CÓRDOBA,

VISTO: *El artículo 41 del Decreto N 1791/2015 y su modificatorio Decreto N° 039/2016, ratificados por Ley Provincial N° 10.337.*

Y CONSIDERANDO:

Que mediante la normativa citada se confiere a esta Secretaría General de la Gobernación, facultades relacionadas con la administración interna del Poder Ejecutivo y su organización con la finalidad de mejorar la calidad de la gestión pública provincial, así como la administración de los recursos informáticos de la Red de Gobierno.

Que en el marco de las políticas referidas al fortalecimiento de la gestión pública que se vienen llevando a cabo en el ámbito de la Administración Pública Provincial, resulta necesario la implementación de un sistema de gestión de calidad, como herramienta fundamental para mejorar la prestación de servicios.

Que en dicho contexto y en miras al objetivo final de certificar Normas ISO/IEC 20000 para la consecución del desarrollo, implementación y mantenimiento de un nuevo Sistema de Gestión de Servicios basados en tecnología de la información, surge la necesidad en esta instancia de diseñar y aprobar los objetivos, términos y definiciones de la Política General de Seguridad, así como determinadas Políticas Particulares de Seguridad.

Que como consecuencia de lo mencionado anteriormente, es menester crear un Comité de Seguridad Informática, el que estará integrado por representantes de distintas áreas de la Dirección General de Coordinación de Infraestructura Tecnológica y que tendrá como principal misión la de revisar en forma continua las políticas de seguridad informática con la finalidad de proponer a la autoridad competente la implementación de nuevas políticas que fueran convenientes en la materia.

Que asimismo serán sus funciones monitorear cambios significativos en los riesgos que afecten a los recursos tecnológicos del gobierno de Córdoba frente a posibles amenazas, sean internas o externas; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad informática; acordar y aprobar metodologías y procesos específicos relativos a la seguridad informática; así como evaluar y coordinar la implementación de controles específicos de seguridad informática para los sistemas o servicios de la Dirección General de Coordinación de Infraestructura Tecnológica, sean preexistente o nuevos.

Por ello, las previsiones de los Decretos Nros. 1791/2015 y 0039/2016, ratificados por Ley N° 10.337, y en uso de sus atribuciones;

LA SECRETARIA GENERAL DE LA GOBERNACIÓN RESUELVE

Artículo 1°

***APRUÉBANSE** a partir de la fecha de la presente Resolución los objetivos, términos y definiciones de la "Política General de Seguridad Informática" contenida en el Anexo I, que de una (1) fojas útiles forma parte integrante de la presente Resolución, a los fines de su implementación en el ámbito de la Administración Pública Provincial.*

Artículo 2°

***APRUÉBASE** a partir de la fecha de la presente Resolución las "Políticas Particulares de Seguridad Informática" contenida en el Anexo II, que de once (11) fojas útiles forma parte integrante de la presente Resolución, a los fines de su implementación en el ámbito de la Administración Pública Provincial.*

Artículo 3º

DISPÓNESE *la creación de un "Comité de Seguridad Informática" el que estará integrado por representantes de distintas áreas de la Dirección General de Coordinación de Infraestructura Tecnológica, destinado a garantizar el cumplimiento de las Políticas de Seguridad aprobadas a través de la presente Resolución.*

Artículo 4º

FACÚLTESE *al señor Director General de Coordinación de Infraestructura Tecnológica a dictar las normas reglamentarias y complementarias necesarias a los fines de tornar operativas las políticas se seguridad informática, así como a designar los miembros del Comité de Seguridad de la Información.*

Artículo 5º

PROTOCOLÍCESE*, comuníquese a la Dirección General de Coordinación de Infraestructura Tecnológica de la Secretaría General de la Gobernación, Publíquese y archívese.*

RESOLUCIÓN

Nº 001930

Cra. SILVINA RIVERO
SECRETARIA GENERAL
DE LA GOBERNACIÓN

ANEXO I

POLÍTICA GENERAL DE SEGURIDAD INFORMATICA

Objetivos Principales:

a) Proteger los recursos de información digital del Gobierno de la Provincia de Córdoba y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad.

b) Asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos informáticos y las medidas de protección para la reducción de riesgos que puedan afectar su normal funcionamiento.

c) Mantener la Política General de Seguridad Informatica del Gobierno de Córdoba actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Otros Objetivos:

d) Administrar la seguridad informática dentro del gobierno y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

e) Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

f) Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a los sistemas de información de la red digital del gobierno de la provincia.

g) Asignar Responsabilidades en Materia de Seguridad informática y Designar la conformación del Comité de Seguridad Informática

h) Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

i) Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

j) Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

k) Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas informáticos.

l) Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

m) Controlar la seguridad en la red del Gobierno de Córdoba cuando se conecta y utiliza computación móvil e instalaciones de trabajo remoto.

n) Minimizar los efectos de las posibles interrupciones de las actividades normales de los servicios informáticos alojados en los centros de cómputos del Gobierno de Córdoba (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento,

Ing. Juan D'An
Director General de Coord
Infraestructura Tecnol
Secretaria General de la Gob
Gobierno de la Provincia de C

acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
o) Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
p) Maximizar la efectividad de las operaciones de contingencia del Gobierno de Córdoba.
q) Asegurar la coordinación con el personal del Organismo y los contactos externos que participará en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.
r) Asesorar y colaborar en materia de seguridad informática con el Responsable de Sistemas del Gobierno de Córdoba y los propietarios de la Información de cada Unidad Organizativa respecto a la seguridad en el desarrollo y mantenimiento de sistemas informáticos.
s) Analizar, documentar y comunicar los resultados de los análisis de vulnerabilidades realizados a los Sistemas de información, con el objetivo de alertar al Responsable de Sistemas y/o los propietarios de la información sobre riesgos detectados que podrían afectar el funcionamiento del sistema informático o poner en riesgo el normal funcionamiento de otros sistemas informáticos que funcionen dentro de la red del Gobierno de la Provincia.
t) Implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
u) Instar la investigación por el incumplimiento de las disposiciones establecidas por las Políticas de Seguridad Informática a los fines de la aplicación de las sanciones correspondientes, de conformidad a la magnitud y característica del aspecto incumplido.

ANEXO II

POLÍTICAS PARTICULARES DE SEGURIDAD INFORMATICA

Política Particular de Seguridad de Acceso.

1.1. Control de Acceso

1.1.1. Objetivo

El principal objetivo de esta política es:
Controlar el acceso a los sistemas informáticos, medios de procesamiento de la información y a activos informáticos del Gobierno de Córdoba sobre la base de los requerimientos de operación de seguridad informática de la Dirección General de Coordinación de Infraestructuras Tecnológicas.

1.1.2. Alcance

Control de acceso sobre los sistemas informáticos e instalaciones de procesamiento asociadas con la infraestructura tecnológica del Gobierno de la Provincia de Córdoba.

1.1.3. Responsabilidad

El Propietario de la información será el responsable de determinar las reglas de control de acceso, los derechos y restricciones asociados a sus activos.
El Responsable de Seguridad Informática supervisa la aplicación consistente de la Política de Control de Acceso por todos los Propietarios de Activos y los administradores técnicos de controles de acceso.

1.1.4. Política

1.1.4.1. Objetivo de Control - Requerimientos del Organismo de control de acceso

Ing. Juan D'Ar...
Director General de Coord...
Infraestructura Tecnol...
Secretaría General de la Gob...
Gobierno de la Provincia de...

- *Limitar el acceso a los sistemas informáticos y a las instalaciones de procesamiento de información.*

1.1.4.2. Controles

Política de Control de Acceso

Deberá establecerse, documentarse y revisarse una Política de Control de Acceso, basada en los requerimientos de operación de la Dirección General de Coordinación de Infraestructura Tecnológica en materia de seguridad de informática. El Gobierno de la Provincia de Córdoba controla el acceso a los sistemas informáticos y a las instalaciones de procesamiento de información asociados con la Infraestructura tecnológica, en base a los requisitos de seguridad externos e internos aplicables.

