WAN.

- Gestión de ancho de banda. Siempre que sea posible, se deberá gestionar el ancho de banda máximo que se utilice para clientes específicos o para acceder a determinados contenidos.

Para facilitar la gestión y administración de la red perimetral, la ASI establece los controles que a continuación se detallan:

- Deben establecerse reglas genéricas de acceso, por ejemplo, en la Extranet, definir un segmento de servidores Web que admitan peticiones al puerto HTTP exclusivamente y habilitar una regla para todas las direcciones de esa red.

- Incluir tiempos de vigencia de las reglas de acceso y revocar automáticamente aquellas que sobrepasen el tiempo para el que fueron definidas.

- Definir y documentar los procesos de administración y establecer herramientas que ayuden a establecer el flujo de las peticiones de modificación en los privilegios de acceso.

- Definir y documentar procesos de revisión de logs y las acciones a tomar en caso de detección de un incidente.

- Establecer fechas periódicas de auditoría.

La gestión independiente de plataformas firewalls supone el consumo de recursos innecesarios, a la vez que denota la ausencia de una planificación de la política general de tráfico de las comunicaciones. A fin de evitar esto la ASI establece los controles que a continuación se detallan:

- Se deberá centralizar la administración de los firewalls, implementando las políticas de tráfico en la red corporativa, a fin de establecer un único punto de gestión (con diferentes privilegios de administración), reduciendo el riesgo que puede provocar una inadecuada gestión de dichos dispositivos.

- Elaborar un plan de implantación, en el que se detallen las acciones a realizar para conseguir el objetivo de una gestión centralizada, dividiendo las diferentes acciones en fases y definiendo los planes de marcha atrás para cada fase, en caso de falla.

- Previo a la centralización de la administración de firewalls, si fuese necesario, se deberá analizar la diversidad de políticas de firewalls existentes en la red corporativa, realizando un estudio sobre el entorno y la configuración de los mismos.

Adicionalmente a los controles de segmentación de red, es imprescindible la utilización de una herramienta centralizada de administración de accesos a los contenidos Web.

Asimismo es necesario evitar el acceso a Internet de forma directa, de los usuarios de la red interna y de las diferentes ubicaciones edilicias que pertenecen al GCABA. Esto debe realizarse a través de unos medios que garanticen el acceso únicamente a los protocolos HTTP o HTTPS y FTP o SSH, a través de algún tipo de Proxy HTTP / FTP (ya sea software instalado sobre un servidor de propósito general o sobre una plataforma dedicada). La ASI dispone de las siguientes medidas que deberán implementarse para garantizar el acceso de los usuarios a Internet de forma segura:

- Gestión de contenidos. Filtrar los contenidos no autorizados (sexo, violencia, juego, sitios inseguros, etc.) evitando el acceso desde las terminales de los usuarios.

- Caché de contenidos. Deberán implantarse dispositivos con capacidad para cachear en disco local, páginas frecuentemente accedidas, a fin de reducir el ancho de banda utilizado y mejorar los tiempos de respuesta a los usuarios de red.

- Autenticación de usuarios. Deberá habilitarse la autenticación de los usuarios ante el Proxy de salida, de manera que los accesos pueden ser registrados y auditados en caso de incidente o de manera sistemática. Es posible, integrar esta autenticación con el servidor de dominio, de manera que sea totalmente transparente para el usuario, evitando el uso de identificadores genéricos o compartidos.

- Homogenizar siempre que sea posible, la plataforma navegador del usuario.

- Registro de actividad. Se deberán mantener logs de todos los accesos realizados, con el propósito de reconstruir incidentes o para su auditoria sistemática. Esto tendrá relación directa con la política de trazabilidad de las aplicaciones, en función de los niveles de clasificación de información definidos.

- Restricción de comunicaciones. Deberán implantarse dispositivos que permitan de manera sencilla, efectiva y segura, administrar qué protocolos se permiten para los usuarios.

- Integración de un sistema de control de software malicioso. Se deberá integrar en el Proxy un sistema de control de software malicioso que filtre los contenidos descargados en busca de malware o código malicioso, en el software recibido.

Finalmente existirán ciertas consideraciones que deberán tenerse en cuenta con el fin de detectar de forma preventiva eventos que supongan una amenaza para los sistemas de información. Los sistemas de detección de intrusión (IDS) están formados por un conjunto de sondas de red que analizan el tráfico que fluye por la misma con el fin de detectar los eventos que están sucediendo en los segmentos más sensibles de la red o en los sistemas más críticos que puedan suponer una amenaza para los sistemas

de información. La ASI dispone de las siguientes medidas a tener en cuenta al momento de implantar un IDS:

- Se deberá procesar previamente la información obtenida de las alarmas de eventos recibidos. Es necesario discriminar los eventos en función de vulnerabilidades conocidas de los servidores (obtenidas de bases de datos), estableciendo un workflow de alertas a los administradores, para acometer acciones según sea el caso.

- Las diferentes sondas de red deberán ser utilizadas para monitorizar:
    a. Los accesos a los servicios publicados en Internet y los accesos a los servidores VPN. Las mismas deberán ubicarse en el segmento externo (detrás de los firewalls).
    b. El tráfico interno / gestión realizados por los usuarios / administradores en sus labores diarias.

- Las sondas de host deberán ubicarse convenientemente para monitorizar el acceso a los servidores que se considere oportuno.

- En todos los casos la gestión de los eventos y recepción de alarmas, deberá realizarse de forma centralizada.

- La instalación y configuración de la consola de administración (software, configuración de reglas iniciales, comunicaciones con los servidores de firmas, BBDD externas, sensores de red y de host) deberá realizarse por personal cualificado y debidamente autorizado por la ASI.

Documentación

La ASI establece la necesidad de documentar y mantener procedimientos operativos que registren los servicios, las características del tráfico y la política de comunicaciones implantada en la red corporativa. Los procedimientos deberán ser tratados como documentos formales y los cambios deberán ser autorizados por la ASI, en todos los casos.

- Se deberán tipificar los servicios que se ofrecen en el entorno de la red GCABA, a través de un inventario, identificando para cada servicio, usuarios (quien accede), la exposición (desde donde se accede), la sensibilidad de los datos (clasificación de la información), la ubicación del servidor que lo alberga (dirección lógica) y la fase del ciclo de vida del software en la que se encuentre (desarrollo, pruebas, homologación, producción), etc.

- Se deberá recopilar y registrar toda la información referente a los perfiles de usuarios definidos y su ubicación dentro de la red GCABA. El objetivo es comprobar que cada usuario tiene las credenciales y los permisos adecuados que limitan sus accesos exclusivamente a los entornos en los que tiene privilegios de acceso.

- Se deberá documentar toda la información referente a las comunicaciones del entorno, obteniendo el siguiente detalle:

    g. Mapas de red

    h. Topología de la red a nivel 2 y 3 del modelo OSI

    i. Inventario de redes

    j. Inventario de dispositivos de comunicaciones

    k. Inventario de dispositivos de seguridad

    l. Relaciones con los respectivos acuerdos de nivel de servicio (SLA)

- Así mismo deberá documentarse toda la información referente a la política de comunicaciones implantada en la red corporativa. Esta política posibilita identificar los flujos de tráfico permitidos y no permitidos de la red, así como los caminos utilizados para acceder de un entorno a otro. Se deberán identificar los protocolos de enrutamiento configurados en la red, el plan de direccionamiento implantado en el entorno de red especificado por la ASI y demás puntos que se consideren de utilidad para su registro y posterior análisis.

- Se deberán documentar las características del tráfico actual de la red, a fin de que sirvan de punto de comparación en futuras elecciones de soluciones tecnológicas. Se procederá a documentar:

    d. Identificación de puntos críticos

    e. Escuchas (sniffers) con fines estadísticos sobre los puntos críticos.

    f. Carga actual de los dispositivos de comunicaciones: firewalls, switches, routers, bridges y ocupación de las líneas de comunicaciones.

Generalidades

Queda prohibido el uso de dispositivos o herramientas que permitan realizar "escuchas", alterar los datos, descifrarlos, desviarlos, entre otros, sobre los equipos o líneas de comunicaciones, salvo autorización expresa de la ASI para permitir diagnosticar o resolver algún inconveniente o mal funcionamiento puntual.

La detección de cualquier irregularidad en el tráfico de red es motivo suficiente para que la ASI proceda a la desconexión sin previo aviso.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0704 - Política de Prevención de Software Malicioso

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Prevención de Software Malicioso

1. Introducción

El software malicioso es código desarrollado que se instala de forma no autorizada e interfiere con el normal funcionamiento de los equipos de procesamiento, almacenamiento o incluso la red de comunicaciones. Ante la amenaza continua de la existencia de *código malicioso* y su nivel de sofisticación para expandirse, es necesario establecer una serie de medidas que velen por la seguridad, disponibilidad e integridad de la *información* de los *usuarios* y sistemas del *GCABA*.

La forma más común en que se transmite el *código malicioso* es por transferencia de archivos, descarga o ejecución de archivos adjuntos de correos, visitando páginas web o leyendo un correo electrónico.

Por ello, se deben tomar las medidas necesarias a fin de poder detectar y eliminar el *software malicioso* de los *equipos de procesamiento centralizado* y las *estaciones de trabajo* conectadas a la red de comunicaciones del *GCABA* mediante la utilización de una herramienta de antivirus.

2. Objetivo

Establecer los requerimientos que deben cumplir todos los *equipos de procesamiento centralizado* y *estaciones de trabajo* conectados a la red de comunicaciones del *GCABA*, de forma de garantizar la detección y eliminación de *software malicioso* (*virus informáticos*, *troyanos, gusanos, malware en general; incluyendo código móvil*), minimizando el riesgo de infección y propagación de los mismos e impedir los accesos no autorizados, robo o destrucción de *información* del *GCABA*.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Implementación del *Antivirus Corporativo*

Todos los *equipos de procesamiento centralizado* y *estaciones de trabajo* conectadas a la red de comunicaciones del *GCABA* deberán tener instalado el *Antivirus Corporativo* determinado por la *ASI*, a fin de prevenir y eliminar cualquier tipo de infección, propagación y/o ejecución de *software malicioso*. Este producto será puesto a disposición a través de los medios que la *ASI* determine.

La implementación del Antivirus Corporativo se realizará teniendo en cuenta lo siguiente:

a. Debe ser instalado por los Agentes de Tecnología Informática.

b. Debe ser configurado para actualizar su base de firmas en forma periódica, con el objetivo de contar con las últimas versiones publicadas por el proveedor.

c. Debe ser configurado en todos los equipos para una protección en tiempo real.

La solución de *Antivirus Corporativo* se encuentra configurada para limpiar, eliminar o poner en cuarentena los archivos detectados con infección.

Restricciones y consideraciones

Los *Agentes de Tecnología Informática* y los *usuarios*, deberán tener en cuenta las siguientes consideraciones sobre las *estaciones de trabajo* y *equipos de procesamiento centralizado*:

a. Todos los *equipos de procesamiento centralizado* y *estaciones de trabajo* conectados a la red del *GCABA* deberán tener instalado el *Antivirus Corporativo*. Si por cualquier razón no fuera posible la instalación de este producto en algún equipo, el responsable del equipo debe ponerlo en conocimiento de la *ASI*, quien buscará la solución técnica más adecuada en cada caso.

b. No se permite instalar una solución distinta al *Antivirus Corporativo* determinado por la *ASI*.

c. No se permite desinstalar o detener la ejecución del *Antivirus Corporativo*, salvo expresa autorización de la *ASI*, o casos en que el *Agente de Tecnología Informática* se encuentre en tareas de soporte, habilitando a tal fin una ventana de tiempo determinada para la ejecución de las tareas.

d. No se permite detener las actualizaciones del *Antivirus Corporativo*, salvo expresa autorización de la *ASI*.

e. La *ASI* podrá realizar controles periódicos y programados en forma automática para verificar y garantizar la instalación del *Antivirus Corporativo* en todos los *equipos de procesamiento centralizado* y *estaciones de trabajo* conectados a la red de comunicaciones del *GCABA*. Si como resultado de éstos controles se identificaran usuarios que no cumplan con la instalación del Antivirus Corporativo, la ASI emitirá un informe dando cuenta de lo sucedido. Este informe será comunicado a la máxima autoridad del *Organismo* donde se haya producido la falta, quien tomará las medidas que considere necesarias en relación a lo sucedido.

f. La *ASI* se reserva el derecho a desactivar el acceso a la red del *equipo de procesamiento centralizado* o *estación de trabajo* que no disponga del *Antivirus Corporativo* debidamente instalado y actualizado, con el fin de proteger a los demás *usuarios* y equipos de la red.

g. Todas aquellas ejecuciones que se realicen a través de *medios de almacenamiento* personales, haciendo uso de discos, pendrives, u otros medios removibles, serán analizados por el *Antivirus*

Corporativo no permitiendo la ejecución de los archivos o elementos que se encuentren infectados o que presenten algún tipo de riesgo para la red de comunicaciones del *GCABA*.

***Antivirus Corporativo* y servicio de correo electrónico**

La *ASI* tomará las medidas que considere necesarias para aplicar el *Antivirus Corporativo* en el envío y recepción de archivos a través de las Cuentas de Correo Electrónico Gubernamental, a fin de evitar la propagación de *virus informáticos* en la red.

Todo correo que presente una posible amenaza será eliminado de forma permanente de los servidores de correo pertenecientes al *GCABA*, dando aviso al destinatario mediante un correo de notificación.

Controles contra código móvil

El código móvil es aquel que sin instalarse en el equipo se ejecuta de manera automática, realizando una función específica con poca o ninguna interacción de los usuarios.

En su gran mayoría dicho código proviene y se ejecuta en el navegador pero puede afectar también al correo electrónico y otras aplicaciones. La incorporación de código malicioso aprovechando alguna vulnerabilidad técnica sobre la aplicación que se esté utilizando, puede tener diversos motivos como robar sesiones, instalar spyware, entre otros.

En este sentido, el empleo de código móvil deberá ser autorizado expresamente por la ASI; probando su ejecución en un ambiente seguro y controlado con el fin de garantizar que el mismo no contenga código malicioso.

Concientización de los *usuarios* finales

La *ASI* implementará las medidas que considere apropiadas para poner a disponibilidad de todos los *usuarios* de la red de comunicaciones del *GCABA*, la *información* necesaria para la concientización sobre los riesgos de pérdida de *información* por efectos de *software malicioso*, así como también la metodología y los procedimientos a llevar adelante para el uso del *Antivirus Corporativo*.

Sospecha de infección

Cuando se sospeche de una infección que no fuere detectada por la solución de *Antivirus Corporativo*, tanto para el caso de una *estación de trabajo* como para un *equipo de procesamiento centralizado*, el usuario deberá desconectar el equipo de la red y contactar a un *Agente de Tecnología Informática* para evaluar la metodología a seguir para evitar la propagación del virus. En ningún caso está permitido instalar otro Antivirus que no sea el que ha determinado la *ASI*.

ANEXO I

Generalidades

Cualquier violación a la presente política puede derivar en la cancelación del acceso a la red de comunicaciones del GCABA, sin perjuicio de otras acciones que pudieran corresponder en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0705 - Política de Instalación de estaciones de trabajo

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Instalación de Estaciones de Trabajo

1. Introducción

La *estación de trabajo* del *usuario* es un recurso clave en la infraestructura de tecnología informática del *GCABA*. Constituye el nexo entre el *usuario* y la *información digital* del Gobierno.

El mal uso de la *estación de trabajo* o la instalación no autorizada de software o hardware*, además de poder constituir violaciones a los derechos de propiedad intelectual,* puede ocasionar el mal funcionamiento dela misma. Por tal motivo se deben tomar los recaudos necesarios para minimizar el riesgo de pérdida de información, vulnerabilidades de seguridad o plagios.

2. Objetivo

Establecer los lineamientos necesarios para regular la instalación de software y hardware de las *estaciones de trabajo del GCABA* y las responsabilidades de los Agentes, cualquiera sea su función asignada.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

La *ASI* tomará las medidas necesarias para regular y estandarizar la instalación de software en *estaciones de trabajo,* estableciendo las siguientes pautas:

Software Corporativo

La *ASI* establecerá el software autorizado que podrá ser utilizado en las *estaciones de trabajo*. Dicho software será denominado corporativo y estará a disposición de los usuarios a través de los medios que la *ASI* determine. Si el software requerido no estuviese disponible dentro de los autorizados, deberá solicitarse a la ASI la aprobación del mismo.

La *ASI* pondrá a disposición, en caso que el software lo permita, las actualizaciones en línea de manera automática, cuando el usuario se conecte a la *red de comunicaciones* del *GCABA.*

ANEXO I

Instalación de Software y Hardware

Si un *Agente* requiere para el desempeño de sus funciones, la instalación de un *software de aplicación* no disponible en su *estación de trabajo*, deberá generar el requerimiento, por medio de los circuitos formales establecidos por la *ASI*.

Los requerimientos deberán ser aprobados por el *Propietario de la Información* en casos de *software de aplicación*, o por la *ASI* cuando se trate de *software utilitario*.

Las instalaciones serán realizadas por los *Agentes de Tecnología Informática* o personal autorizado para tal fin, quienes son los encargados de instrumentar los medios para aplicar los requerimientos fijados por la ASI en materia de seguridad.