Los derechos de acceso toman en consideración:

- *Los niveles de clasificación de criticidad del activo informático, servicio informático o información procesada dentro de la aplicación y aseguran que existe consistencia entre los niveles de clasificación y los derechos de acceso.*
- *Los requisitos provenientes de la legislación vigente y el marco regulatorio para el gobierno de Córdoba.*
- *Los principios de asignación basados en la necesidad de conocer y la necesidad de uso, asignando sólo los permisos mínimos de acceso a la información y a las instalaciones de procesamiento de información necesarias para el rol*
- *La regla estándar en todos los sistemas y redes que todo se encuentra prohibido excepto lo expresamente permitido.*

El proceso de control de accesos lógicos, seguirá una secuencia de tres fases:

- *Solicitud de acceso*
- *Autorización de acceso por parte del Propietario de la información*
- *Administración de acceso*

Acceso a redes y servicios de red

Se proveerá a los usuarios acceso solamente a la red y los servicios a los cuales hayan sido específicamente autorizados a usar.
Se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.
El Responsable de Operaciones tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal emitido por un responsable de área que lo solicite para personal de su incumbencia.
Se definirán:

- *las redes y servicios de red a los cuales se permite el acceso*
- *los procedimientos de autorización para determinar a quién se le permite acceder a qué redes y servicios de red*
- *controles de gestión y procedimiento para proteger el acceso a las conexiones de red y servicios de red*
- *los medios utilizados para acceder a las redes y servicios de red*
- *los requerimientos de autenticación de usuarios para acceder a los diferentes servicios de red*
- *el monitoreo del uso de los servicios de red.*

Estas definiciones serán consistentes con la Política de Control de Acceso.

1.1.4.3. Objetivo de Control - Gestión de acceso de usuario

- *Asegurar el acceso de usuario autorizado y prevenir el acceso no autorizado a los sistemas y servicios.*

1.1.4.4. Controles

Registro de usuario y cancelación de registro

Se implementará un proceso formal de registro de usuarios y de cancelación de registro para permitir la asignación de derechos de acceso.
El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información, el cual debe comprender:

Ing. Juan D'A...
Director General de Coord...
Infraestructura Tecnol...
...taria General de la G...
...de la Provincia de...

- *Utilizar identificadores de usuario únicos, de manera que se pueda relacionar a los usuarios con sus acciones.*

- *Evitar la existencia de múltiples perfiles de acceso para un mismo empleado.*

- *El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas, y deberá ser aprobado y documentado.*

- *Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.*

- *Deshabilitar o eliminar los identificadores de usuarios de quienes no pertenecen más a la organización o no requieren del acceso por un cambio de función.*

- *Periódicamente identificar y eliminar o deshabilitar los identificadores de usuarios redundantes.*

- *Asegurar que los identificadores redundantes no sean asignados a otros usuarios.*

Asignación de acceso a usuario

Se implementará un proceso formal de asignación de acceso a usuario para asignar o revocar derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.

El Responsable de Seguridad Informática definirá un procedimiento formal de asignación de acceso a usuarios, el cual debe comprender:

- *La solicitud de autorización, la cual tendrá dos instancias de aprobación, primero por la jurisdicción de la cual depende el usuario y segundo por el dueño del sistema de información o servicio.*

- *Se verificará que el nivel de acceso otorgado es consistente con la presente Política y con otros requisitos de control interno del gobierno de la provincia como la segregación de funciones.*

- *No se activarán los accesos por parte de los Administradores de Acceso antes que los procedimientos de autorización se hayan completado.*

- *Se adaptarán los derechos de acceso de los usuarios que hayan cambiado sus roles o funciones, y se eliminarán o bloquearán los derechos de acceso de los usuarios que se desvinculen de la organización.*

- *Se revisarán en forma periódica los derechos de acceso con los dueños de los sistemas de información o servicios.*

Gestión de derechos de acceso privilegiado

La asignación y uso de derechos de acceso privilegiados será restringida y controlada.

El Responsable de Seguridad de la información implementará un proceso formal para la asignación y la cancelación de los derechos de acceso privilegiado, que contemple las siguientes reglas:

- *Se identificarán los derechos de acceso privilegiado asociado a cada plataforma (Sistema Operativo, Sistema de Gestión de Base de Datos y Aplicaciones, Servicios o Sistema) y los usuarios a los cuales es necesario asignar los privilegios.*

- *Los derechos de acceso privilegiado se asignarán a los usuarios basado en los principios de esta Política y por evento.*

- *Se mantendrá un registro de todos los privilegios asignados.*

- *La autorización para la asignación de privilegios deberá contar con la aprobación del Responsable de Seguridad Informática y no se proveerán los*

Ing. Juan D'Am...
Director General de Coord...
Infraestructura Tecnol...
Secretaría General de la Gob...
Gobierno de la Provincia de ...

accesos privilegiados hasta tanto se haya completado el proceso de autorización.

- *Se establecerá el criterio de caducidad del privilegio al momento de su autorización.*

- *Se asignarán los derechos de acceso privilegiado a identificadores de usuario diferentes de aquellos usados para las actividades regulares de operación, las cuales no deberán ser realizadas con los identificadores privilegiados.*

- *Se revisarán en forma periódica las asignaciones de privilegios con el objeto de asegurar que siguen vigentes las necesidades de su asignación.*

- *No se permitirá el uso de usuarios genéricos privilegiados, salvo los proporcionados por las plataformas.*

- *El proceso de asignación de usuarios privilegiados genéricos por plataforma asegurará la segregación para su uso, la preservación de la confidencialidad de la información de autenticación y el cambio periódico de dicha información e inmediato después de su uso.*

- *Se mantendrán registros de auditoría para toda cuenta privilegiada.*

Gestión de información de autenticación secreta de usuarios

La asignación de información secreta de autenticación deberá controlarse a través de un proceso formal de administración.

El Responsable de Seguridad informática implementará un proceso formal para la asignación de información de autenticación secreta que incluya los siguientes requerimientos:

- *Los usuarios firmarán su compromiso de mantener confidencial su información de autenticación secreta, y en el caso de utilizar usuarios grupales, mantenerla sola dentro de los miembros del grupo.*

- *Se proporcionará de manera segura a los usuarios la información de autenticación secreta inicial, la cual es temporal y se cambiará en forma obligatoria con el primer uso.*

- *La información de autenticación secreta temporal será única para cada individuo y no seguirá un padrón deducible para su generación.*

- *Se verificará la identidad del usuario previo a la provisión de nueva o reemplazo de la información de autenticación secreta.*

- *Todo usuario deberá dar acuse de recibo de la información de autenticación secreta.*

- *La información de autenticación secreta por defecto de los productos provistos por los proveedores se cambiará en forma inmediata a la instalación del software o sistema.*

- *El almacenamiento de información de autenticación secreta se realizará en sistemas protegidos.*

- *La configuración de los sistemas de administración de información de autenticación secreta, seguirá los siguientes lineamientos:*

    - *las contraseñas sean del tipo "password fuerte" y tengan una cantidad no menor a 8 caracteres. La misma deberá estar conformada por números y letras.*
    - *suspendan o bloqueen permanentemente al usuario luego de 5 intentos fallidos cantidad no mayor a 5)*
    - *solicitar el cambio de la contraseña cada 180 días*
    - *impedir que las últimas 3 contraseñas sean reutilizadas*
    - *pasados 3 días de la asignación de la contraseña temporal, se bloqueará el usuario si la misma no es cambiada*

Ing. Juan D'Am...
Director General de Coordinación...
Infraestructura Tecnológ...
Secretaría General de la Gobe...
Gobierno de la Provincia de C...

001930

- *para usuarios privilegiados la contraseña deberá ser del tipo "password fuerte" y contar con una cantidad no menor a 8 caracteres. Esta deberá contener al menos una mayúscula y un carácter especial.*

Revisión de derechos de acceso de usuario

Los Propietarios de activos deberán revisar los derechos de acceso de usuario a intervalos regulares.