La instalación de cualquier hardware será realizado por los Agentes de Tecnología Informática o personal autorizado por la ASI para tal fin.

No se permite a los usuarios instalar o desinstalar hardware en las *estaciones de trabajo*.

En el caso de gestiones que impliquen reasignaciones, transferencias o cambios de destino de las *estaciones de trabajo*, los datos contenidos en la misma deberán ser eliminados de forma segura antes de ejecutarse la gestión.

Requisitos de Seguridad Lógica

Al momento de encender la *estación de trabajo*, la misma deberá contar con una contraseña o credencial válida de arranque como mecanismo de seguridad por defecto.

No se permite el arranque del sistema operativo desde cualquier medio de almacenamiento que no sea el disco interno.

En períodos de inactividad de la *estación de trabajo*, se deberá implementar el bloqueo automático de la misma, mediante contraseña o credencial válida.

La ASI evaluará la necesidad de establecer medidas de autenticación adicionales en aquellos servicios que crea conveniente.

Restricciones

Debido al riesgo que implica comprometer los mecanismos de seguridad existentes en recursos informáticos, ningún *Agente* del *GCABA* puede instalar:

a. Copias ilegales de cualquier software.

b. Software descargado de internet.

c. Software adquirido para uso personal del usuario.

d. Software de entretenimiento.

e. Cualquier otro software que no corresponda al autorizado como Software Corporativo por la *ASI*.

Los *Agentes* no deberán participar en la copia, distribución, transmisión o cualquier otra práctica no autorizada en las licencias de uso de software.

Responsabilidades

Cada *estación de trabajo* será asignada a un *Agente*, quién será el responsable de los datos que se manipulen en la estación de trabajo y para todos los efectos, del uso del mismo.

Los *Agentes* no podrán retirar o trasladar la *estación de trabajo* fuera de las instalaciones del GCABA o de la dependencia a la cual fue asignada sin la previa autorización del Referente de la Información y del área administrativa correspondiente.

Los *Agentes de Tecnología Informática* serán los responsables de mantener el inventario de los equipos conectados a la red que administran, conjuntamente con sus configuraciones, pertenencia, software instalado, ubicación y modelo. Dicho inventario debe estar disponible de acceso para la ASI en todo momento.

Si se detecta o evidencia que la estación de trabajo fue vulnerada, se deberá notificar de manera inmediata a la ASI, y al *Agentes de Tecnología Informática* a efectos de tomar las medidas tecnológicas necesarias.

Los *Responsables de la Información* definirán la disponibilidad en las estaciones de trabajo de la incorporación, deshabilitación o modificación de los componentes de hardware o elementos tecnológicos requeridos para la implementación de medios de almacenamiento removible.

Consideraciones

Los *Agentes de Tecnología Informática* y el personal autorizado por el Propietario de la Información son los únicos autorizados para la Administración sobre su *estación de trabajo*.

La *ASI* podrá realizar controles periódicos del *software* instalado en las *estaciones de trabajo* conectadas a la *red de comunicaciones* del *GCABA*. Si como consecuencia a éstos controles se detectara el incumplimiento a la presente política, la *ASI* podrá emitir un reporte dando cuenta de lo sucedido y

comunicarlo a la máxima autoridad del *Organismo* donde se haya producido la falta, quien tomará las medidas que considere necesarias.

Generalidades

Todo usuario está obligado a conocer el alcance de uso de cada una de las licencias de software disponible a su disposición, siendo el responsable ante el *GCABA* y/o ante terceros del uso que haga del mismo

La *ASI* se reserva el derecho de solicitar la devolución temporal de la *estación de trabajo* para desinstalar los programas de software que no cumplan con lo establecido en la presente política, sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0706 - Política de uso de Correo Electrónico

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Uso de Correo Electrónico

1. Introducción

La utilización del correo electrónico como medio de transmisión de *información* del *GCABA* es recomendada frente a otros medios tradicionales en función de sus notorias ventajas: economía, rapidez, eficiencia y confiabilidad. Sin embargo, sus características exigen un comportamiento responsable por parte de los *usuarios*, con el fin de convertirlo en un sistema ágil y seguro.

Al utilizar una Cuenta de Correo Electrónico Gubernamental, los usuarios deben tomar en consideración que están actuando en representación del Organismo al cual pertenecen.

2. Objetivo

Establecer las pautas de comportamiento referidas a la utilización del *servicio* de Cuenta de Correo Electrónico Gubernamental (*CCEG*) por parte de los *usuarios*, de forma de garantizar una adecuada protección de la *información* y los *recursos informáticos* y prevenir el tráfico de *Spam* en la red de comunicaciones del *GCABA*.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Solicitud del *servicio*

Las solicitudes de altas, bajas y modificaciones de las CCEG del GCABA se realizarán conforme a lo establecido en la Resolución N° 11/ASINF/11 o aquella que en el futuro la reemplace.

Cuentas de Correo Electrónico Gubernamental (CCEG)

Toda cuenta de correo electrónico cuyo dominio sea "@dominio.gob.ar" es propiedad del *GCABA*.

Todas las *CCEG* deben corresponder a una persona física en particular. La misma debe tener como dominio la identificación del usuario, con su nombre y apellido o similar (ej.: jperez@dominio.gob.ar).

ANEXO I

La creación de cuentas genéricas de correo electrónico será generada solo en aquellos casos en que fuera estrictamente necesario, ya que deben asignarse a un usuario del *GCABA* (que posea *CCEG*) y requieren mantenimiento constante. La necesidad deberá encontrarse justificada en la solicitud, la que deberá ser emitida por un funcionario con rango no inferior a Director General, Equivalente o Superior Jerárquico.

Uso del servicio

Al utilizar el correo electrónico del *GCABA* el usuario acepta los siguientes términos y condiciones de uso:

a. Los usuarios son los únicos responsables del contenido y del uso de sus cuentas de acceso y buzón provistos por el GCABA.

b. El uso del mail es personal y sus claves son confidenciales e intransferibles.

c. No está permitido el uso del correo electrónico con fines privados, ya que el mismo es una herramienta del trabajo.

d. Las comunicaciones privadas deben realizarse a través de los buzones ofrecidos por cualquier proveedor de Internet, y sólo de manera excepcional desde los sistemas provistos por el GCABA. En el caso que se realicen por este último medio, quedarán sujetas a los términos y condiciones de esta normativa.

e. Está prohibida la participación de los usuarios en la propagación de cartas encadenadas y/o la distribución de mensajes en forma masiva, ya sea a CCEG o externas. La distribución de mensajes masivos sólo puede realizarse a través de cuentas definidas para tal fin.

f. La redacción de las comunicaciones debe ser breve, estilo telegráfica, para evitar el congestionamiento de la red. Si es imprescindible enviar un alto volumen de información deberá insertarse como documento adjunto.

g. La información que se recibe de manera personal y confidencial por correo electrónico no puede reenviarse a otra persona, sin autorización del remitente.

h. Todos los mensajes deben enviarse correctamente identificados con el nombre, función y Organismo al que pertenece el remitente.

i. Los usuarios deben evitar transmitir o almacenar información considerada confidencial. Se recomienda utilizar un medio de encriptación seguro en caso de enviar un mensaje de este tipo.

La ASI se reserva el derecho de administrar o limitar el tráfico de archivos adjuntos u otro tipo de información anexa al servicio de correo electrónico, por motivos de seguridad o rendimiento de la red.

ANEXO I

Control del Spam

Se denomina *Spam* al uso del correo electrónico para enviar mensajes no solicitados o no deseados, habitualmente de tipo publicitario y enviados de forma masiva.

La ASI establece las medidas necesarias para el control de este tipo de mensajes a fin de minimizar los riesgos de seguridad y maximizar el rendimiento de la red de comunicaciones del *GCABA*.

Listas de distribución

Los mails masivos de información general del GCABA (tales como newsletters o comunicaciones internas) sólo podrán ser enviados desde cuentas que se destinen para tal fin, denominadas "listas de distribución".

La creación de listas de distribución deberá ser solicitada solo en aquellos casos en que fuera estrictamente necesario, debiendo ser requeridas por un funcionario con rango no inferior a Director General, Equivalente o Superior Jerárquico, a través de una nota.

Para solicitar la creación de una lista de distribución, se deberán suministrar los siguientes datos:

a. Nombre de la Lista de Distribución

b. Lista de usuarios miembros

c. Motivo de la solicitud

d. Sector y Usuarios autorizados para su utilización

Generalidades

Cualquier violación a la presente política puede derivar en la cancelación inmediata de la cuenta de correo, sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0707 - Política de Uso de Internet

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Uso de Internet

1. Introducción

Internet constituye la herramienta más efectiva para el acceso y la transmisión de *información*. Es el medio de mayor alcance que puede utilizar cualquier *Organismo, tanto* público como privado, para difundir *información* acerca de sus actividades.

Por otra parte, mientras que Internet es la red en general abierta a todos, una Intranet es una red interna, propia de una organización, que utiliza protocolos de Internet para compartir *información* y parte de sus *sistemas informáticos*. La Intranet puede estar configurada de forma que sus *usuarios* tengan acceso a Internet y sin permitir que los *usuarios* de Internet tengan acceso a los equipos de la Intranet, o bien puede estar aislada, es decir, no conectada a Internet. La intranet facilita la publicación de *información* interna en todo el *GCABA*.

El *GCABA* promueve el uso de Internet e Intranet para que los *agentes* realicen trabajos específicos a su función.

2. Objetivo

Establecer las pautas de comportamiento referidas a la utilización de Internet para un uso debido por parte de los *usuarios* conectados a la red de comunicaciones del *GCABA,* de forma de garantizar una adecuada protección de la *información*.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

El servicio de acceso a Internet deberá ser utilizado únicamente con fines laborales.

Todos los accesos desde Internet a *recursos informáticos* de la red de comunicaciones del *GCABA* deben utilizar protocolos de comunicación que garanticen un adecuado nivel de integridad y confidencialidad de los datos transmitidos.

Solicitud del *servicio*

El servicio de acceso a Internet deberá ser solicitado al Área de Servicios del *Organismo,* por el superior jerárquico del *usuario*.

ANEXO I

Todo personal que no sea agente del GCABA, que se encuentre prestando un servicio y requiera acceso a Internet podrá disponer del mismo, el cual contará con las reglas de filtrado de contenido que el GCABA tiene para las comunicaciones.

Contenido filtrado en la navegación

Los *usuarios* tendrán prohibido el acceso a todo contenido considerado inapropiado para el ámbito laboral. En la medida que los sistemas lo posibiliten, la *ASI* se reserva el derecho de limitar a los *usuarios* el acceso a los sitios que pudieran perjudicar los intereses y la reputación del *GCABA* o pongan en riesgo la red de comunicaciones del *GCABA*.

Prohibiciones

Las restricciones y prohibiciones definidas a continuación deben ser respetadas por todos los *usuarios* que utilicen cualquiera de los recursos de la red de comunicaciones del *GCABA* para el acceso a Internet, ya sea porque utiliza una *estación de trabajo* y/o porque utiliza alguno de los recursos de comunicaciones para conectarse.

Quedan prohibidos los siguientes usos de Internet, utilizando *recursos informáticos* del *GCABA* durante el horario laboral o fuera del mismo:

a. Intentar obtener acceso no autorizado o comprometer el desempeño o la privacidad de cualquier sistema de computación.

b. Descargar archivos de video o voz, salvo que los mismos sean para fines laborales. Esta limitación se debe al considerable espacio de almacenamiento que ocupan dichos archivos y la tasa de transferencia que requiere.

c. Realizar cualquier actividad ilegal o contraria a los intereses del *GCABA*, tales como publicar *información* reservada, acceder sin autorización a recursos o archivos o impedir el acceso a otros *usuarios* mediante el mal uso deliberado de recursos comunes.

d. Efectuar cualquier actividad comercial en Internet, excepto que lo haga en representación del *GCABA* mediando autorización expresa.

e. Iniciar cualquier actividad que pueda comprometer la seguridad de los servidores del *GCABA*.

f. Dar a conocer sus contraseñas de acceso o compartirlas con otros *usuarios*. La contraseña es personal y confidencial. De detectarse esta situación el *usuario* quedará automáticamente inhabilitado.

g. Realizar cualquier actividad de recreación personal o de promoción de intereses personales (tales como creencias religiosas, hobbies, etc.).

h. Iniciar sesiones de Internet desde ubicaciones remotas, usando recursos de *información* del *GCABA,* excepto aquellos casos que estén debidamente autorizados por la *ASI*.

i. Utilizar Internet para violar derechos de propiedad intelectual.

j. Aceptar descargas de software propuestas por páginas WEB durante su navegación.

k. Establecer una página como predeterminada, diferente a la intranet de *GCABA*.

l. Intentar eludir o eludir los mecanismos de control y filtrado.

m. Utilizar lenguaje inapropiado.

n. Realizar cualquier actividad que atente contra la moral y las buenas costumbres.

o. Llevar a cabo cualquier práctica que pueda considerarse discriminatoria.

Responsabilidades de los *Usuarios*

Los *usuarios* tendrán las siguientes responsabilidades:

a. Aplicar lo establecido en la presente política.

b. Respetar la presente política para el uso de los *servicios* de Internet y evitar toda práctica que pueda dañar los *recursos informáticos* y/o la *información* del *GCABA*.

c. Tomar en consideración todo requerimiento especial para proteger y acceder a *información* según lo establecido en por la ASI, incluyendo material protegido por las Leyes de Propiedad Intelectual (Ley Nacional N° 11.723, o aquella en su futuro la reemplace) y Protección de Datos Personales (Ley del *GCABA* N° 1.845 y Ley Nacional N° 25.326, o aquella en su futuro la reemplace), o en lo que hace a la privacidad de sus propios datos.

d. Utilizar Internet en forma apropiada (*netiquette*)[1], incluyendo los procedimientos e indicaciones a seguir cuando se usen *servicios* de computadoras remotas y cuando se transfieran archivos de otras computadoras.

e. La *ASI* se reserva el derecho de monitorear las actividades que realicen los *usuarios* en internet. El simple uso de los *servicios* de Internet implica el consentimiento a este monitoreo de seguridad, quedando a criterio de cada *usuario* evaluar su nivel de exposición, de acuerdo con el establecimiento de sesiones que en su mayoría no son privadas.

f. Cada persona es responsable tanto de los sitios, como de la *información* a la que accede con su cuenta de *usuario*, así como también de toda *información* que se copia para su conservación en los equipos del *GCABA*.

[1] Conjunto de normas de comportamiento general en Internet.

ANEXO I

Monitoreo

Todos los accesos pueden ser sujetos a monitoreo y conservación permanente por parte de la ASI.

Los *usuarios* no deben desactivar ninguno de los mecanismos de control definidos por la ASI, tales como programas de filtrado de sitios y contenidos o de monitoreo de accesos.

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a internet, sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0801 - Política de Uso de Equipos Portátiles

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Uso de Equipos Portátiles

1. Introducción

Los *equipos portátiles* son utilizados como herramienta de trabajo profesional, se conectan a la *red de comunicaciones*, se procesa y almacena en ellos gran cantidad de *información* del *GCABA*, en muchos de los casos de tipo confidencial. Es por esto que se deben aplicar medidas de seguridad adecuadas que permitan garantizarla protección de la *información* procesada en dichos equipos.

2. Objetivo

Establecer los lineamientos de seguridad a implementar para el tratamiento de los *equipos portátiles* que procesan, almacenan *información* del *GCABA* o requieran conexión a su *red de comunicaciones*.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Equipos portátiles propiedad del *GCABA*

Los *equipos portátiles* pertenecientes del *GCABA* deben cumplir con las medidas de seguridad definidas para su tratamiento y protección:

a) Asignación y Administración

- Con el fin de que la *ASI* cuente con *información* de la asignación de los equipos portátiles, las áreas de patrimonio de cada *Organismo* mantendrán un registro de los equipos suministrados a los *Agentes* del *GCABA*, en el cual se detalle los datos correspondientes del dispositivo (marca, modelo y número de serie) y del *Agente* del *GCABA* a quien se le ha otorgado el mismo. Dicho registro se deberá encontrar disponible en el caso en que sea requerido por la ASI.

- Para la asignación de un equipo portátil a un *Agente* será condición necesaria que el mismo cuente con un *ID de Usuario GCABA* a través del cual será identificado.

- Las áreas de servicio de los *Organismos* informarán a la *ASI* cuando un *Agente* deje de prestar servicios en el *GCABA*, a fin de proceder a la baja de los accesos y recursos que el usuario tiene asignado.

- Los *Organismos* informarán a la *ASI* cuando sea necesaria la baja o reasignación del *equipo portátil*.

- Los *Organismos* capacitarán al personal que opere equipamiento fuera de las instalaciones del GCABA, con el objeto de cumplir con las pautas de control de acceso y seguridad física requeridas por la *ASI*.

b) Software

- La ASI establecerá el software autorizado que podrá ser utilizado en los equipos portátiles. Dicho software será denominado corporativo y estará a disposición de los usuarios a través de los medios que la ASI determine. Si el software requerido no estuviese disponible dentro de los autorizados, deberá solicitarse a la ASI la aprobación del mismo.
- La *ASI* pondrá a disposición, en caso que el software lo permita, las actualizaciones en línea de manera automática, cuando el usuario se conecte a la *red de comunicaciones* del *GCABA.*

- La instalación de cualquier software en el *equipo portátil* será realizada por los *Agentes de Tecnología Informática* o personal autorizado por la *ASI* para tal fin, quienes son los encargados de instrumentar los medios para aplicar los requerimientos fijados por la ASI en materia de seguridad.

- Si un *Agente* requiere para el desempeño de sus funciones, la instalación de un software de aplicación no disponible en su *equipo portátil*, deberá generar el requerimiento, por medio de los circuitos formales establecidos por la ASI.

- Los requerimientos de instalación de *software de aplicación* deberán ser aprobados por el *Propietario de la Información*, o por la *ASI* cuando se trate de *software utilitario*.

- Los *equipos portátiles* pertenecientes al GCABA no podrán sufrir modificaciones, ni ser remplazadas sus configuraciones de seguridad.

- En el caso de gestiones que impliquen reasignaciones, transferencias o cambio de titularidad del *equipo portátil,* los datos contenidos en el mismo deberán ser eliminados de forma segura antes de ejecutarse la gestión

- Debido al riesgo que implica comprometer los mecanismos de seguridad existentes en recursos informáticos, ningún *Agente* podrá descargar o instalar en el equipo portátil software que no corresponda con el Software Corporativo autorizado por la ASI.

c) Hardware

- La instalación de cualquier hardware será realizado por los *Agentes de Tecnología Informática* o personal autorizado por la *ASI* para tal fin.

- No se permite a los usuarios instalar o desinstalar hardware en los equipos portátiles.

d) Seguro

- Los equipos portátiles que sean retirados de las instalaciones del GCABA, deberán contar para su protección con una adecuada cobertura de seguro para su protección.

Requerimientos de seguridad y uso

Todos los *equipos portátiles* que se conecten a la *red de comunicaciones del GCABA* o bien que almacenen o procesen información perteneciente a éste, deben cumplir con las medidas de seguridad definidas para su tratamiento y protección:

a) Requisitos de Seguridad Lógica

- La información del GCABA almacenada o procesada en los equipos portátiles debe ser protegida de manera de imposibilitar los accesos no autorizados. El mecanismo utilizado para la protección deberá ser aprobado por la ASI.

- Al momento de encender el equipo, el mismo deberá contar con una contraseña o credencial válida de arranque como mecanismo de seguridad por defecto.

- No se permite el arranque del sistema operativo desde cualquier medio de almacenamiento que no sea el disco interno.

- En períodos de inactividad, se deberá implementar el bloqueo automático del *equipo portátil,* mediante contraseña o credencial válida.

- La *ASI* evaluará la necesidad de establecer medidas de autenticación adicionales en aquellos servicios que crea conveniente.

b) Conexión a la red

- No se permite la conexión de los *equipos portátiles* a la *red de comunicaciones* del *GCABA* simultáneamente con otros entornos como son las redes públicas, Internet, vía dispositivos de acceso móvil o redes inalámbricas no controladas.

- Los *equipos portátiles* podrán contar con mecanismos de control de conexiones establecidos por la *ASI*, a fin de prevenir y controlar las conexiones no autorizadas, cuando se encuentre conectado a la *red de comunicaciones del GCABA*.

- El registro de eventos de acceso se mantendrá habilitado para que la *ASI* pueda detectar, en caso de necesidad, cualquier incidente de seguridad o intentos de accesos no autorizados.

c) Seguridad física

- Los equipos no deberán encontrarse desatendidos, cuando se trabaje en oficinas o sean llevados a salas de reuniones, aunque sea por un corto período.

- El *equipo portátil* en caso de ser propiedad del GCABA, debe ser transportado, por el *Agente* del *GCABA*, en el bolso que se le ha asignado, a fin de reducir accidentes de transporte.

- El *equipo portátil* no deberá dejarse en compartimientos o ubicaciones externas a las instalaciones del *GCABA*, ni tampoco estar desatendidos en áreas de paso sin vigilancia o de acceso público. El *Agente* deberá evaluar el riesgo de uso del equipo fuera de las instalaciones y actuar en consecuencia, a fin de minimizar el impacto.

- Si el *equipo portátil* del GCABA o el equipo del tercero fuese sustraído o extraviado durante el transcurso de la prestación del servicio al GCABA, se deberá realizar la correspondiente denuncia policial y notificar de manera inmediata a la *ASI,* a efectos de tomar las medidas tecnológicas necesarias.

d) Software malicioso

- Los *equipos portátiles* pertenecientes al GCABA, deberán tener e instalada, actualizada y habilitada la solución corporativa de prevención de software malicioso definida por la ASI

- Los *equipos portátiles* de terceros o propiedad de Agentes del GCABA tendrán que contar con una solución de prevención de software malicioso con soporte vigente y lista de definiciones actualizada.

Ingreso y egreso de equipos portátiles

Todos los ingresos y egresos de equipos portátiles a los *Organismos*, sean propios del *GCABA* o de terceros, serán registrados dejando constancia de al menos los siguientes datos:

- Marca
- Número de serie
- Persona responsable de la misma (NyA ,DNI)
- Repartición / Empresa a la cual pertenece

- Fecha y hora

Dichos requisitos serán solicitados por el personal de seguridad edilicia, responsable de comprobar la veracidad de los datos y su posterior asiento.

Generalidades

Cualquier violación a la presente política puede derivar en la cancelación del acceso a la *red de comunicaciones* del *GCABA*, sin perjuicio de otras acciones que pudieran corresponder en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0802- Política de seguridad en dispositivos móviles

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de seguridad en dispositivos móviles

1. Introducción

La utilización de *dispositivos móviles* con fines laborales incrementa la productividad, pero como sucede con toda nueva tecnología, puede transformarse en una vía de ataque y tener un impacto negativo en el modelo actual de seguridad si no se implementan los controles adecuados.

Cuando se utiliza un *dispositivo móvil*, se debe garantizar que no se comprometa la información ni la infraestructura de TI del GCABA. Esta política establece los lineamientos a tener en cuenta al trabajar con dichos dispositivos.

2. Objetivo

Asegurar una adecuada protección de la *información* en los dispositivos móviles que se conectan a la *red de comunicaciones, procesen o almacenen información del GCABA*.

1. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

2. Contenido

Asignación y Administración de dispositivos del GCABA

- Con el fin de que la *ASI* cuente con *información* de la asignación de los *dispositivos móvile*s, el área responsable de administración mantendrá un registro de los dispositivos suministrados a los *Agentes* del *GCABA*, en el cual se detalle los datos correspondientes del dispositivo (marca, modelo, número y número de serie) y del *Agente* del *GCABA* a quien se le ha otorgado el mismo. Dicho registro se deberá encontrar disponible en el caso en que sea requerido por la ASI.

- Para la asignación de un dispositivo móvil a un *Agente* será condición necesaria que el mismo cuente con un *ID de Usuario GCABA,* a través del cual será identificado .

- Las áreas de servicio de los Organismos informarán al área responsable de la administración de *dispositivos móviles* cuando un Agente deje de prestar servicios en el

ANEXO I

GCABA, a fin de proceder con las acciones administrativas y tecnológicas correspondientes.

Requerimientos de seguridad y uso

Todos los dispositivos móviles que se conecten a la red de comunicaciones del GCABA o bien que procesen o almacenen información perteneciente a éste, deben cumplir con las medidas de seguridad definidas para su tratamiento y protección:

a. Requisitos de Seguridad Lógica

- La información del GCABA almacenada o procesada en los dispositivos móviles debe ser protegida de manera de imposibilitar el acceso no autorizado. El mecanismo utilizado para la protección, deberá ser aprobado por la ASI.

- La información del GCABA no debe almacenarse en la tarjeta de memoria del dispositivo, excepto que se tomen medidas para el cifrado de la misma.

- Al momento de encender el dispositivo, el mismo deberá contar con una contraseña o credencial válida de arranque como mecanismo de seguridad por defecto.

- En períodos de inactividad, se deberá implementar el bloqueo automático del dispositivo, mediante contraseña o credencial válida.

- En el caso de gestiones que impliquen reasignaciones, transferencias o cambio de titularidad del *dispositivo móvil,* los datos contenidos en el mismo deberán ser eliminados de forma segura antes de ejecutarse la gestión.

- Los *dispositivos móviles* pertenecientes al GCABA no podrán sufrir modificaciones, ni ser remplazadas sus configuraciones de seguridad.

b. Conexión a la red de comunicaciones del GCABA

- Los *dispositivos móviles* podrán contar con mecanismos de control de conexiones establecidos por la *ASI*, a fin de prevenir y controlar accesos no autorizados, cuando se encuentre conectado a la *red de comunicaciones del GCABA*.

- Se encontrará habilitado el registro de eventos de acceso para que la *ASI* pueda detectar, en caso de necesidad, cualquier incidente de seguridad o intentos de accesos no autorizados sobre aquellas conexiones provenientes de dispositivos móviles.

c. Software malicioso

- Cuando se sospeche de una infección que no fuere detectada por la solución de Antivirus Corporativo, la ASI podrá cancelar el acceso del dispositivo móvil a la red de comunicaciones del GCABA, sin perjuicio de otras acciones que pudieran corresponder en el ámbito administrativo, civil o penal

d. Seguridad física

- Los dispositivos no deberán encontrarse desatendidos cuando se trabaje en oficinas o sean llevados a salas de reuniones o espacios públicos, aunque sea por un corto período de tiempo.

- Si el dispositivo fuese sustraído o extraviado se deberá notificar de manera inmediata al Organismo que asignó el dispositivo, o sector que se encarga de la gestión de los dispositivos, a efectos de tomar las medidas tecnológicas necesarias. Siempre que la tecnología lo permita, se efectuará el borrado remoto de la información contenida en el mismo, de manera que no pueda ser accedida por personas no autorizadas.

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0803 - Política de Registro de Eventos en Servicios de TI

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Registro de Eventos en Servicios de TI

1. Introducción

Para garantizar un adecuado esquema de seguridad frente a los accesos a los recursos de infraestructura de TI y el software del GCABA, es indispensable contar con mecanismos de registro de eventos, que garanticen la trazabilidad y faciliten el posterior monitoreo de los accesos y actividades realizadas sobre dichos recursos.

2. Objetivo

Definir las pautas generales para asegurar una adecuada registración de eventos relacionados con los servicios de TI del GCABA, maximizando la trazabilidad de los mismos.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

A fin de efectuar un adecuado registro de los eventos relacionados con la seguridad de la información, se deben tener en cuenta las siguientes consideraciones en la registración de eventos.

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información, a fin de permitir la detección e investigación de incidentes., violación o infracción normativa en el acceso o uso de los recursos de infraestructura de TI, software de base y software de aplicación del GCABA.

Registro de los eventos de auditoría

Todo el hardware y software empleado debe permitir la registración automática y explotación de la información considerada como evento de auditoría.

ANEXO I

Todo software de base y de aplicación implementado en GCABA debe brindar facilidades de registro automático de eventos, pudiendo utilizarse software complementario en aquellos casos en los que el software de base o la aplicación no posea dicha funcionalidad.

Los registros se llevarán y mantendrán de forma cronológica de acuerdo con las operaciones efectuadas por el sistema u aplicación.

Los registros contendrán información que permita identificar al usuario, el evento o acción realizada, los recursos involucrados y el registro cronológico, como mínimo. Adicionalmente, deberán contar con controles de seguridad apropiados a fin de evitar su alteración.

Todos los registros serán tratados como información de criticidad alta de acuerdo con lo establecido por la ASI y en función del nivel de clasificación asignado.

Los usuarios no poseerán permisos de modificación sobre los archivos de configuración, ni tampoco podrán acceder a funcionalidades que permitan deshabilitar la grabación de registros de eventos. Se deben tomar las medidas de seguridad necesarias para garantizar su protección frente a intentos de eliminación u modificación no autorizados.

Los registros de eventos estarán previstos para generar trazas que permitan detectar, diagnosticar, auditar y analizar, tanto problemas de seguridad, como aspectos relacionados con el tratamiento de la información, y la detección de errores accidentales.

Gestión del registro de eventos

De ser posible técnicamente, la ASI consolidará automáticamente todos los eventos de forma centralizada considerando como elementos clave la automatización (configuración inicial y revisión posterior si fuese necesario), el tipo de almacenamiento y la compresión.

De acuerdo a las directrices establecidas por la ASI, los resguardos de registros de eventos deberán realizarse de forma independiente a los resguardos de la información en producción

El Propietario de la Información cuyos eventos sean registrados, podrá acceder al archivo de resguardo de registros de eventos, solo con permisos de lectura. Asimismo, con la debida autorización podrá acceder el personal de Sindicatura General y el personal de Unidad de Auditoría Interna (UAI).

Registro de eventos para software de aplicación

El registro de este tipo de eventos poseerá en su alcance la registración de todos aquellos cambios o acciones críticas que se realicen dentro de las bases de datos o repositorios con los cuales opere la aplicación; estos cambios se ejecutan a través de transacciones, las cuales deben quedar registradas.

ANEXO I

Para que un registro de eventos transaccionales cumpla con la finalidad requerida, deberá realizarse un análisis y estudio previo de la información que procesa cada aplicación y cuáles son las necesidades de trazabilidad de la misma; en concordancia con los criterios de clasificación de la información establecidos por la ASI.

Partiendo de la base de que cada acción / transacción que procesa el software de aplicación va a generar un nuevo evento, todas las acciones, cualesquiera sean, van a compartir un set de datos informativos básicos y obligatorios, que se registrarán siempre. De esta manera, se obtiene la trazabilidad y la referencia del cambio de la información, se recogen las modificaciones de datos y se detalla cual fue la actividad general del software de aplicación.

Existe, para estos casos, información general como identificación de usuario que realiza la acción, fecha hora, identificación del equipo, ubicación, transacción ejecutada, información de la acción, entre otras, que deberá registrarse de forma obligatoria y será aplicable al software en ambientes de producción dentro del ámbito del GCABA.

Asimismo existe información particular de resguardo. La información particular y de gestión de gobierno, que impactará en los registros de auditoría de cada software de aplicación deberá ser evaluada al momento de realizar el análisis de la misma, teniendo en cuenta y definiendo lo que se quiere controlar, el tráfico de información de mayor riesgo y la sensibilidad que posee la ejecución de validaciones, cambios o consultas especificas. El Propietario de la Información de cada Organismo, tendrá sus registros de eventos alineados con sus misiones y funciones, los cuales deberán ser validados con la Unidad de Auditoría Interna que le corresponde.

Para todo el software de aplicación que se opere dentro del ámbito del GCABA, el Organismo adquiriente o desarrollador del software deberá incorporar como mínimo, en los registros de eventos las acciones o actividades realizadas con:

- Información reservada, de acuerdo con lo definido por la ASI.
- Todo dato que pueda en su contexto, modificar valores monetarios.
- Modificaciones a datos presupuestarios, catastrales o impositivos.
- Cualquier dato personal, de conformidad a lo establecido en la Ley Municipal (Ley 1845/05)
- Modificaciones en el modelo de autorización del software de aplicación.

Para la implementación de un nuevo software, la configuración y el contenido de los registros de eventos deberán ser aprobados por la Sindicatura General en conjunto con la ASI, quienes aprobarán u observarán los correspondientes registros, antes de ser incorporados en el ambiente productivo de la ASI. Los cambios posteriores a las aplicaciones productivas deberán cumplir idénticos requerimientos y serán

evaluados previamente a su implementación por la ASI, quienes darán intervención a la UAI del Organismo, en caso de ser necesario para su aprobación.

Auditoría de base de datos por fuera de una aplicación

Toda modificación de los datos operativos del ambiente de producción por fuera del software de aplicación y que se realice por excepción justificada y aprobada, deberá reflejar el cambio en los registros de eventos correspondientes, como requisito obligatorio para la ejecución de dicha modificación.

En el caso en que el recurso tecnológico lo permita, se deberá activar la automatización de registración de actividades, a fin de evidenciar cualquier tipo de instrucción ejecutada sobre los repositorios de datos.

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0804 - Política de Control de Eventos en Servicios de TI

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Control de Registros de Eventos en Servicios de TI

1. Introducción

A fin de monitorizar todos los sucesos importantes que se producen en los sistemas informáticos del GCABA y poder anticiparse a los problemas, resolverlos o incluso prevenirlos, se debe realizar un control sobre los eventos capturados en los registros. A efectos de la operación del servicio, se denomina evento a todo suceso detectable que tiene importancia para la estructura de TI, para la prestación de un servicio o para la evaluación del mismo. Por ejemplo, notificaciones creadas por los servicios, los elementos de configuración o las herramientas de monitoreo y control.

2. Objetivo

Definir las pautas generales para asegurar una adecuada identificación y seguimiento de los eventos en los servicios de TI registrados en los sistemas del GCABA.