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate conjuntamente con el responsable informático de las unidades organizativas del gobierno de la provincia, con el soporte del Responsable de Seguridad informática llevará a cabo un proceso formal, a intervalos regulares de un año, a fin de revisar los derechos de acceso de los usuarios.
Se deben contemplar la revisión de las autorizaciones de privilegios especiales de derechos de acceso a intervalos regulares de 6 meses a fin de garantizar que no se obtengan privilegios no autorizados.

Eliminación o ajuste de derechos de acceso

Los derechos de acceso de todos los usuarios de empleados y de terceras partes a la información y a las instalaciones de procesamiento de información deberán eliminarse al momento de la terminación de su empleo, contrato o acuerdo, o ajustarse según cambie.
Los derechos de acceso físico y lógicos de todo colaborador o tercera parte serán eliminado con la terminación de su empleo o contrato según corresponda, y se modificará con los cambios.
Ante cambios de asignación de puesto o funciones, se eliminarán los derechos de acceso correspondiente a la función anterior y que no hayan sido aprobados para la nueva asignación.
Se cambiará la información de autenticación conocida por un colaborador o tercera parte desvinculado y que pertenezca a un identificador de usuario que se mantenga activo o acceso activo.
Para los casos en los que se observe un riesgo alto dado la sensibilidad en los accesos, responsabilidades del usuario en cuestión y causa de la separación de la función se realizará el ajuste de accesos físicos y lógicos en forma inmediata anterior al término o cambio de función.

1.1.4.5. Objetivo de Control - Responsabilidades de usuario

- *Hacer responsables a los usuarios por el cuidado de su información de autenticación.*

1.1.4.6. Controles

Uso de la información de autenticación secreta

Se requerirá a los usuarios seguir las prácticas de la organización para el uso de la información de autenticación secreta.
Los usuarios deben cumplir las siguientes directivas:

- *Mantener la información de autenticación en secreto, asegurando que no sea divulgada a ninguna otra parte, incluyendo personal jerárquico.*

- *Evitar mantener un registro de la información de autenticación a menos que pueda ser almacenada en forma segura y el método de almacenamiento haya sido aprobado.*

- *Cambiar la información de autenticación secreta siempre que exista un posible indicio de compromiso.*

- *Informar a la Dirección Gral. de Coordinación de Infraestructura tecnológica o al referente informático y/o propietario de la información de su repartición, en caso de detectar o sospechar que su información de autenticación ha sido puesta en riesgo o vulnerada, para que se tomen las medidas necesarias para su mitigación.*

- *Seleccionar contraseñas de calidad, y que:*
  - *Sean fáciles de recordar.*

Ing. Juan D'Amico
Director General de Coordinación
Infraestructura Tecnológica
Secretaría General de la Gobernación
Gobierno de la Provincia de Córdoba

- *No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.*

- *No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.*

- *Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.*

- *Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").*

- *Evitar incluir contraseñas en los procesos automatizados de inicio de sesión o en el almacenamiento automático de los exploradores web.*

- *Notificar de acuerdo al Proceso de Gestión de Incidentes, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.*

1.1.4.7. Objetivo de Control - Control de acceso a aplicaciones y sistemas

- *Prevenir el acceso no autorizados a sistemas y aplicaciones.*

1.1.4.8. Controles

Restricción de acceso a la información

El acceso a la información y a las funciones de sistemas de aplicación se restringirá de acuerdo con la política de control de acceso.
Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la unidad organizativa para el acceso a la información. Desde la DGCIT se realizaran las actividades para brindar apoyo a los requerimientos

de limitación de accesos, siendo responsabilidad del referente informático o el propietario de los datos cumplir con los siguientes controles:

- *Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones.*
- *Controlar qué datos pueden ser accedidos por un usuario en particular.*
- *Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.*
- *Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.*
- *Controlar los derechos de acceso de otras aplicaciones.*
- *Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.*
- *Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.*
- *Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.*
- *Proporcionar controles de acceso lógicos y físicos para el aislamiento de las aplicaciones sensibles, los datos o sistemas.*

Ing. Juan D'Amico
Director General de Coordinación
Infraestructura Tecnológica
Secretaría General de la Gobernación
Gobierno de la Provincia de Córdoba

Procedimientos de conexión (log-on) seguros

El acceso a los sistemas y a las aplicaciones deberá controlarse por un procedimiento de conexión (log-on) seguro.