Asegurar que se registren y se evalúen todos los eventos significativos para la seguridad de accesos

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

La *ASI* realizará un control sobre todas las actividades registradas en los *recursos informáticos* y *recursos de infraestructura IT* del *GCABA*. Para el caso del *software de aplicación*, la *ASI* realiza el registro de los eventos y su guarda, recayendo el control de esos eventos en el Propietario de la Información del Organismo al que pertenece el mismo, quienes son los responsables de indicar la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

A fin de efectuar un adecuado control de los eventos relacionados con la seguridad de la información, se deben tener en cuenta las siguientes consideraciones:

ANEXO I

Clasificación de eventos

La ASI reconoce la siguiente tipología de eventos a aplicar:

a. Eventos informativos: Se utiliza la ocurrencia de estos eventos con el fin de reunir información sobre el hardware, el software, los problemas del sistema y los hechos que sean oportunos se informe a la ASI. Son sucesos cuya ocurrencia no implica una amenaza potencial para la gestión de los servicios de TI, sino que tan sólo son reportados como medida preventiva y con la finalidad de lograr el control interno.

b. Eventos de advertencia: Eventos que no son necesariamente significativos, pero podrían indicar un posible problema futuro para el mantenimiento de la gestión de los servicios de TI.

c. Eventos de alerta: Eventos que pueden afectar la continuidad de los servicios de TI ó que pueden constituir una violación a la seguridad informática.

Existen eventos que por sí mismos pueden caer dentro de una de las categorías pero, en conjunto con otros eventos, pueden configurar una situación de mayor nivel de riesgo.

Acceso a la información de los registros

Los registros de eventos serán accedidos por personal autorizado de la ASI, pudiendo disponer de la utilización de herramientas o software apropiados para llevar a cabo el control de los mismos.

Sindicatura General de la Ciudad, tendrá acceso al control de los registros de eventos y tiene la capacidad de efectuar recomendaciones sobre modificaciones a los aspectos de seguridad. Las Unidades de Auditoría Interna de cada Organismo también tendrán la misma disponibilidad de acceso, pero restringido a la información del ámbito de incumbencia de la misma.

Los Órganos de Control u otros Organismos que requieran acceso a la información deberán contar con la correspondiente notificación del Propietario de la Información indicando el alcance y la justificación de la solicitud. La información a acceder será brindada por la ASI en la medida que los sistemas lo permitan. La recuperación de la información será realizada por personal experimentado y adecuadamente habilitado por la ASI.

El usuario autorizado para llevar a cabo los procesos de generación de copias de resguardo de los registros de eventos solo deberá tener los accesos que su función requiere, es decir, no contando con acceso al contenido de los mismos. Los agentes que realizan las funciones de revisión y aquellos cuyas actividades están siendo monitoreadas, deberán encontrarse obligatoriamente separadas.

No está permitida la eliminación de los registros de eventos, a menos que se trate de una depuración programada y realizada por personal autorizado por la ASI.

No está permitida la desactivación de la herramienta de registro, la alteración de eventos registrados o la sobrescritura de los mismos. La ASI ejecutará los controles de acceso necesarios a fin de garantizar que no ocurran dichas situaciones.

La ASI realizará revisiones periódicas de los registros de eventos obtenidos, con el fin de analizar las actividades definidas para tal fin y generará un registro de dichas revisiones

Ante situaciones de anormalidad, la ASI evaluará la necesidad de notificación al Propietario de la Información cuyas actividades están siendo monitoreadas, acerca de las anomalías detectadas determinando de manera conjunta la severidad del hallazgo y las acciones a tomar que sean necesarias, en caso de corresponder.

Disponibilidad de espacio para el almacenamiento de los registros de eventos

El Propietario de la Información cuyas actividades serán registradas, deberá proveer los medios necesarios para asegurar la disponibilidad de espacio para el almacenamiento de los registros de eventos.

La ASI mantendrá informado al Propietario de la Información sobre el estado situacional y la disponibilidad del espacio de almacenamiento de los registros de eventos.

Se podrá evaluar de manera conjunta con el Propietario de la Información de los eventos registrados, la limitación de los registros, contando con una debida justificación, notificaciones y acuerdo de la Unidad de Auditoría Interna correspondiente al Organismo.

La ASI determinará el plan de depuración necesario, y el cronograma de realización de las copias de resguardo de los registros, disponiendo los medios y acciones necesarias para que los permisos de acceso establecidos sobre el recurso informático cumplan con las medidas de seguridad y control establecidas.

Protección de registros de eventos

Los registros de eventos deberán ser almacenados históricamente en línea o en medios de almacenamiento que aseguren su recuperación en caso de ser necesario.

Los archivos de registro de eventos deberán encontrarse protegidos contra accesos no autorizados, cualquiera sea su medio de almacenamiento.

Se prohíbe la modificación o alteración de los archivos de registro de eventos almacenados.

ANEXO I

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0805 - Política de Administración de Usuarios GCABA

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Administración de Usuarios *GCABA*

1. Introducción

Es fundamental identificar a cada persona que utiliza un *recurso informático* del *GCABA*, manteniendo un registro completo y actualizado de los datos del mismo, el área donde presta servicios y su superior directo, entre otros. Este registro conforma el padrón de usuarios del *GCABA* y requiere la implementación de ciertas medidas para una adecuada administración del mismo.

En esta política se establecen los lineamientos principales que deberán seguirse al momento de crear, modificar o remover usuarios *GCABA*, además de otras consideraciones que deberán cumplirse en el tratamiento de los mismos.

2. Objetivo

Establecer los lineamientos que permitan asegurar una adecuada administración de los *usuario*s del *GCABA*.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Usuarios *GCABA*

La *ASI* establece las siguientes consideraciones y condiciones para la administración de usuarios de los sistemas y servicios informáticos:

a. La identificación de los usuarios en los sistemas y servicios informáticos del *GCABA* se realiza por medio de un ID de *Usuario GCABA*.

b. Todo *Agente* que preste servicio dentro del ámbito del *GCABA*, y que sus funciones requieran acceso a *información digital*, datos, *servicios*, *software de aplicación* o *software de base*, deberá estar acreditado con un ID de *Usuario GCABA* para el desempeño de las mismas.

c. El ID de *Usuario GCABA* identifica unívocamente a una persona física en particular. Es, para cada usuario, único, nominal e intransferible.

d. El ID de *Usuario GCABA* debe tener *asociado l*os datos de la persona responsable del mismo –usuario-, incluyendo su CUIT/L, tipo de contratación, repartición, lugar donde presta servicios en el *GCABA, el sup*erior directo, datos de contacto, ent*re ot*ros.

e. Los Agentes que no posean un ID de *Usuario GCABA*, *no podrá*n *acce*der a los *recursos informáticos* del *GCABA*.

f. La administración y el registro de *los IDs* de *Usuario*s *GCABA* es responsabilidad de las áreas de servicio de cada *Organismo*.

g. La nomenclatura empleada para los *IDs de Usuarios GCABA* seguirán las recomendaciones establecidas por la ASI dentro del Marco Normativo de TI.

Altas, bajas y modificaciones de IDs de Usuarios *GCABA*

La *ASI* establece los siguientes requisitos y condiciones para las altas, bajas y modificaciones de los ID de *Usuario*s *GCABA*:

a. Alta de ID de Usuario *GCABA*

- Solicitud

  La solicitud debe ser realizada por el Director General, Equivalente o Superior Jerárquico de la repartición a la cual pertenece el Agente que requiere el ID de usuario. Todas las solicitudes deben ser generadas y enviadas al *área de servicios* del Organismo de pertenencia indicando como mínimo, los siguientes datos del usuario:

  - Nombre y Apellido
  - CUIT/L
  - Tipo de contratación
  - Repartición donde presta servicios en el *GCABA*
  - Superior jerárquico
  - Datos de contacto (establecimiento, teléfono)

  Las áreas de servicio son las administradoras de los accesos a correo electrónico, internet y mensajería. En la solicitud se deberá indicar si el usuario requiere alguno de estos servicios.

- Implementación

El *área de servicios* del *Organismo* tiene la capacidad de aprobar o rechazar las solicitudes de alta, en base a los datos recibidos. En caso de ser aprobada generará un nuevo ID de *Usuario GCABA* y asignará, el acceso a los servicios requeridos.

En caso de rechazo de la solicitud, el *área de servicios* del *Organismo deberá* comunicar al solicitante los motivos del rechazo.

b. Baja y Desactivaciones de ID de Usuario *GCABA*

Se deberá dar de baja el usuario cuando éste deje de prestar servicios para el *GCABA*, ya sea por rescisión del contrato, renuncia o cualquier otra situación que amerite el cese de funciones.

Se consideran desactivaciones de usuario a aquellas inhabilitaciones temporales realizadas en los sistemas, en las cuales se desea conservar el ID del usuario. Los IDs de Usuarios *GCABA* desactivados se reservarán y podrán ser posteriormente reactivados o dados de baja, según corresponda. La reactivación debe ser solicitada por el superior jerárquico inmediato del usuario o por el Director General, Equivalente o Superior Jerárquico de la repartición a la que pertenece.

La baja o desactivación de ID de usuario, impide al mismo la utilización de servicios o accesos que tenga asociados y habilitados para ese ID de usuario.

Tanto las bajas como desactivaciones siguen el siguiente lineamiento:

- Solicitud

Debe ser solicitada al área de servicios del Organismo, por el superior jerárquico inmediato del usuario o Director General, Equivalente o Superior Jerárquico de la repartición.

- Implementación

El *área de servicios* dará de baja el ID de *Usuario GCABA* en el sistema. La baja de un ID de *Usuario GCABA* se realiza en primer instancia como baja "lógica", deshabilitando o bloqueando el ID, manteniendo los datos y reserva del mismo. Se podrá reactivar el ID de Usuario *GCABA* en caso de ser necesario y contando con la autorización correspondiente.

La baja "física" del ID de *Usuario GCABA* implica su eliminación de los *sistemas informáticos* y se realizará con la autorización del Director General, Equivalente o Superior Jerárquico de la repartición a la que pertenecía el Agente.

c. Modificación de ID de Usuario *GCABA*

Existen dos tipos de cambios para la modificación de los IDs de *Usuario*s *GCABA*: el cambio de datos particulares de contacto y el cambio de datos críticos. El primero los

podrá llevar adelante el mismo Usuario, mientras que el segundo, correspondientes a sus datos de identificación y de relación laboral con el GCABA, deben ser verificados y ejecutados por las áreas de servicio.

Es responsabilidad del usuario verificar que sus datos se encuentren correctos y actualizar sus datos particulares de contacto, tales como teléfonos y lugar físico (dirección y piso) de la repartición en donde presta servicios, a través de la aplicación que se encuentra dispuesta para tal fin en la intranet del *GCABA*.

Es su responsabilidad dar aviso al área de servicio de su Organismo, en caso en que los datos considerados críticos no se encuentren correctos y actualizados.

- Solicitud

  La modificación de datos críticos del usuario debe ser solicitada por el superior jerárquico inmediato o funcionario a cargo de la repartición a la que pertenece el usuario y notificada al *área de servicios* del *Organismo* correspondiente. Los datos críticos a modificar incluyen:

  - Cambio de Repartición dentro del mismo Organismo
  - Cambio de Superior Directo
  - Cambio de Tipo de Contratación
  - Requerimiento / Anulación de Servicios de Internet, Correo o Mensajería

- Implementación

  El área de servicio deberá realizar el mantenimiento de *información* sensible, según lo solicitado por el superior jerárquico inmediato o funcionario a cargo de la repartición a la que pertenece el usuario y de acuerdo a los cambios de personal que se susciten en el *Organismo*, solicitando a quien corresponda en cada caso la actualización de la información.

d. Transferencia de Usuario *GCABA*

La transferencia de usuario se utiliza en aquellos casos en donde un Agente deje de brindar servicios en una repartición, para comenzar a operar en otra. El área de servicios del Organismo al cual pertenecía el usuario deberá transferirlo.

El usuario transferido continuará habilitado pero no poseerá datos de pertenencia con la antigua repartición, pasando a formar parte del repositorio de usuarios transferidos, hasta tanto lo tome como propio el nuevo Organismo al cual se transfiere.

La transferencia puede implicar la remoción de accesos a información y recursos informáticos, continuando en actividad los servicios de correo, uso de internet y mensajería.

El área de servicios del Organismo destino, tomará al usuario como propio incorporándole todos los datos de referencia y, a partir de allí, el ID de Usuario queda activado y habilitado para asignarle los accesos correspondientes a sus nuevas funciones. El usuario no podrá quedar sin repartición asignada. Es responsabilidad del usuario asegurar que sus datos de pertenencia sean correctos.

Si el *Usuario GCABA* no tiene asignado una repartición por seis meses consecutivos, la *ASI* procederá a ejecutar la desactivación del mismo.

Usuarios Externos

Los *usuarios externos* se generarán en el padrón de usuarios como "usuarios ajenos al GCABA" y contarán con tiempo limitado de habilitación del servicio, el cual podrá ser solicitado nuevamente en caso de necesidad. Una vez vencido el tiempo de habilitación establecido, se dará de baja al usuario de manera automática previo aviso al funcionario solicitante.

Los usuarios externos solo podrán tener acceso a los siguientes servicios:

- Internet.
- Aplicaciones.

Los usuarios externos no se encuentran habilitados para el uso de una cuenta de correo del GCABA.

La administración de estos usuarios es responsabilidad de cada una de las áreas de servicio del Organismo que tiene relación con el usuario externo, a través de la misma metodología para solicitudes de ID de usuarios *GCABA*. La administración de acceso a las aplicaciones y servicios debe seguir los lineamientos establecidos por la *ASI*.

Compromiso del Usuario

Los usuarios, sean internos o externo, son responsables por todas las acciones que se realicen con su ID de usuario en los recursos y sistemas informáticos del *GCABA*.

La *ASI* propicia que todos los usuarios, internos o externos, a quienes se les habilite un ID de *GCABA* suscriban, con los organismos correspondientes, un compromiso de responsabilidad y confidencialidad del uso de su usuario, contraseña y de la *información* residente en los sistemas informáticos a los que acceda.

ANEXO I

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0806 - Política de Administración de Usuarios en Custodia

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Usuarios en Custodia

1. Introducción

En los diferentes ambientes de procesamiento y *recursos informáticos* existen cuentas específicas que poseen permisos especiales con los cuales es posible efectuar actividades sensitivas como por ejemplo la instalación y actualización de software, habilitación de servicios, accesos, cambios en la configuración u otros.

Estas cuentas deben ser utilizadas sólo en ocasiones de emergencia en donde una necesidad o fuerza mayor lo requiera. Debido a las acciones críticas que se pueden llevar a cabo, se requiere que todas las actividades que se realizan a través de las mismas, sean registradas y controladas.

2. Objetivo

Establecer las medidas de control para la utilización de *usuarios en custodia* que poseen privilegios en los sistemas aplicativos, software de base y equipamiento tecnológico del *GCABA*, de manera que los mismos sean utilizados solo en situaciones de emergencia que lo ameriten.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Se establecen las medidas de control a realizar desde que se genera la necesidad de acceso al ambiente de producción a través de cuentas de usuarios en custodia -durante una situación de emergencia-, hasta la revisión posterior de las acciones realizadas, la regeneración de la contraseña de acceso y custodia de la misma.

Usuarios en Custodia

Se considera usuarios en custodia a:

g. Toda cuenta por defecto del software que:

- posea características de administrador.

- sea capaz de realizar tareas críticas que pudieran afectar tanto la información como cualquiera de los recursos informáticos productivos (*equipos de procesamiento y almacenamiento centralizado*, equipos de comunicaciones y de seguridad, u otros).

- pueda ejecutar procesos con un dominio total del equipo de procesamiento centralizado.

- permita crear nuevos usuarios o modificar los accesos de los existentes.

h. Todos aquellos usuarios no nominales que se encuentran incorporados en el *software de aplicación* y que posean permisos especiales para la comunicación y gestión de *recursos informático*s del *GCABA*, y que en su función de uso puedan afectar de manera real o potencial la continuidad de los servicios o *información digital* del *GCABA*.

i. Todos aquellos usuarios no nominales que posean permisos críticos en las aplicaciones y que la ASI considere necesario resguardar su contraseña.

Los usuarios en custodia son usuarios de utilización limitada, aplicables solo en casos de emergencia que no puedan ser resueltos a través de ningún otro medio, a fin de garantizar la continuidad operativa.

Responsabilidades

La *ASI* identificará los *usuarios en custodia* de cada uno de los sistemas y *recursos informáticos*, y será quien genere, conserve y resguarde las credenciales (usuario y contraseña) en sobres lacrados y etiquetados con los datos referenciales del sistema y el *recurso informático* al que pertenece, *usuario en custodia* y datos de trazabilidad para el seguimiento y utilización de los mismos.

El *Propietario* y la *ASI*, son responsables por la correcta asignación de los permisos otorgados frente a una contingencia. Además, en conjunto definirán los *Agentes* capacitados y habilitados para utilizar los usuarios en custodia en los sistemas o *recursos informáticos* donde se almacena la información bajo su responsabilidad, identificando que usuario en custodia podrá acceder cada uno de ellos.

La *AS*I generará las contraseñas de los *usuarios en custodia*, así como también el cambio de la contraseña utilizada.

Solicitud de uso de los usuarios en custodia

Frente al acontecimiento de una emergencia o un caso particular en el que se requiera utilizar un *usuario en custodia*, el requirente deberá presentar una solicitud formal a la *ASI*, indicando la siguiente información:

- Datos del solicitante

- Repartición de pertenencia

- Usuario en custodia a utilizar.

- Recurso al que se va a acceder.
- Justificación de la solicitud.
- Actividades a realizar.
- Tiempo estimado de utilización del *usuario en custodia*.