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.
Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.
El procedimiento de identificación debe:

- *Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se haya llevado a cabo exitosamente el proceso de conexión.*

- *Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.*

- *Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.*

- *Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.*

- *Proteger contra intentos de conexión por fuerza bruta.*

- *Limitar el número de intentos de conexión no exitosos permitidos y:*
  - *Registrar los intentos exitosos y no exitosos.*
  - *Impedir otros intentos de identificación, una vez superado el límite permitido.*
  - *Generar un evento de seguridad si se detecta un intento potencial o una ruptura exitosa de los controles de conexión*

- *Desplegar la siguiente información, al completarse una conexión exitosa:*
  - *Fecha y hora de la conexión exitosa anterior.*
  - *Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.*

- *No mostrar las contraseñas en el proceso de conexión*

- *No transmitir las contraseñas en texto claro sobre la red.*

- *Terminar las sesiones inactivas luego de un tiempo definido de inactividad*

- *Restringir los horarios de conexión*

- *Limitar el tiempo máximo permitido para el procedimiento de conexión. Si éste es excedido, el sistema debe finalizar la conexión.*

Sera responsabilidad del propietario de la información y el responsable de sistemas del gobierno de Córdoba la realización y control de los procedimientos de conexión seguros. Desde la DGCIT se realizara el apoyo para la detección de aplicaciones que no cumplan estos procedimientos, informando al Responsable de Sistemas del Gobierno con un informe detallado de las desviaciones, riesgos y vulnerabilidades encontradas.

Sistemas de gestión de contraseñas

Los sistemas de gestión de contraseñas deberán ser interactivos y asegurar contraseñas de calidad.

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

- *Imponer el uso de identificadores de usuario y contraseñas individuales para determinar responsabilidades.*

Ing. Juan D'Amico
Director General de Coordinación
Infraestructura Tecnológica
Secretaría General de la Gobernación
Gobierno de la Provincia de Córdoba

- *Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.*

- *Imponer una selección de contraseñas de calidad según lo señalado en el punto Uso de la información de autenticación secreta.*

- *Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas.*
- *Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.*

- *Mantener un registro de las últimas tres contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.*

- *Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.*

- *Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.*

- *Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.*

- *Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware.*

- *Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.*

Uso de programas utilitarios privilegiados

El uso de programas utilitarios que podrían ser capaces de saltear los controles de sistemas y de aplicaciones deberá ser restringido y estrictamente controlado.

Deberán considerarse las siguientes guías para el uso de programas utilitarios:

- *Utilizar procedimientos de identificación, autenticación y autorización para programas utilitarios.*
- *Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados y evitar que personas ajenas al Gobierno de Córdoba tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.*
- *Establecer autorizaciones para uso ad hoc de utilitarios de sistema.*
- *Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.*
- *Registrar todo uso de utilitarios del sistema.*
- *Definir y documentar los niveles de autorización para utilitarios del sistema.*
- *Remover o deshabilitar todo los programas utilitarios innecesarios.*
- *No proporcionar acceso a los programas utilitarios a usuarios con acceso a las aplicaciones sobre los sistemas donde se requiere segregación de funciones.*

Control de acceso al código fuente

El acceso al código fuente de programas deberá restringirse.