La *ASI* validará que el *Agente* se encuentre autorizado a solicitar el *usuario en custodia*. Si el solicitante no se encuentra autorizado, la solicitud será rechazada y la *ASI* informará al *Agente* los motivos de su rechazo y notificará al Responsable correspondiente.

La apertura de los sobres que contienen las credenciales de los *usuarios en custodia*, deberá realizarse con la autorización explícita de la máxima autoridad de la *ASI* y, en caso de tratarse de un usuario de aplicación, también deberá contar con la autorización del *Propietario*.

La *ASI* dejará registro de la apertura del sobre y verificará que se encuentre habilitado el registro de auditoría del *usuario en custodia*.

Utilización de usuarios en custodia

Los *usuarios en custodia* deben ser utilizados exclusivamente por el *Agente* autorizado por la *ASI* y por el *Propietario*.

Todo *Agente* del *GCABA* que utilice un *usuario en custodia* es responsable de informar las acciones realizadas al Propietario que corresponda. Una vez finalizado la utilización del *usuario en custodia, se d*eberá informar de manera inmediata a la *ASI* y al Propietario que ha solicitado el acceso.

La *ASI* dejará registro de la finalización del uso del *usuario en custodia* y procederá a la generación de una nueva contraseña.

En caso de que la solicitud de excepción por la cual se requirió el usuario en custodia haya sido resuelta y el *Agente* no informó la finalización de su uso, o que el tiempo autorizado haya expirado, la *ASI* podrá realizar el cambio de contraseña del *usuario en custodia*, notificando sobre la situación al *Agente* y al Responsable que lo autorizó.

Cambio de la contraseña

La *ASI* realizará el cambio de contraseña de los *usuarios en custodia*, cada vez que finalice el uso y de forma periódica. La definición de la contraseña será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.

Una vez realizado el cambio se volverá a ensobrar la contraseña en un sobre lacrado, registrando la fecha en la que se realizó la modificación y los datos de trazabilidad necesarios.

El resguardo de la contraseña quedará bajo responsabilidad y custodia de la *ASI.*

ANEXO I

Control de actividades realizadas

Todas las acciones realizadas con el *usuario en custodia* serán trazables y registradas. La *ASI* validará, a partir del registro de actividades realizadas, que solamente se hayan ejecutado las tareas que fueron autorizadas.

Cada vez que finalice la utilización del usuario en custodia o se cambie su contraseña, el evento quedará documentado.

La *ASI* llevará un registro de la utilización del *usuario en custodia* conteniendo al menos la siguiente información:

- Fecha /hora de entrega de *usuario en custodia*
- Fecha / hora de inicio de operaciones
- Agente habilitado para el uso
- Motivos para utilizar el usuario en custodia
- Tareas realizadas con el usuario en custodia
- Fecha /hora de fin de actividades

Generalidades

La *ASI* podrá determinar las acciones a tomar en el caso de incumplimiento a los puntos de la presente política una vez evaluadas las consecuencias, que sobre los recursos y servicios informáticos del *GCABA* se haya podido ocasionar. Todo ello sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI.* En caso de conflicto de interpretación se resolverá de buena fe y de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0807 - Política de Administración de Contraseñas

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Administración de Contraseñas

1. Introducción

A los efectos de proteger tanto la *información digital* como los *recursos informáticos* del *GCABA* se deben tomar las medidas de seguridad necesarias y aplicar controles de acceso. La efectividad de estos controles, en su gran mayoría, depende de la manera en que se apliquen.

La *autenticación* permite verificar la identidad del usuario que requiere conectarse a un *recurso informático* y el control de acceso permite asegurar que el *sistema o recurso informático* es utilizado solamente por aquellos usuarios autorizados. La *autenticación* del usuario a partir de contraseñas forma parte de estos controles, con lo cual una correcta administración de las claves resulta indispensable para lograr la protección deseada.

2. Objetivo

Asegurar una adecuada administración de las contraseñas de *usuarios* a los *recursos informáticos* del *GCABA* durante su generación, modificación, utilización y almacenamiento.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Todo usuario que acceda a cualquier *recurso informático* del *GCABA* debe tener asociado obligatoriamente un *ID* y una clave de acceso o contraseña, la cual es personal, confidencial, intransferible y de exclusiva responsabilidad del usuario.

Se deberán contemplar los siguientes requisitos para una adecuada administración de las contraseñas de usuarios; siempre que sea técnicamente posible:

Requisitos generales de seguridad de las contraseñas

a. Deben permanecer cifradas utilizando un algoritmo unidireccional y residir en archivos ocultos y protegidos.

b. No deben ser visibles por pantalla al momento de ser ingresadas.

c. No podrán estar en blanco (nulas).

d. No debe contener información personal o de fácil identificación del usuario (por ejemplo, DNI, domicilio, teléfono, fecha de nacimiento y fecha de ingreso).

e. No debe ser impresa en listados del sistema, ni escrita en lugar visible a otras personas.

Características de las contraseñas

Las características de las contraseñas pueden variar para la autenticación de los usuarios de dominio, usuarios en custodia y usuarios administradores de equipos de seguridad y comunicaciones. A continuación se describen las características de las contraseñas que la *ASI* establece para cada caso:

a. Contraseñas para usuarios de dominio, servicios y software de aplicación:

- Establecer una longitud mínima de ocho (8) caracteres.
- No permitir identificadores de usuario (nombre, apellidos o ID).
- Obligar la utilización de contraseñas compuestas por la combinación de caracteres especiales, números y letras mayúsculas y minúsculas.
- Bloquear el usuario frente a repetidos intentos de acceso.
- Obligar su cambio cuando el usuario ingrese por primera vez al sistema o servicio.
- Solicitar el cambio obligatorio de la contraseña de forma periódica.
- Conservar un histórico de los sucesivos cambios a fin de evitar su reutilización de forma no controlada.

b. Contraseñas para utilizar con los *usuarios en custodia*.

- Para los *usuarios en custodia* se aplicarán los mismos criterios que para los usuarios de dominio, servicios y software de aplicación. Para estos usuarios se establecerá una longitud mínima de quince (15) caracteres.

c. Contraseñas a utilizar en la administración de equipos de seguridad o de comunicaciones, por ejemplo routers, proxy, firewall, IDS, otros.

- Todos los equipos de seguridad y comunicaciones utilizarán usuarios nominales (usuarios *GCABA*), por tal, las características de las contraseñas se alinearán con las utilizadas en los accesos a servicios y software de aplicación.

- Las contraseñas predeterminadas por hardware o software (superusuario / root) deberán ser ensobradas y guardadas siguiendo los lineamientos establecidos para usuarios en custodia y se adecuarán los accesos para ingresar a través de usuarios *GCABA.*

- De ser necesario podrán existir equipos de seguridad o comunicaciones que cuenten con dos (2) factores de *autenticación,* que incluya como primer factor la utilización de clave de acceso y como segundo factor una medida seguridad superior (filtros, certificados u otros).

Bloqueo y desconexión de usuarios

- Cuando el usuario se haya bloqueado o sea necesario restablecer su clave, sólo el *Administrador de Accesos* correspondiente podrá desbloquearlo.

- Todo usuario que no haya accedido al sistema por (60) días corridos será bloqueado. El Administrador de Accesos correspondiente iniciará los procesos de autorización necesarios para darlo de baja definitivamente en caso de corresponder. Ante situaciones de carácter excepcional y previa autorización formal por parte del Director General, Equivalente o Superior Jerárquico a cargo de la repartición de pertenencia del usuario, se mantendrá activo.

- Se desconectará toda sesión activa cuando la estación de trabajo no verifique uso.

Responsabilidad de los usuarios

Todos aquellos usuarios de los *servicios*, software y *recursos informáticos* del *GCABA* que tienen asignada una cuenta o cualquier otro tipo de acceso en los sistemas del *GCABA,* son responsables de cumplir con las siguientes pautas de seguridad:

a. Deberán cambiar periódicamente sus contraseñas y, en caso de sospechar que alguna de ellas es conocida por otros usuarios, cambiarla inmediatamente.

b. No podrán compartir su identificador de usuario y clave con otras personas.

c. No deberán revelar su contraseña a NADIE, ni siquiera a aquellos que hablen en nombre de la *ASI* o de un superior del *GCABA.*

d. No deberán revelar la contraseña en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica.

e. No deberán escribir la contraseña en papel. Tampoco almacenar las contraseñas en archivos en su estación de trabajo sin proveerlo de algún mecanismo de seguridad.

f. No deberán revelar su contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.

g. No deberán utilizar la característica de "Recordar Contraseña", en ninguna aplicación o servicio que posea esta opción.

h. Cuando, por razones de ausencias prolongadas, deba reemplazarse la tarea de un usuario, no está permitido la utilización de su cuenta de identificador y clave de acceso por otra persona. En estos casos, el sector del cual el usuario se ausente y desempeña sus funciones, debe designar su reemplazante y solicitar los accesos correspondientes para éste, quien debe siempre acceder identificándose con su propio identificador y clave de acceso.

Administración de las contraseñas

La administración y entrega de las contraseñas de usuarios del *GCABA* será realizada por las *áreas de servicios* de los Organismos, quienes tendrán en cuenta los siguientes puntos:

a. Las *áreas de servicio* de los Organismos serán las únicas con capacidad entregar, blanquear y restablecer las contraseñas de usuarios *GCABA* siguiendo los procedimientos normados.

b. La contraseña otorgada por el *área de servicios* será generada mediante un algoritmo, brindando una clave de acceso aleatoria inicial para cada usuario.

c. La entrega de la contraseña inicial se realizará a través de un medio seguro que garantice que la misma puede ser recibida solo por el usuario al cual se le generó la clave.

d. En la entrega de la primera clave o ante un blanqueo de contraseña, el usuario deberá proceder al cambio de la misma en el próximo inicio de sesión, cualquiera sea el *recurso informático* a acceder.

e. Las *áreas de servicio* podrán revocar las contraseñas de los usuarios *GCABA*, cuando las mismas se encuentren comprometidas o cuando el usuario se desvincule del organismo.

Generalidades

Se considera falta grave que el usuario que revele a otra persona su propia clave de acceso o solicite la revelación de una clave de acceso que no le corresponda.

Cualquier violación a esta política puede derivar en la cancelación inmediata de la cuenta, sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

ANEXO I

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI.* En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0808 - Política de Administración de Accesos a Software de Aplicación

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Administración de Accesos a Software de Aplicación

1. Introducción

La administración accesos de *usuarios* a las aplicaciones del *GCABA* es una parte fundamental para la seguridad de la *información*. Es de vital importancia poder identificar a cada una de las personas que utilizan las aplicaciones del *GCABA*, además de determinar los permisos de acceso que tienen o podrán tener, teniendo en cuenta las funciones que ellos desempeñan en el *GCABA*.

En esta política se establecen los lineamientos principales a tener en cuenta al momento de otorgar, modificar o remover accesos de *usuario*s a aplicaciones.

2. Objetivo

Establecer los lineamientos que permitan asegurar una adecuada administración de los accesos de *usuario*s al software de aplicaciones del *GCABA*.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Condiciones requeridas sobre el software de aplicación

Todo software de aplicación implementado (ambiente de Producción) deberá contar con un modelo de autorización de usuarios y perfiles, a fin de controlar el acceso a funcionalidades, información o a aplicaciones, a través de una adecuada segregación los mismos, conforme a los niveles de criticidad que el software posea.

Cada aplicación debe contar con un perfil administrativo particular, que permita la gestión y mantenimiento del modelo de perfiles y accesos, cumpliendo con los requerimientos establecidos para autenticación de usuarios.

Al incorporarse una aplicación en producción, el modelo de autorización no deberá tener ningún usuario asignado, salvo el usuario *Propietario de la información* y el usuario de quien éste determine como Administrador de Accesos. Las acciones sobre el modelo de autorización se realizarán a través del software de aplicación una vez que se encuentre en producción.

ANEXO I

Administración de accesos de usuarios a aplicaciones

La *ASI* establece los siguientes lineamientos que se deberán cumplir para el acceso de usuarios a las aplicaciones del *GCABA*:

- Los usuarios con acceso a aplicaciones deben ser nominales, estar identificados en el padrón GCABA y estar asociados a un *ID de Usuario GCABA* activo.

- Todos los usuarios que se encuentren identificados en el modelo de autorización de las aplicaciones, deberán tener como identificador obligatorio y no exclusivo, el CUIT/L de la persona a quien pertenece dicho el ID de Usuario, con el fin de contar con una trazabilidad de actividades de usuarios que sea transversal a todo el GCABA. El CUIT/L debe pertenecer a personas físicas, identificadas en el padrón GCABA, no permitiendo identificadores referenciales de personas jurídicas.

- No se permitirá el uso de identificadores no nominales (genéricos) para uso personal o acceso a aplicaciones. Los identificadores no nominales estarán reservados para tareas de administración del sistema, usuarios por defecto de software e identificadores con privilegios funcionales críticos. Las contraseñas de este tipo de usuarios, estarán bajo resguardo de la *ASI*.

a. Solicitud de Alta, Baja o Modificación

La solicitud de alta, baja o modificación de accesos deberá ser realizada por el Director General, Equivalente o Superior Jerárquico de la repartición a la que pertenece el usuario requirente, de acuerdo a los datos de pertenencia que el mismo posea en el padrón *GCABA*, a través de una nota dirigida al *Propietario de la Información* o a quien éste designe para tal fin.

La solicitud de alta o modificación de acceso deberá contener la siguiente información:

- Nombre, apellido y ID del Usuario.

- Repartición de pertenencia.

- Aplicación al que se solicita acceder o modificar el acceso.

- Perfil requerido de acceso o modificación.

- Justificación de la solicitud.

- Condiciones de uso del acceso.

Las condiciones de uso del acceso, deberán indicar si existen observaciones sobre el uso del acceso solicitado, tiempo pre definido de caducidad del acceso, anulación de acceso en caso de cambio de repartición de pertenencia del usuario, y otros.

ANEXO I

La solicitud de baja de acceso deberá contener la siguiente información:

- Nombre, apellido y ID del Usuario.
- Repartición de pertenencia.
- Aplicación al que se solicita remover el acceso.
- Perfil a dar de baja.
- Justificación de la solicitud.
- Condiciones de baja del acceso.

Las bajas de accesos se podrán realizar de manera manual o automatizada al momento de caducidad de vigencia de pedido de acceso, desactivación de usuarios o cualquier otra situación que amerite el cese de funciones. El solicitante debe indicar si la baja de acceso es temporal o permanente.

b. Autorización

Las solicitudes de altas, bajas y modificaciones de accesos a software de aplicación requieren la autorización del *Propietario de la Información* correspondiente, o quien éste designe formalmente esta atribución.

El *Propietario de la Información* o quien éste designe para tal fin, deberá verificar el ID de Usuario que requiere el acceso y la información contenida en la solicitud. El *Propietario de la Información*, solo podrá aprobar o desaprobar la información recibida, no pudiendo modificar las mismas, una vez emitidas.

En caso en que el pedido de acceso exceda los permisos pre establecidos para la aplicación, no corresponda con alguna de las condiciones de la solicitud (justificación de uso, repartición de pertenecía del usuario u otro), o no sea determinado como excepción autorizada por el *Propietario de la Información*, el mismo podrá ser rechazado y devuelto indicando el motivo de rechazo.

c. Implementación

De no existir motivo de rechazo, el *Administrador de Accesos*, incorporará dentro del modelo de autorización de la aplicación, la modificación según lo solicitado.

De tratarse de altas o modificaciones, deberá incorporar la asociación del ID de Usuario GCABA y el perfil de acceso requerido.

En caso de baja deberá remover del modelo de autorización el perfil solicitado. Si el usuario de la aplicación queda sin perfil asignado, será dado de baja del modelo de autorización.

En todos los casos, luego de implementar los accesos autorizados, dará aviso formal a los solicitantes.

Cada Administrador de Accesos debe mantener un registro de los usuarios, los permisos o perfiles otorgados, las solicitudes de acceso y autorizaciones correspondientes.

Bajas por desvinculación

Si la baja del usuario se debe a desvinculación del *GCABA*, los *Administradores de Accesos* verificarán todos los accesos que el usuario tiene asignado y realizarán la remoción de los mismos.

La baja del ID de *Usuario GCABA* será realizada por el área de servicio del Organismo al que pertenece el usuario, según los lineamientos establecidos por la *ASI* para tal fin.

Revisión periódica de usuarios activos

Los *Administradores de Accesos* realizarán una revisión periódica, al menos una vez por mes, de los accesos otorgados a los usuarios en las aplicaciones, a fin de identificar que los mismos sigan activos en el padrón de Usuarios *GCABA*. En caso de identificar usuarios en las aplicaciones cuyo ID de Usuario *GCABA* en el padrón fue deshabilitado o eliminado, se procederá a realizar la baja de los accesos en la aplicación.

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0809 - Política de Administración de Accesos a Recursos de Infraestructura de TI

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Administración de Accesos a Recursos de Infraestructura de TI

1. Introducción

Los *recursos de infraestructura de TI* conforman la base para brindar soporte al procesamiento y almacenamiento de la información del *GCABA*. La correcta administración de los accesos de *usuarios* a estos recursos es fundamental para garantizar la seguridad de la *información*. Es necesario poder identificar a cada una de las personas que utilizan los *recursos de infraestructura de TI*, además de determinar los permisos de acceso que tienen o podrán tener, teniendo en cuenta las funciones que ellas desempeñan en el *GCABA*.

En esta política se establecen los lineamientos principales a tener en cuenta al momento de otorgar, modificar o remover accesos de *usuario*s a dichos *recursos*.

2. Objetivo

Establecer los lineamientos que permitan asegurar una adecuada administración de los accesos de *usuario*s a los *recursos de infraestructura de TI* del *GCABA*.

3. Alcance

Todos de usuarios que requieran acceso a los *recursos de infraestructura de TI* del *GCABA*, incluyendo:

- Sistemas operativos.
- Software de base de datos.
- Dispositivos de redes y seguridad informática.

El acceso de usuarios administradores será realizado conforme a lo establecido por la ASI.

La presente política no alcanza a los usuarios en custodia, cuya administración y uso se establece en otro documento.

4. Contenido

Condiciones requeridas para el acceso a recursos de TI

Todo sistema operativo, software de base de datos, dispositivo de red y de seguridad informática (en adelante, recurso) que sea implementado en producción deberá contar con los permisos correspondientes, a fin de controlar el acceso a funcionalidades e información, a través de una adecuada segregación de los mismos, conforme a los niveles de criticidad que el recurso posea.

ANEXO I

Administración de accesos de usuarios a recursos de TI

La *ASI* establece los siguientes lineamientos que se deberán cumplir para el acceso de usuarios a los *recursos de infraestructura de TI* del *GCABA*:

- Los usuarios con acceso a los *recursos de infraestructura de TI* deben ser nominales, estar identificados en el padrón GCABA y estar asociados a un ID de Usuario GCABA activo.

- Todos los usuarios que se encuentren identificados en el modelo de autorización de los *recursos de infraestructura de TI*, deberán tener como identificador obligatorio y no exclusivo, el CUIT/L de la persona a quien pertenece dicho el ID de Usuario, con el fin de contar con una trazabilidad de actividades de usuarios que sea transversal a todo el GCABA. El CUIT/L debe pertenecer a personas físicas, identificadas en el padrón GCABA, no permitiendo identificadores referenciales de personas jurídicas.

- No se permitirá el uso de identificadores no nominales (genéricos) para uso personal o acceso a recursos de infraestructura de TI. Los identificadores no nominales estarán reservados para tareas de administración del sistema, usuarios por defecto de software e identificadores con privilegios funcionales críticos. Las contraseñas de este tipo de usuarios, estarán bajo resguardo de la ASI.

d. Solicitud de Alta, Baja o Modificación

La solicitud de alta, baja o modificación de accesos deberá ser realizada por el Director General, Equivalente o Superior Jerárquico de la repartición a la que pertenece el usuario requirente, de acuerdo a los datos de pertenencia que el mismo posea en el padrón GCABA, a través de una nota dirigida al *Propietario* de la Información o a quien éste designe para tal fin.

La solicitud de alta o modificación de acceso deberá contener la siguiente información:

- Nombre, apellido y ID del Usuario.

- Repartición de pertenencia.

- *Recurso de infraestructura de TI* al que se solicita acceder o modificar el acceso.

- Perfil requerido de acceso o modificación.

- Justificación de la solicitud.

- Condiciones de uso del acceso.

Las condiciones de uso del acceso, deberán indicar si existen observaciones sobre el uso del acceso solicitado, tiempo pre definido de caducidad del acceso, anulación de acceso en caso de cambio de repartición de pertenencia del usuario, y otros.

ANEXO I

La solicitud de baja de acceso deberá contener la siguiente información:

- Nombre, apellido y ID del Usuario.
- Repartición de pertenencia.
- *Recurso de infraestructura de TI* al que se solicita remover el acceso.
- Perfil a dar de baja.
- Justificación de la solicitud.
- Condiciones de baja del acceso.

Las bajas de accesos se podrán realizar de manera manual o automatizada al momento de caducidad de vigencia de pedido de acceso, desactivación de usuarios o cualquier otra situación que amerite el cese de funciones. El solicitante debe indicar si la baja de acceso es temporal o permanente.

e. Autorización

Las solicitudes de altas, bajas y modificaciones de accesos a *recursos de infraestructura de TI* requieren la autorización del *Propietario* de la Información, o quien éste designe formalmente esta atribución.

El *Propietario* de la Información o quien éste designe para tal fin, deberá verificar el ID de Usuario que requiere el acceso y la información contenida en la solicitud. Sólo podrá aprobar o desaprobar la información recibida, no pudiendo modificar las mismas una vez emitidas.

En caso en que el pedido de acceso no corresponda con alguna de las condiciones de la solicitud (justificación de uso, repartición de pertenecía del usuario u otro), o no sea determinado como excepción autorizada por el *Propietario* de la Información, el mismo podrá ser rechazado y devuelto indicando el motivo de rechazo.

f. Implementación

De no existir motivo de rechazo, el *Administrador de Accesos* de la *ASI,* incorporará dentro del modelo de autorización del recurso, la modificación según lo solicitado.

De tratarse de altas o modificaciones, deberá incorporar la asociación del *ID de Usuario GCABA* y el perfil de acceso requerido.

En caso de baja deberá remover del modelo de autorización el perfil solicitado. Si el usuario queda sin perfil asignado, será dado de baja del modelo de autorización.

En todos los casos, luego de implementar los accesos autorizados, dará aviso formal a los solicitantes.

Cada *Administrador de Accesos* de la *ASI* debe mantener un registro de los usuarios, los permisos o perfiles otorgados, las solicitudes de acceso y autorizaciones correspondientes.

Bajas por desvinculación

Si la baja del usuario se debe a desvinculación del *GCABA*, los *Administradores de Accesos* de la ASI verificarán todos los accesos que el usuario tiene asignado y realizarán la remoción de los mismos.

La baja del ID de *Usuario GCABA* será realizada por el *área de servicio* del *Organismo* al que pertenece el usuario, según los lineamientos establecidos por la *ASI*.

Revisión periódica de usuarios activos

Los *Administradores de Accesos* de la *ASI* realizarán una revisión periódica, al menos una vez por mes, de los accesos otorgados a los usuarios en los recursos de infraestructura de TI, a fin de identificar que los mismos sigan activos en el padrón de Usuarios *GCABA*. En caso de identificar usuarios cuyo ID de Usuario *GCABA* en el padrón fue deshabilitado o eliminado, se procederá a realizar la baja de los accesos a los recursos de infraestructura de TI.

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y nacional, y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0810 - Política de Accesos Remotos

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de accesos remotos

1. Introducción

El servicio de acceso remoto permite a los usuarios conectarse a la *red de comunicaciones* del *GCABA* desde un sitio externo.

Existen usuarios que se conectan a través de este servicio con la finalidad de tener acceso a la *información* y *software de aplicación* que se encuentra disponible en la *red de comunicaciones* del *GCABA*. Estos accesos se realizan a través de una red privada virtual (VPN), empleando redes de dominio público para conectar la *estación de trabajo* con la *red de comunicaciones del GCABA.* El riesgo que implica el empleo de redes públicas hace necesario establecer medidas de seguridad que garanticen la protección de la información transmitida por este medio.

2. Objetivo

Establecer los criterios y controles de seguridad que deberán cumplirse al conectar usuarios remotos a la *red de comunicaciones* del *GCABA*, a fin de garantizar una adecuada protección de la *información* y los *recursos informáticos* de la misma.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

El acceso remoto de usuarios a la red de comunicaciones del GCABA se lleva a cabo utilizando un método de autenticación físico (dispositivo de autenticación por hardware). La ASI establece los siguientes lineamientos para la prestación de este servicio:

Solicitud del *servicio*

El acceso remoto deberá ser solicitado únicamente en situaciones que justifiquen la imposibilidad de otra forma de acceso, tales como trabajo fuera de horario laboral o en ubicaciones fuera de los *Organismos*, entre otros.

La ASI, como órgano rector de tecnología y comunicación, es el único organismo con la capacidad de otorgar accesos remotos a la red de comunicaciones del GCABA.

La solicitud de acceso debe ser enviada a la ASI, por medio de una nota suscripta por el Director General, Equivalente o Superior Jerárquico de la repartición a la que pertenece el usuario, indicando los *recursos*

informáticos a los que se requiere acceder, los datos del usuario, la justificación o motivo del requerimiento y el período de tiempo que el usuario requerirá del acceso.

El acceso remoto a los *recursos informáticos* deberá estar autorizado por el *Propietario* correspondiente a dichos recursos.

El usuario para el cual se requiere el acceso debe tener un ID de Usuario *GCABA,* el cual es reconocido como usuario válido para acceder a los recursos informáticos. En caso de personal externo, deberá formar parte del padrón de usuarios externos (padrón GCABA) el cual contiene los datos de las personas que prestan servicios al GCABA y podrían requerir acceso a un recurso informático.

El funcionario solicitante debe pertenecer a la línea de dependencia (árbol jerárquico) del usuario que requiere el acceso. La ASI controlará la relación de dependencia existente entre el usuario y el funcionario solicitante y rechazará todas las solicitudes que no cumplan con esta condición, observando la misma.

Una vez cumplida la condición anterior, la *ASI* verificará si el *recurso informático* a acceder se encuentra bajo el ámbito de responsabilidad del funcionario solicitante, caso contrario la solicitud deberá contar con la autorización del *Propietario* correspondiente al recurso. De no ser así, la ASI tendrá la facultad de rechazar la solicitud.

La ASI hará entrega presencial del dispositivo de hardware al usuario final, en correspondencia con los accesos que hayan sido solicitados.

Carácterísticas de los *accesos remotos*

Las medidas de seguridad implementadas por la *ASI* para los accesos remotos a la *red de comunicaciones* del *GCABA* son las siguientes:

a. Las conexiones externas sólo podrán acceder a los *servicios*, sistemas y/ o aplicaciones a los que estén autorizados.

b. El *servicio* de acceso remoto sólo podrá ser utilizado para conexiones entrantes.

c. Los *usuarios* que utilicen el *servicio* de *acceso remoto*, deberán autenticarse mediante la utilización del ID de *Usuario GCABA* y su correspondiente contraseña.

d. La ASI podrá monitorear los eventos relacionados con: cambios de derechos de acceso remoto, accesos exitosos y fallidos, la identificación del usuario responsable, la fecha y hora de inicio de conexión, tiempo de conexión, las líneas y protocolos empleados.

e. La ASI realizará la gestión y administración de los accesos y dispositivos de autenticación llevando un registro de la asignación de los mismos. Asimismo pondrá a disposición la información de los usuarios, a los Organismos que se encuentren bajo su órbita y sean poseedores de dispositivos de autenticación.

f. La ASI verificará que las conexiones establecidas correspondan con los accesos otorgados.

La detección de cualquier irregularidad en los accesos remotos será motivo suficiente para que la ASI tome las medidas correspondientes al caso.

Baja del *servicio*

El funcionario solicitante deberá informar a la *ASI* cualquier situación que amerite la baja o modificación de los accesos remotos.

En el caso de que la baja de accesos requiera la devolución del dispositivo de autenticación, el funcionario solicitante será el responsable de operar los mecanismos de recupero del dispositivo, el cual debe ser devuelto a la *ASI* en iguales condiciones físicas a las que fueron entregadas.

Será responsabilidad del usuario la protección y custodia del dispositivo de autenticación. El usuario deberá informar a la ASI de forma inmediata, cualquier sospecha de compromiso de las claves del dispositivo.

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO0901 - Política de Separación de Ambientes

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Separación de Ambientes

1. Introducción

La *información*, *software de aplicación* y *software de base* utilizados y administrados por el *GCABA* requieren un adecuado esquema de seguridad y control a fin de minimizar el riesgo de actualizaciones erróneas en el entorno productivo (accidentales o intencionales), ingresar programas no probados y evitar accesos no autorizados a los datos. Por esta concepción, resulta necesario tomar medidas para establecer una adecuada separación de ambientes y una apropiada configuración de accesos sobre los mismos. Esta separación se debe realizar de manera tal que las funciones de los operadores de los distintos ambientes no se solapen, evitando el ingreso de desarrolladores a cualquier activo productivo y, a su vez, que los implementadores con acceso a producción no tengan acceso a herramientas de desarrollo.

2. Objetivo

Establecer los lineamientos y definir las pautas generales para garantizar una adecuada separación de ambientes de procesamiento de la información del GCABA, estableciendo las características de los ambientes de desarrollo, homologación y producción a fin de minimizar el riesgo de generar un impacto negativo o errores en producción, y asegurando una apropiada segregación de funciones y limitaciones de acceso.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

La separación de funciones y ambientes de procesamiento del *GCABA*, debe considerar lo que se enuncia a continuación.

Implementación de ambientes de procesamiento

La *ASI* define implementar como mínimo los siguientes ambientes de procesamiento para todo *software de aplicación* y *software de base*:

a. Desarrollo

   Ambiente de uso exclusivo de los *Agentes* de Desarrollo de Software del GCABA o proveedor de desarrollo (en adelante "*Agentes* de Desarrollo de Software"), donde residen todas las herramientas informáticas necesarias para llevar a cabo el proceso de construcción, desarrollo,

actualización y pruebas técnicas. Asimismo, todos los desarrollos y modificaciones sobre los distintos sistemas serán realizados en este *ambiente de desarrollo,* siguiendo las buenas prácticas establecidas por la ASI para desarrollo seguro. En el caso de ambientes de desarrollo que se encuentren en centros de procesamiento de proveedores, la *ASI* debe contar con los componentes necesarios para replicar el ambiente dentro de la infraestructura propia, que permita generar nuevas versiones del *software de aplicación*.

b. Pruebas

Ambiente donde se implementan las versiones generadas en el ambiente de desarrollo. Utilizado por Agentes de QA para realizar pruebas de integración, validar las funcionalidades requeridas por los usuarios y verificar los requerimientos no funcionales definidos (logging, disponibilidad, escalabilidad, estilo, performance, etc.). En este ambiente y durante este proceso, el software es evaluado y sometido a una serie de pruebas para verificar el cumplimiento de las pautas de calidad y seguridad (evaluación de vulnerabilidades a nivel aplicación).

c. Homologación

Es una réplica del ambiente de producción en términos de arquitectura, configuraciones, accesos, control de seguridad, software de aplicación y software de base. En este ambiente se debe contar con la misma versión de software que el que se encuentra implementado en Producción, o una versión superior.

Toda información del ambiente de producción que se requiera para las pruebas de homologación debe ser obligatoriamente despersonalizada.

Este ambiente es utilizado para comprobar la efectividad de los cambios en software de aplicación, software de base, configuraciones e infraestructura, en el mismo se deberán realizar las pruebas de aceptación del usuario y la evaluación de vulnerabilidades a tanto a nivel aplicación, como de plataforma.

d. Producción

Ambiente de uso exclusivo de los usuarios finales, en el mismo se ejecutan y residen los datos y todos los recursos informáticos que soportan las versiones homologadas del software de aplicación y software de base. Todos los cambios que se realicen en este ambiente deberán cumplir con los lineamientos establecidos por la ASI.

Este ambiente debe cumplir con todos los requisitos funcionales y no funcionales, pautas de calidad y seguridad del software, asegurando el buen funcionamiento de los servicios.

Los ambientes de homologación y producción deberán estar físicamente separados entre sí y a su vez separados de los ambientes de desarrollo y prueba, a través de medidas de seguridad de cada ambiente y en distintos segmentos de la red de comunicaciones del GCABA.

ANEXO I

Los ambientes de homologación y producción deben estar soportados dentro de la infraestructura de TI propia del GCABA.

La *ASI* se reserva el derecho de poder auditar cualquier ambiente dentro del ciclo de vida de desarrollo de la aplicación. Asimismo, de ser necesario, podrá implementar un ambiente de capacitación de acuerdo a requerimientos particulares que serán acordados con el *Propietario de la Información*:

a. Capacitación

   Ambiente de uso exclusivo para capacitación de usuarios, preparado a solicitud del Propietario de la Información y por tiempo determinado. Este ambiente deberá contar con la misma versión del software que va a implementarse o que se encuentra instalado en el ambiente de producción u homologación.

   En este ambiente los datos deberán ser obligatoriamente despersonalizados y exclusivos.

Datos de producción

Cuando sea necesaria la copia de archivos y/o datos con información operativa de producción hacia los otros ambientes, debe existir previa autorización expresa del *Propietario de la Información* y de la máxima autoridad de la ASI o a quienes éstos designen formalmente en su reemplazo. La autorización deberá realizarse por medio fehaciente y ser conservada en poder de la ASI.

Accesos a los ambientes de procesamiento

Los distintos ambientes deberán estar configurados de acuerdo con lo establecido por la ASI, para asegurar una adecuada separación de funciones y un control de los accesos. Solo los usuarios finales podrán tener acceso a los datos reales con el fin de poder cumplir con sus funciones laborales.