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

001930

Ing. Juan D'Amico
Director General de Coordinación
Infraestructura Tecnológica
Secretaría General de la Gobernación
Gobierno de la Provincia de Córdoba

- *El código fuente de programas no será mantenido en los sistemas operacionales*
- *Las bibliotecas de código fuente y el código fuente será administrado por el responsable de sistemas*
- *El personal de soporte no tendrá acceso irrestricto a las bibliotecas de código fuente.*
- *La actualización de las bibliotecas de código fuente y los ítems asociados y la asignación de código fuente a programadores sólo será realizado con la aprobación del responsable de sistemas*
- *Los listados de programas se mantendrán en un ambiente seguro.*
- *El mantenimiento y copia de las bibliotecas de código fuente estará sujeto al Procedimiento de Control de Cambios.*

Sera responsabilidad del propietario de la información y el responsable de sistemas del gobierno de Córdoba la realización y control del acceso al código fuente y a la manipulación de este por parte de los desarrolladores. Desde la DGCIT se realizara el apoyo para la detección de códigos fuente o repositorios alojados en aplicaciones productivas o en equipos informáticos no destinados para tal fin, como estaciones de trabajo. Informando al Responsable de Sistemas del Gobierno con un informe detallado con la información detectada.

Política Particular de Seguridad en las relaciones con proveedores

1.2. Relaciones con Proveedores

1.2.1. Objetivo

Establecer y mantener el nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos con proveedores, y proteger los activos del organismo que sean accesibles por proveedores.

1.2.2. Alcance

Los activos informáticos del Gobierno de Córdoba accedidos y los servicios de proveedores en el ámbito de la Infraestructura Tecnológica a cargo de la Secretaria General de la Gobernación.

1.2.3. Responsabilidad

El Responsable de Seguridad Informática, junto con el Propietario de la Información o referente informático, deben definir en función a la criticidad del sistema o servicio informático, los requerimientos de protección cuando sea accedida por proveedores.

El Responsable Jurídico debe garantizar que en los contratos se definan y se acuerden los niveles de seguridad establecidos por el organismo, para lo cual determinará en conjunto con el Responsable de Seguridad Informática y el Responsable de Sistemas la incorporación de consideraciones relativas a la seguridad informática involucrada en la gestión de los productos o servicios prestados.

El Responsable de la Dirección General de Coordinación de Infraestructura Tecnológica cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad Informática y de todas las normas, procedimientos y prácticas relacionadas.

Ing. Juan D'Amico
Director General de Coordinación de Infraestructura Tecnológica
Secretaría General de la Gobernación
Gobierno de la Provincia de Córdoba

001930

1.2.4. Política

1.2.4.1. Objetivo de Control - Seguridad informática en las relaciones con proveedores

- *Asegurar la protección de los activos informáticos del organismo que son accesibles por proveedores.*

1.2.4.2. Controles

Política de Seguridad informática para relaciones con proveedores

Los requisitos de seguridad informática para mitigar los riesgos asociados con acceso de proveedores a los activos del organismo serán acordados con el proveedor y documentados.
Toda persona física o jurídica que acceda, procese, comunique o administre información de la Infraestructura Tecnológica del Gobierno de la Provincia de Córdoba a cargo de la DGCIT, lo realizará de forma tal que las obligaciones legales, regulatorias y definidas por la Política de Seguridad sean cumplidas.
Toda persona con el nivel de autoridad para realizar contrataciones a Proveedores de tecnología deberá aplicar los requisitos fijados por esta Política y los procesos asociados de compras públicas. Toda relación con una tercera parte seguirá el ciclo de vida indicado en los procedimientos específicos de compras, y será respaldado con un contrato.
Los accesos a los activos informáticos y sistemas serán los mínimos necesarios para alcanzar los propósitos de la prestación de funciones.
Cuando finalice la necesidad de acceder a los sistemas de información de la Infraestructura Tecnológica a cargo de la DGCIT, activos y sistemas de información, todo equipamiento de la Infraestructura Tecnología (equipamiento móvil, credenciales de acceso, entre otros) deberán ser devueltos a previo a la finalización del contrato.
La Dirección General de Coordinación de Infraestructura Tecnológica podrá monitorear el uso de su información, activos de información y sistemas de información con propósitos legales.
Todo usuario con acceso otorgado a la información, activos de información y sistemas de información deberá cumplir con los requisitos especificados en