En tal sentido, se definen las medidas para asegurar que el acceso a los distintos ambientes cumpla con las siguientes condiciones:

a. Los Agentes de Desarrollo de Software sólo podrán acceder al ambiente de Desarrollo para realizar las modificaciones y pruebas técnicas de los cambios en software de aplicación y configuraciones. No tendrán acceso a los restantes ambientes, ni tampoco a los datos reales.

b. Los Agentes de QA sólo podrán acceder a los ambientes de prueba y homologación para realizar de las pruebas de funcionamiento del software de requerimientos funcionales o no funcionales. No tendrán acceso a los restantes ambientes, ni tampoco a los datos reales.

c. Los Agentes Implementadores sólo podrán tener acceso a los ambientes de Homologación y Producción, con los privilegios necesarios para realizar la transferencia de los cambios en

software de aplicación, software de base, configuraciones y arquitectura. No tendrán acceso a los restantes ambientes, ni tampoco a los datos reales.

d. Ningún usuario podrá tener acceso a la modificación de fuentes y/o programas que se encuentren implementados en el ambiente de producción.

Segregación de Funciones

La *ASI* tomará medidas para delimitar la distribución de las tareas entre las distintas funciones. El siguiente cuadro muestra las incompatibilidades entre las funciones, desde el punto de vista de control interno.

Referencias:

NO: Funciones incompatibles, deberán tomarse medidas para la segregación de tareas, a fin de evitar su concentración en un solo sector.

X: Preferentemente estas tareas no deberían recaer en un mismo sector, y en el caso de que las mismas estuviesen concentradas, deberán evidenciarse claras medidas de control compensatorio.

SI: Funciones compatibles, no es necesario tomar medidas de segregación.

Descripción de las funciones:

a. Análisis Funcional / programación: diseño y desarrollo de los sistemas aplicativos, de acuerdo con las necesidades del GCABA.

b. Control de calidad: prueba de calidad del software de aplicación para la puesta en producción.

c. Operaciones: gestión operativa del procesamiento de información y el equipamiento afectado.

d. Administración de resguardos: custodia, guarda y mantenimiento de los archivos de datos y programas almacenados en distintos medios.

e. Implementación: puesta en producción de software de aplicación, software de base, configuraciones e infraestructura de TI.

f. Administración de bases de datos: definición y mantenimiento de la estructura de los datos de las aplicaciones que utilizan este tipo de software.

g. Propietario de la Información: aprobación de los cambios en la información y software de aplicación.

h. Control y monitoreo de seguridad informática: seguimiento de las actividades relacionadas con el empleo de los activos de información.

Por cada servicio o aplicación deberá aplicarse la segregación de funciones descripta en el siguiente cuadro:

	Análisis Funcional / Programación	Control de Calidad	Operaciones	Administración de Resguardos	Implementación	Administración de Bases de Datos	Propietario de la Información	Control y Monitoreo de Seguridad Informática
Análisis Funcional / Programación		X	NO	NO	NO	NO	NO	NO
Control de Calidad	X		NO	NO	X	NO	SI	NO
Operaciones	NO	NO		SI	X	X	NO	NO
Administración de Resguardos	NO	NO	SI		X	NO	X	NO
Implementación	NO	X	X	X		NO	NO	NO
Administración de Bases de Datos	NO	NO	X	NO	NO		NO	NO
Propietario de la Información	NO	SI	NO	X	NO	NO		NO
Control y Monitoreo de Seguridad Informática	NO	NO	NO	NO	NO	NO	NO	

No será permitido ningún tipo de accesos de usuarios, que no cumplan con la segregación de funciones determinada en la presente política.

Generalidades

Toda excepción a los accesos o a la existencia e implementación de los ambientes establecidos en esta política, deberá ser explicitada y fundamentada por el *Propietario de la Información* siendo sometida a la evaluación de riesgo implícito y su viabilidad por parte de la *ASI*.

ANEXO I

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe y de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

Política de Control de Cambios

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Control de Cambios

1. Introducción

A los efectos de esta política, un cambio en los ambientes de homologación y producción es una actualización o agregado de *software*, *hardware*, datos o estructuras de datos. Debido a la existencia de diferentes ambientes de procesamiento y entornos de activos y, con el fin de minimizar el riesgo de actualizaciones accidentales o intencionales sobre los mismos, resulta necesario definir un adecuado esquema de control para la realización de estos cambios en los ambientes de Homologación y Producción de los centros de procesamiento del GCABA.

2. Objetivo

Establecer los controles que deberán realizarse en el proceso de cambios de *software de aplicación*, *software de base, información* e infraestructura tecnológica del ambiente de Producción y Homologación, de manera de asegurar la integridad de dichos ambientes y minimizar el riesgo de pérdida de *información*, accesos no autorizados e indisponibilidad del servicio.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

La *ASI* define las medidas necesarias para el control de cambios en los *ambientes de Homologación* y *Producción*, estableciendo las condiciones que deben cumplirse para efectuar cambios de *software, hardware* y/o *información* en dichos ambientes.

Consideraciones generales

De acuerdo a los lineamientos establecidos por la *ASI* para la separación de ambientes de procesamiento (ver *Política de Separación de Ambientes*), todos los desarrollos y modificaciones sobre los distintos sistemas deberán ser realizados en el a*mbiente de Desarrollo*, sean los mismos ejecutados por personal del *GCABA* o por terceros.

Las pruebas y validaciones de cumplimiento de los desarrollos realizados se deberán efectuar en el *ambiente de Prueba*, con el fin de verificar el cumplimiento de las pautas de calidad y seguridad antes de su pasaje al ambiente de Homologación. La implementación de los cambios en los a*mbientes de Homologación y Producción*, es realizada por Agentes del GCABA ajeno a las tareas de desarrollo, de modo de establecer un control por oposición.

ANEXO I

Categorización de Cambios

Para el tratamiento de los cambios en *software de aplicación* en los ambientes de Homologación y Producción se considera necesario la evaluación de la magnitud del cambio, teniendo en cuenta el impacto que el mismo genera en el ambiente de procesamiento.

La *ASI* determinará, en base a la documentación requerida para la ejecución o implementación del cambio, la categorización del mismo y procede a la revisión de cumplimiento de los requerimientos antes de la autorización e implementación en el ambiente de Homologación y/o Producción.

De la evaluación, dependiendo de sus resultados, se establecen las siguientes categorías de cambio:

e. **Cambio Menor**: corresponde a un cambio realizado sobre un software de aplicación pre existente en los ambientes de Homologación y Producción y que, a su vez, no tiene impacto de riesgo potencial en el ambiente en el cual se implementa.

   Un cambio se categorizará como menor cuando cumple con las siguientes condiciones:

   - No afecta a los datos.
   - No afecta el esquema de seguridad.
   - No requiere cambios en la infraestructura.
   - No afecta la arquitectura de la aplicación.
   - No tiene relación con alguna aplicación o software crítico del GCABA.
   - No afecta la funcionalidad de la aplicación.
   - No afecta a otras aplicaciones.
   - Los riesgos y su resolución son de impacto menor en caso de implementaciones no satisfactorias

   Como ejemplos de cambios menores se pueden señalar: cambio de logos, de labels (etiquetas), de información estática, entre otros.

f. **Cambio Regular**: por exclusión, serán todos los cambios que no sean catalogados como menores. Si el cambio a realizar no cumple con alguna de las condiciones indicadas en el punto anterior, será tratado como Cambio Regular.

Cambios en *software de aplicación*

a. Ambiente de Homologación

ANEXO I

Todo requerimiento de implementación de un nuevo *software de aplicación* o cambio a un *software de aplicación* preexistente en este ambiente*,* debe cumplir con una serie de requisitos y estándares establecidos, con el fin de contar con las condiciones necesarias para su integración y minimizar el riesgo de fallas en el ambiente.

La implementación del cambio en el ambiente de Homologación deberá ser autorizada por:

- El *Propietario*, quien notificará a la *ASI* su conformidad respecto de la documentación del cambio, aceptando el cumplimiento de los requisitos definidos en esta política.

- La *ASI*, quien realizará el análisis de la documentación recibida y la evaluación de impacto.

En caso que el requerimiento cumpla con los lineamientos mencionados, la *ASI* dará curso a la solicitud cumpliendo los procedimientos establecidos para este fin.

b. Ambiente de Producción

Para el ingreso productivo e implementación de un nuevo *software* de aplicación o cambio a un *software de aplicación* preexistente en este ambiente, se debe cumplir con las siguientes condiciones:

- Se debe certificar de manera formal que los cambios fueron probados y aprobados en el ambiente de homologación por:

    - el *Propietario:* quien dará conformidad que los cambios o novedades a implementar cumplen en un todo de acuerdo con los requerimientos funcionales esperados.

    - la *ASI*: quien será el Organismo responsable de dar conformidad de cumplimiento de los requerimientos no funcionales que fueron definidos y aprobados por el *Propietario* para el activo.

- Las solicitudes de implementaciones productivas deberán cumplir con los procedimientos establecidos por la ASI. De ser necesario, la ASI evaluará, de manera consensuada con el *Propietario*, la urgencia del cambio para planificar su implementación.

La *ASI* se reserva el derecho de rechazar cualquier solicitud de cambio que no cumpla con lo establecido en esta política.

ANEXO I

Cambios en *información* por fuera del *software de aplicación*

Toda aquella modificación de información operativa del ambiente de producción por fuera del software de aplicación definido para tal fin, se podrá realizar por excepción mediante la ejecución de scripts sobre las bases de datos, dejando reflejado el cambio en los logs de auditoría correspondiente como requisito obligatorio para la ejecución del mismo.

Para la ejecución de éste tipo de modificación, se debe seguir los lineamientos establecidos a continuación:

a. Ambiente de Homologación

   El *Propietario* deberá presentar a la *ASI* el requerimiento detallando el motivo, tipo de cambio y el alcance, juntamente con la siguiente información:

   - Script a implementar.
   - Documentación técnica del script.
   - El script debe incorporar tareas para registrar los cambios realizados sobre la información y extraer un reporte de los mismos.

   Anterior a la implementación del script en el ambiente Homologación, la *ASI* validará la solicitud y el procedimiento a ejecutar, dando la consiguiente conformidad en caso de cumplimento e inexistencia de riesgos potenciales.

b. Ambiente de Producción

   La ejecución del script debe cumplir los siguientes lineamientos:

   - Ser probado y aprobado por la ASI en el ambiente de homologación.
   - Asegurar que se cuenta con una copia de respaldo de la información afectada, ante posibles fallos y necesidad de restauración de los datos.
   - Garantizar el cumplimiento de las regulaciones de auditoría sobre los cambios de información productiva.
   - Estar autorizado expresamente por un funcionario de rango no inferior a Director General, Equivalente o Superior Jerárquico a través de una nota a la ASI.

ANEXO I

Cambios en infraestructura de Tecnología de la *Información* (TI)

El *software de base* y *hardware* de TI son alcanzados en los cambios de infraestructura de TI. Se deberá considerar que los cambios en la infraestructura de TI pueden tener impacto en el *software de aplicación*. Por tal motivo, los cambios deberán estar integrados y se deberán tener en cuenta las siguientes consideraciones:

a. Las modificaciones a la infraestructura de TI de los ambientes de Homologación y Producción deberán ser autorizadas por la ASI.

b. Todos los cambios de software de base que se realicen en el ambiente productivo, deben previamente ser homologados en el ambiente destinado a tal fin.

c. Un cambio de hardware que implique una modificación en la arquitectura del ambiente de producción, deberá implementarse en primera instancia en el ambiente de homologación, ya que éste debe constituir una arquitectura semejante al primero.

Condiciones aplicables a todos los cambios

a. Todos los cambios están sujetos a un control estricto y deben ser identificados y registrados formalmente. Dichos registros deberán contener toda la información relevante de los cambios realizados, que permita realizar una trazabilidad del cambio desde su solicitud hasta su implementación en los ambientes de Homologación y Producción.

b. Las solicitudes de cambio deberán quedar documentadas de acuerdo a lo establecido por la *ASI*.

c. Todo cambio de software o infraestructura que se requiera implementar de manera productiva, será sometido por la *ASI* a un análisis de vulnerabilidades, a fin de evaluar debilidades que puedan ocasionar pérdidas o daños en los activos. La ASI no aprobará ni ejecutará ninguna implementación en el ambiente de Producción para el cual no se ha realizado el análisis de vulnerabilidades, o bien, que habiéndose realizado se haya detectado algún riesgo de daño potencial a servicios, recursos o software de aplicación.

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe y de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO1001 - Política de Respuesta Ante Incidentes

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de Respuesta Ante Incidentes

1. Introducción

Se define *incidente* a cualquier evento que desvíe la operación normal de un *servicio* y cause una interrupción o reducción de la calidad del mismo. La gestión de *incidentes* es un *proceso* continuo utilizado para administrar y minimizar el impacto de los eventos que comprometan la confidencialidad, integridad, disponibilidad de los *servicios de Tecnología Informática* del *GCABA*.

2. Objetivo

Establecer lineamientos que permitan corregir con la máxima celeridad posible, las consecuencias y efectos negativos de los *incidentes* de los servicios de TI, a fin de minimizar su impacto.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

El objetivo de la gestión de *incidentes* es recuperar la operación de los *servicios* estándar tan rápido como sea posible. La *ASI* requiere que todos los *servicios* de Tecnología Informática (*TI*) cuenten con un soporte ante incidencias, y que se establezcan medidas y mecanismos que permitan prevenir y detectar a tiempo, la posibilidad de ocurrencia de todos los *incidentes* que sea posible prever. Algunos de ellos pueden ser: alertas o eventos que afecten a la infraestructura de TI y operaciones de los sistemas informáticos del *GCABA*; anomalías o eventos que afecten la confidencialidad, integridad o disponibilidad de la *información* del *GCABA*; fallas o errores en las aplicaciones del *GCABA* que afecten su normal funcionamiento.

El responsable de cada *servicio* de *TI* disponible en el *GCABA* deberá asegurar un soporte para los *incidentes* que puedan ocurrir y garantizar la resolución de los mismos en tiempo y forma, aún ante la necesidad de escalamiento en niveles de soporte, ya sea en el *GCABA* o por un tercero. Todos los incidentes se clasificarán de acuerdo a su prioridad y complejidad de resolución.

Requerimientos del soporte ante *incidentes*

Para cada *servicio* de *TI*, la ASI requiere que los *usuarios* cuenten con un único punto de contacto disponible para notificar los posibles *incidentes*. Asimismo, el responsable de cada *servicio* de *TI* deberá establecer un *procedimiento* formal de comunicación, junto con un *procedimiento* de respuesta que determine la acción a emprender al recibir un informe sobre un *incidente* y, luego de su tratamiento, verifique la efectiva resolución del mismo.

ANEXO I

Todos los *usuarios* deberán notificar los posibles *incidentes* y no intentarán, bajo ninguna circunstancia, explotar o probar un posible punto débil o vulnerabilidad en el esquema de seguridad establecido para los sistemas y componentes de la red de comunicaciones del *GCABA* y/o alguno de los *servicios* de *TI* brindados.

El soporte ante *incidentes* generalmente se divide en niveles para atender de una forma más eficaz y eficiente a los usuarios. El número de niveles en los que se organiza el soporte depende de las necesidades de cada servicio.

La estructura más generalizada de servicio de soporte multinivel se conforma por:

a. Soporte de Nivel 1

   Es el nivel de soporte inicial, responsable de las incidencias básicas del usuario. Generalmente actúa como punto de entrada de todas las incidencias. La tarea principal en este nivel es reunir toda la información del usuario y determinar la incidencia mediante un análisis de los síntomas expresados y la determinación del problema. En el soporte de Nivel 1 habitualmente se tratan problemas simples de resolución sencilla. El personal a este nivel podría tener conocimiento básico y general de los *servicios*.

b. Soporte de Nivel 2

   Es el nivel de soporte especializado, donde se resuelven incidencias en redes de comunicación, sistemas de información, sistemas operativos y bases de datos, entre otras. Las personas encargadas de realizar este soporte deberán contar con conocimientos avanzados de los *servicios* a los que brinda soporte, además de los conocimientos de Nivel 1.

c. Soporte de Nivel 3

   En este nivel se brinda soporte para la resolución de problemas a nivel experto y de análisis avanzado. Los individuos asignados a estas tareas deberán ser especialistas en sus campos y serán además responsables, no sólo de ayudar tanto al personal de Nivel 1 y 2, sino también de la investigación y desarrollo de soluciones a problemas nuevos o desconocidos.

Habitualmente los sistemas de soporte ante incidencias se gestionan con un máximo de tres niveles, siendo el tercer nivel el de mayor capacidad para resolver problemas. Sin embargo, pueden incorporarse más niveles de acuerdo con la necesidad de soporte del *servicio*, así como también se puede contar con soporte por parte del proveedor de un producto o servicio dentro de la jerarquía de niveles de soporte ante incidencias.

ANEXO I

Acuerdo de Nivel de Servicio

Toda contratación de servicio TI deberá contener en los Pliegos de Bases, Condiciones Particulares y Especificaciones Técnicas, un soporte ante incidencias (acuerdo de nivel de servicio) que garantice la resolución de los incidentes en tiempo y forma. El acuerdo de nivel de servicio tiene como objeto de fijar el nivel acordado para la calidad de dicho servicio, en aspectos tales como su definición, medición del rendimiento, gestión de los problemas, tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, deberes del cliente ó usuario, garantías, finalización del acuerdo, entre otros.