la Política General de Seguridad Informática, incluyendo las Políticas Particulares de Acceso y Uso Aceptable de Activos. El no cumplimiento de estas políticas y otras instrucciones aplicables puede constituir una brecha al contrato y conducir a su terminación y/o acciones legales.
Los medios removibles y los dispositivos móviles podrán ser utilizados para gestionar información de los sistemas informáticos que corren en Infraestructura Tecnológica de Gobierno, solamente con el consentimiento explícito del Responsable de la DGCIT. Deberán aplicarse controles criptográficos a todo medio removible y dispositivo móvil autorizado.
Todo acceso físico de la tercera parte o de su personal dependiente a áreas seguras será escoltado y deberán portar en forma permanente y visible su identificación.
Todo proveedor firmará un Acuerdo de Confidencialidad previo al inicio de las prestaciones o cuando exista un cambio en las características de la prestación. Cada una de las personas que actúen en nombre del proveedor, independiente de su relación con el mismo, firmarán también un Acuerdo de Confidencialidad con la Dirección General de Coordinación de Infraestructura Tecnológica del Gobierno de la Provincia de Córdoba.

Seguridad de la información en los acuerdos con proveedores

Todos los requisitos de seguridad de la información relevantes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer componentes de infraestructura de TI para la información del organismo.
Se deberán establecer acuerdos con los proveedores en los cuales se incluyan los requisitos de seguridad relevantes. En los acuerdos deberá participar de forma obligatoria el propietario de la información o referente informático de la unidad organizativa que contrate al proveedor

Cadena de abastecimiento de Tecnología de la Información y Comunicaciones

Los acuerdos con proveedores deberán incluir los requerimientos para abordar los riesgos de seguridad informática asociados con la cadena de abastecimiento de productos y servicios de tecnología de la información y comunicaciones.

Se deberán establecer los requerimientos de seguridad informática a aplicar a la adquisición de productos o servicios de Tecnología de la Información y

001958

Ing. Juan D'Amico
Director General de Coordinación de
Infraestructura Tecnológica
Secretaría General de la Gobernación
Gobierno de la Provincia de Córdoba

Comunicaciones, adicionales a los requerimientos generales de seguridad informática para las relaciones con proveedores.

1.2.4.3. Objetivo de Control - Gestión de la prestación de servicios de proveedores

- *Mantener un nivel acordado de seguridad informática y entrega de servicios en línea con los acuerdos de proveedores.*

1.2.4.4. Controles

Monitoreo y revisión de los servicios de proveedores

LA DGCIT monitoreará, revisará y auditará en forma regular la prestación de servicios de proveedores.
Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad informática y las condiciones definidas en los acuerdos, y que los incidentes de seguridad informática y los problemas son manejados en forma apropiada.
LA DGCIT mantendrá control suficiente y visión general de todos los aspectos de seguridad para los sistemas informáticos sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte.

Gestión de cambios a los servicios de proveedores

Los cambios a la provisión de servicios por proveedores, incluyendo el mantenimiento y la mejora a las políticas, procedimientos y controles de seguridad informática, serán gestionados, teniendo en cuenta la criticidad del sistema informático del gobierno, los activos informáticos y procesos involucrados y las re-evaluaciones de riesgos.
Se considerarán los siguientes aspectos para la gestión de cambios a los servicios de proveedores:

- *Cambios a los acuerdos de proveedores tecnológicos*

- *Cambios realizados por el Gobierno para implementar:*

- *modificaciones o actualizaciones de las políticas y procedimientos del Organismo*
- *nuevos o cambios en los controles para resolver incidentes de la seguridad de la información y para mejorar la seguridad*

- *Cambios en los servicios de proveedores para implementar:*
  - *cambios y mejoras de las redes*
  - *uso de nuevas tecnologías*
  - *adopción de nuevos productos o nuevas versiones*
  - *nuevas herramientas de desarrollo y ambientes*
  - *cambios de las ubicaciones físicas de las instalaciones de servicio*
  - *cambio de proveedores*
  - *subcontratación a otro proveedor.*

Ing. Juan D'Amico
Director General de Coordinación de
Infraestructura Tecnológica
Secretaría General de la Gobernación
Gobierno de la Provincia de Córdoba