Adicionalmente, todo responsable de un servicio del *GCABA* deberá asegurar un nivel de servicio para cada uno de los servicios bajo su responsabilidad, de la misma manera en que se establece en los acuerdos de nivel de servicio con terceros.

Requerimientos de la gestión de los *incidentes*

Todos los *incidentes* deberán registrarse de manera independiente, excepto aquellos casos en que se presenten incidencias masivas en un *servicio*. En cada caso registrado se deberán detallar las actividades realizadas durante la investigación antes de cerrar el caso.

Se recomienda que el sector que brinde el soporte a un *servicio* determinado mantenga una base de conocimientos que documente todos los análisis realizados sobre los *incidentes* ocurridos y su manera de resolución. Esto puede contribuir a mitigar las debilidades que lo causaron y a utilizar resoluciones pasadas para resolver *incidentes* actuales y futuros. Se deberá considerar el resguardo de la evidencia original, sin procesar, que se hubiera reunido durante la investigación y respuesta de un *incidente*.

La ASI requiere que se implementen mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los *incidentes*. Esta *información* se utiliza para identificar *incidentes* recurrentes o de alto impacto, lo cual indicará la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la ASI. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO1201 - Política de licencias y legalidad del software

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Política de licencias y legalidad del software

1. Introducción

El software es un recurso indispensable para el procesamiento de la información del GCABA, permite acceder, recopilar, organizar, analizar y distribuir información en grandes volúmenes de manera eficiente. Los Organismos del GCABA dependen en gran medida del software para el tratamiento de la información y, para garantizar la calidad y confiabilidad en dicho tratamiento, es necesario implementar medidas de control sobre la legalidad del software que utiliza.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico. Dicha licencia es un contrato entre el proveedor y el GCABA que establece cuáles son los derechos y obligaciones de cada una de las partes.

2. Objetivo

Establecer los lineamientos necesarios para asegurar que todo software que sea utilizado por el personal del GCABA en el desarrollo de sus tareas (tanto adquirido como desarrollado internamente) tenga la licencia de uso legal correspondiente.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

Software adquirido a terceros

Para evitar el uso de software no autorizado sin su correspondiente licencia legal y que se encuentre instalado en cualquiera de los equipos informáticos, deben tenerse en cuenta las siguientes medidas de seguridad:

c. Todo software debe ser adquirido, con previa autorización de la *ASI*, a nombre del *GCABA*, y debe contar obligatoriamente con una licencia legal para su utilización, exceptuando a aquellos que sean de "uso libre". Adicionalmente debe seguir los procedimientos y controles correspondientes para cualquier compra de recursos en el *GCABA*.

d. En el momento de la contratación se deben considerar la cantidad de usuarios que utilizarán el software, y así poder contar con un número suficiente de copias licenciadas del mismo, de forma tal de evitar la existencia de copias no autorizadas.

e. Los Organismos del *GCABA* deberán solicitar la intervención de la ASI para la realización de contratos específicos de licencias de software.

f. En caso que se reciba software de terceros bajo la modalidad de comodato para su prueba y evaluación, se debe poseer una constancia de la licencia temporal otorgada por el canal autorizado para comercializar dicho software.

g. El proveedor de software repentinamente podría dejar de operar o de prestar sus servicios, con lo cual (si esto sucede) deben contemplarse en los acuerdos de adquisición del software, los medios necesarios para obtener los datos, código fuente, manuales y documentación asociada, a efectos de garantizar la continuidad de las actividades del GCABA.

h. El organismo que requiera la licencia de un nuevo software deberá informar a la ASI:

- La justificación del tipo de producto y fabricante requerido;
- El responsable de la recepción de las licencias frente al organismo;
- El presupuesto disponible;
- Los equipos en donde se van a instalar las licencias.

i. El proveedor de software deberá garantizar como mínimo las tareas de mantenimiento y soporte técnico anual y las correspondientes actualizaciones periódicas. Las actualizaciones periódicas deberán incluir parches, mejoras, etc.

j. Las licencias adquiridas a favor del *GCABA* serán resguardadas patrimonialmente e incluidas dentro del inventario gestionado por la ASI.

k. Cuando el software implique un desarrollo realizado por terceros, la ASI deberá autorizar el pliego de base de condiciones.

Software desarrollado internamente

a. Todo desarrollo que se realice internamente deberá cumplir con los lineamientos / estándares vigentes, determinados por la ASI.

b. Todo software desarrollado internamente por los usuarios finales y/o desarrolladores es propiedad del *GCABA*, por lo que la ASI evaluará la necesidad de registrarlo a nombre del mismo.

c. Los derechos de propiedad intelectual, así como todo otro derecho de cualquier naturaleza, sobre los trabajos realizados (con independencia de la modalidad contractual), documentación, desarrollo de código, resultados de análisis y cualquier otro producto pertenecerán exclusivamente al GCABA.

ANEXO I

Solicitudes de Adquisición/Desarrollo a la ASI

Toda solicitud que deba realizarse tanto a nivel adquisición de licencias como desarrollo de software, deberá canalizarse en cumplimiento de la Resolución Nro. 190/12.

Transferencia a Terceros

Toda transferencia a terceros del software desarrollado internamente debe estar autorizada por la ASI, debiendo contar con el correspondiente respaldo legal.

Uso de software autorizado

La ASI podrá eliminar cualquier software instalado que no posea la correspondiente licencia legal de uso.

Control de las licencias en los equipos

a. La ASI podrá mantener un registro actualizado y permanente de las versiones de software instaladas en todos los equipos de procesamiento centralizado del *GCABA*.

b. La ASI podrá revisar en forma periódica los equipos conectados a la red de comunicaciones del *GCABA*, a fin de verificar la inexistencia de copias de software no licenciado o, en caso de software adquirido legalmente, la inexistencia de copias no autorizadas de dicho software.

Generalidades

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe y de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

ANEXO I

Marco Normativo de IT

PO1301 – Glosario de Términos y Definiciones

Gobierno de la Ciudad Autónoma de Buenos Aires

ANEXO I

Glosario de Términos y Definiciones

- **A**

Término	Definición
ABM	Altas, bajas y modificaciones
Acceso Remoto	Acceso desde una computadora personal o dispositivo móvil a un recurso informático ubicado físicamente en otro lugar, a través de una red externa.
Activo	Cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos del GCABA. Todo aquello que tiene valor para el GCABA.
Activo de Información	Cualquier recurso informático que permita que la información sea procesada, almacenada, trasportada a través de la infraestructura tecnológica propia o de terceros.
Administrador de Accesos	Persona Física, activa en el padrón GCABA, designada por el Propietario de la Información con la capacidad de ejecutar el ABM de los accesos a usuarios en el modelo de autorización del software de aplicación para el cual es designado.
Administrador de Accesos de la ASI	Persona Física, activa en el padrón GCABA, designada por el Propietario de la Información de la ASI con la capacidad de ejecutar el ABM de los accesos a usuarios en el modelo de autorización del software de aplicación para el cual es designado.
Agente	Persona que presta funciones en el Poder Ejecutivo del GCABA, cualquiera sea su situación de revista, pasantes, asistentes técnicos y contratados bajo la modalidad de locación de servicios u obra.
Agentes de Tecnología Informática	Responsable de la administración de cada plataforma tecnológica, incluyendo la seguridad lógica de cada uno de los equipos y/o servicios donde se procese información.
Ambiente de Producción	Entorno de trabajo que presta servicios para la operación y funcionamiento del GCABA. En el mismo se encuentran alojados los sistemas informáticos e información operativa del GCABA.
Ambiente de Homologación	Entorno de trabajo que presta servicios para la prueba y control de vulnerabilidades de los sistemas informáticos e información relacionada del GCABA.
Ambiente de Desarrollo	Entorno de trabajo donde se realiza la construcción de los sistemas informáticos del GCABA.
Antivirus Corporativo	Software de aplicación utilizado para prevenir, detectar y eliminar cualquier tipo de infección, propagación y/o ejecución de virus informático, definido por la ASI para su instalación en todos los equipos de procesamiento centralizado y estaciones de trabajo conectados a la red de comunicaciones de GCABA.
Áreas Críticas	Comprende tanto los centros de procesamiento de datos como los centros de almacenamiento de copias de resguardo que contengan información del GCABA, sean propios o de terceros.
Áreas de Servicios	Sectores encargados de administrar y gestionar las cuentas de correo, los servicios de internet y mensajería de los agentes que se encuentran bajo la

	órbita de su responsabilidad. Estas áreas realizan la gestión de RRHH y están al corriente de los datos y de las acciones que se realizan con los usuarios (bajas, pases, licencias, entre otras).
ASI	Agencia de Sistemas de Información del GCABA creada por ley N° 2689.

- **B**

Término	**Definición**

- **C**

Término	**Definición**
CCEG	Cuentas de Correo Electrónico Gubernamental.
Centro de almacenamiento de datos	Recinto en el cual residen los medios de conservación de copias de resguardo del GCABA.
Cifrado	Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
Custodio	Responsables de la posesión de la información y administrar técnicamente los sistemas que utilizan esta información. Este rol comúnmente es asignado a los Administradores de Sistemas, Administradores de Bases de Datos, Personal de Microinformática, Personal de Centros de Procesamiento de Datos y Centros de Almacenamiento de Copias de Resguardo.

- **D**

Término	**Definición**
Datos personales	Información referida a personas físicas o de existencia ideal.
Dispositivo Móvil	Recurso Informático, con capacidades de procesamiento, conexión permanente o intermitente a una red, memoria limitada, diseñados específicamente para una función, pero que pueden llevar a cabo otras funciones más generales. En este sentido, podrán ser: PDA (Asistente Personal Digital) y/o Teléfonos Celulares (SmartPhones).

- **E**

Término	**Definición**

Equipo de procesamiento centralizado	Recurso informático dedicado al procesamiento centralizado de información del GCABA, ya sea como servidor de aplicación o base de datos.
Equipo Portátil	Computadora móvil.
Estación de trabajo	Computadora personal (desktops y portátiles) conectadas a la red de comunicaciones del GCABA, utilizadas por los usuarios.

- **F**

Término	**Definición**
Firewall	Recurso Informático diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
Funcionario	Persona que desempeña un empleo público, cumpliendo funciones dentro de la estructura del GCABA.

- **G**

Término	**Definición**
GCABA	Gobierno de la Ciudad Autónoma de Buenos Aires
Gerencia Operativa de Seguridad Informática	Dependencia del GCABA constituida por personal encargado de dar seguimiento a los asuntos de Seguridad Informática que conciernen a todos los Organismos.

- **H**

Término	**Definición**
Hardware	Término que hace referencia a cualquier componente físico tecnológico, que forma parte, trabaja o interactúa de algún modo con un sistema informático. No sólo incluye elementos internos como el disco duro, placa madre, dispositivos magnéticos, ópticos, etc. sino que también hace referencia al cableado, circuitos, gabinete, etc., e incluso hace referencia a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.

- **I**

Término	**Definición**

ANEXO I

Información	Conjunto organizado de datos procesados que son comprendidos por el sujeto o sistema que lo recibe.
Información digital	Información almacenada, procesada y/o transportada por un recurso informático.
Insumo informático	Bien consumible utilizado en la producción de otro bien, es decir, para la obtención de un bien más complejo o diferente tras un proceso productivo. Por sus propias características, los insumos suelen perder sus propiedades para transformarse y pasar a formar parte del producto final. (Ejemplos: cartuchos de tinta, toners, resmas de papel, etc.)
Inventario de activos	Registro total de los activos hecho con orden y precisión.
Incidente	Un incidente es cualquier evento que desvíe la operación normal de un servicio de TI y cause una interrupción o reducción de la calidad del mismo.

- **J**

Término	**Definición**

- **K**

Término	**Definición**

- **L**

Término	**Definición**

- **M**

Término	**Definición**
Medio de almacenamiento	Dispositivo o periférico donde se almacenan datos, tales como discos magnéticos, discos ópticos (CD, DVD), tarjetas de memoria, pendrives.

ANEXO I

- **N**

Término	Definición

- **Ñ**

Término	Definición

- **O**

Término	Definición
Organismo	Toda entidad que dependa directa o indirectamente del GCABA.

- **P**

Término	Definición
Personal externo	Todo aquel personal que no pertenece en forma directa al GCABA.
Política	Documento de alto nivel que expresa la filosofía, orientación y directriz del GCABA.
Procedimiento	Describe de manera estructurada la forma de realizar una actividad. Un procedimiento define el modo en que se debe ejecutar la actividad para lograr un objetivo determinado.
Proveedores de TI	Persona física o jurídica contratada para la prestación de servicios y/o compra de insumos informáticos.

- **Q**

Término	Definición

ANEXO I

- **R**

Término	Definición
Recursos informáticos	Todos aquellos elementos de hardware y software que componen un sistema informático.
Recursos de infraestructura de TI	Recursos informáticos administrados por la ASI y Agentes de Tecnología Informática. Incluye elementos de hardware (equipamiento de red, seguridad informática, comunicaciones, servidores, entre otros) y software (sistemas operativos y bases de datos).
Red de comunicaciones	Red del GCABA mediante la cual se establece la interconexión entre los distintos Organismos.
Propietario de la Información	Funcionario al que se le ha asignado la responsabilidad de la gestión y utilización de una *información* en particular. Autoridad de cada Organismo perteneciente al GCABA.
Referente de la información	Persona designada por el Propietario de la Información para colaborar con las tareas de administración y control de la información.

- **S**

Término	Definición
Servicio Informático	Asistencia brindada a través de un sistema informático, software o hardware el cual es utilizada por un usuario para la realización de sus actividades.
Servicio de TI	Es un conjunto de actividades que buscan responder las necesidades de un usuario por medio de un cambio de condición en los bienes informáticos, potenciando el valor de estos y reduciendo el riesgo inherente del sistema.
Sistema informático	Es el conjunto de partes interrelacionadas, hardware, software y recurso humano que permite almacenar y procesar información.
Software	Comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas en un sistema informático.
Software Corporativo	Software adquirido y autorizado por la ASI para ser empleado por las estaciones de trabajo (p.ej. SAP, MS Office 2010, etc.).
Software de aplicación	Es, genéricamente, todo producto de software específico o adaptado para la función que un equipo o grupo de equipos realizan en una organización determinada (p.ej. SADE, SIGAF, etc.). Puede ser: - Contratado bajo licencia de uso: cuando existe un convenio entre GCABA y un proveedor mediante el cual este otorga derecho de uso a GCABA de un producto determinado, el cual sigue siendo de su propiedad. En general, toda modificación a esta clase de software debe ser formalmente solicitada al proveedor. - Propio: es aquel desarrollado y/o mantenido bajo responsabilidad de GCABA, quien tiene acceso y propiedad sobre los programas

	fuente que forman parte de ese software. - De uso personal: es aquel desarrollado para uso exclusivo en un puesto de trabajo, utilizando software estándar instalado. Se consideran dentro de esta clasificación las planillas de cálculo y macros asociadas, consultas automatizadas, reportes específicos, etc.
Software de base	Software que tiene como principal finalidad la de proveer, integrado con el hardware, un sistema informático general y efectivo. Generalmente se encarga de proveer los servicios de más bajo nivel desde el punto de vista informático (p.ej. sistemas operativos, compiladores, herramientas de desarrollo de software, etc.)
Software malicioso	Software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento del usuario. Se consideran software malicioso, entre otros, los virus, gusanos, troyanos, spyware, adware y rootkit.
Software utilitario (o de escritorio)	Es aquel que es adquirido como producto terminado, en general bajo régimen de licencia de uso, y que sirve genéricamente para resolver funcionalidades a nivel del usuario final para automatización de oficinas, productividad, etc. (p.ej. Paquete Office, Navegadores de internet, etc.)
SPAM	Correo electrónico no solicitado, habitualmente de tipo publicitario, y generalmente enviados masivamente.

- **T**

Término	**Definición**
TI	Tecnología Informática

- **U**

Término	**Definición**
Unidad de suministro continuo de energía (UPS)	Fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica
Usuario GCABA	Persona física que interactúa con los sistemas informáticos del GCABA por sí misma y que se encuentra registrado de manera unívoca, en el padrón de usuarios de la Ciudad, a través de su área de servicios de pertenencia.

- **V**

Término	**Definición**

Virus informático	Software malicioso cuya finalidad es alterar el correcto funcionamiento de los recursos informáticos, sin el permiso o el conocimiento del usuario.

- **W**

Término	**Definición**
Wi-Fi	Mecanismo de conexión a una red de dispositivos electrónicos de forma inalámbrica.

- **X**

Término	**Definición**

- **Y**

Término	**Definición**

- **Z**

Término	**Definición**

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
2013. Año del 30 aniversario de la vuelta a la democracia

Hoja Adicional de Firmas
Anexo

Número: IF-2013-06227164- -ASINF

Buenos Aires, Lunes 4 de Noviembre de 2013

Referencia: ANEXO - Marco Normativo de TI

El documento fue importado por el sistema GEDO con un total de 174 pagina/s.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales, c=AR, o=GCBA, ou=Aplicaciones, serialNumber=846
Date: 2013.11.04 15:01:32 -03'00'

GUSTAVO EDUARDO GAZZANEO
DIRECTOR EJECUTIVO
AGENCIA DE SISTEMAS DE INFORMACIÓN (MMGC)

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales, c=AR, o=GCBA, ou=Aplicaciones, serialNumber=846