CEDOM.

Municipalidad de la Ciudad de San Juan

INTENDENCIA

DECRETO N° 0436.-.-

San Juan 16 de Marzo de 2021.-

VISTOS:

El Expediente Nº 11083- S/20, la Ley Nacional Nº 25.326 y

CONSIDERANDO:

Que el Sr. Subsecretario de Modernización dependiente de Coordinación de Gabinete impulsa a través de las presentes actuaciones el dictado de una norma a través de la cual se implemente, diseñe y publicite en todo el ámbito de la Municipalidad de la Ciudad de San Juan una política de tratamiento de datos personales.

Que el principio fundante de dicha política seria garantizar la protección integral de los datos personales asentados tanto en archivos, registros, como en bancos de datos u otros medios técnicos de tratamiento de datos.

Que la iniciativa responde a la necesidad de adecuar la legislación Municipal a lo ya dispuesto por el Congreso de la Nación Argentina a través de la sanción de la Ley 25.326 de octubre de 2000, cuyas disposiciones, en particular lo prescripto por los Capítulos I, II, III y IV, y artículo 32, son de orden público y resultan aplicables en todo el territorio de la Nación conforme lo establece su Artículo 44 (Ámbito de Aplicación).

Que con tal objeto resulta necesario avanzar en una nueva etapa profundizando la cultura de protección de datos personales en el ámbito del gobierno municipal.

Que a tal fin la Subsecretaría de Modernización dependiente de la Coordinación de Gabinete del Municipio de la Ciudad de San Juan ha elaborado un texto basado en la "Política Modelo De Protección De Datos Personales Para Organismos Públicos" elaborada por la Agencia de Acceso a la Información Pública dependiente de la Jefatura de Gabinete de Ministros de la Nación Argentina, correspondiendo sea aprobada por el Ejecutivo Municipal.

Que han tomado intervención Fiscalía General y Dirección de Legal y Técnica, sugiriendo prosiga trámite de adhesión y aprobación pertinente.

POR ELLO:

ES COPIA
OPTO. ADMINISTRACION

EL INTENDENTE DE LA MUNICIPALIDAD DE LA CIUDAD DE SAN JUAN

DECRETA:

ARTICULO 1º: Aprúebase el documento: "Política de Seguridad de la Información para el Municipio de la Ciudad de San Juan" que como Anexo I forma parte integrante de la presente, como pauta básica sugerida para el diseño del documento que publicite la protección de datos personales de los organismos del Municipio titulares de bases de datos personales.

ARTICULO 2º: Desígnase como Autoridad de Aplicación de la presente al Sr. Coordinador de Gabinete, o a quien en el futuro lo reemplace.

ARTICULO 3º: Invítase al Concejo Deliberante a adherir a la presente.

ARTICULO 4º: Protocolícese, publíquese y dese al Registro Oficial.-

Dr. EMILIO BAISTROCCHI
INTENDENTE MUNICIPAL
MUNICIPALIDAD DE LA CIUDAD DE SAN JUAN

Lic. SERGIO MORDACCI
COORDINADOR DE GABINETE
MUNICIPALIDAD DE LA CIUDAD DE SAN JUAN

ANEXO I

Política de Seguridad de la Información para el Municipio de la Ciudad de San Juan.

1) TÉRMINOS Y DEFINICIONES

A los efectos de este documento se aplican las siguientes definiciones:

1. **Seguridad de la Información.**

La seguridad de la información se entiende como la preservación de las siguientes características:

1. **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
0. **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
3. **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

4. **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
5. **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
6. **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
7. **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
8. **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la Municipalidad de la Ciudad de San Juan .
9. **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

10. **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
11. **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
12. **Tecnología de la Información**: Se refiere al hardware y software operados por la Municipalidad de la Ciudad de San Juan o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la

Municipalidad de la Ciudad de San Juan, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2. **Evaluación de Riesgos.**
   Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la Municipalidad de la Ciudad de San Juan.
3. **Administración de Riesgos.**
   Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
4. **Amenaza:** Una causa potencial de un incidente no deseado que puede ocasionar daños a un sistema u organismo.
5. **Vulnerabilidad**: Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.
6. **Incidente de Seguridad.**
   Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
7. **Activos de Información.**
   Son los bienes relacionados a un sistema de información en cualquiera de sus etapas. Ejemplos de activos son:
   1. **Información**: Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, resultados de proyectos de investigación, etc.

2. Software: Software de aplicaciones, software de sistemas, herramientas de desarrollo, etc.

3. Activos físicos: Computadoras, equipamiento de redes y comunicaciones, medios de almacenamiento, mobiliario, lugares de emplazamiento.

4. Servicios: Servicios informáticos y de comunicaciones.

8. **Aplicación.**
   Se refiere a un sistema informático, tanto desarrollado por la Municipalidad de la Ciudad de San Juan como por terceros, o al sistema operativo o software de base, que integren los sistemas de información o donde estos estén alojados.
9. **Norma.**
   Regla de comportamiento dictada por una autoridad competente que se debe seguir o a la que se deben ajustar las conductas, tareas, actividades, etc.
10. **Procedimiento.**

Acciones que se realizan, con una serie común de pasos claramente definidos, que permiten realizar correctamente una tarea o alcanzar un objetivo. Se distinguen dos clases de procedimientos: obligatorios y recomendados. Estos últimos representan "buenas prácticas", que son aconsejables, pero no

requeridas. Si en un procedimiento no se utiliza la palabra "recomendado" se asume que es obligatorio.

11. **Proceso de Información.**
    Conjunto de tareas relacionadas lógicamente que se realizan para lograr un resultado determinado en un Sistema de Información.

12. **Registro.**
    Conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos, informatizada o no.

2) EVALUACIÓN Y TRATAMIENTO DE RIESGOS

1. GENERALIDADES

Todo Organismo se encuentra expuesto a riesgos en materia de seguridad de la información. No existe la seguridad completa, por lo que es necesario conocer cuál es el mapa de riesgos al cual se enfrenta el organismo y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos.
Es por ello que resulta imprescindible gestionar los riesgos del Organismo, como pilar fundamental para la gestión de seguridad.

2. OBJETIVO

Conocer los riesgos a los que se expone el Organismo en materia de seguridad de la información.
Generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

3. ALCANCE

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

4. RESPONSABILIDAD

El Comité de Seguridad de la Información será responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo.
El Responsable de Seguridad de la Información junto con los Titulares de Unidades Organizativas será responsable del desarrollo del proceso de gestión de riesgos de seguridad de la información.

5. POLÍTICA

I. EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD

El Organismo evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos. Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de una evaluación de riesgos puede incluir a todo el Organismo, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios. Resulta recomendable seguir una metodología de evaluación de riesgos para llevar a cabo el proceso.

2. TRATAMIENTO DE RIESGOS DE SEGURIDAD

Antes de considerar el tratamiento de un riesgo, el Organismo debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Los riesgos pueden ser aceptados si por ejemplo: se evaluó que el riesgo es bajo o que el costo del tratamiento no es económicamente viable para la organización. Tales decisiones deben ser tomadas por las autoridades y debidamente documentadas.

Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

A. Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos;
B. Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del Organismo;
C. Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de estos;
D. Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedores.

Para aquellos riesgos donde la decisión ha sido la mitigación, se buscará reducir los riesgos a un nivel aceptable mediante la implementación de controles, teniendo en cuenta lo siguiente:

A. requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales;
B. objetivos organizacionales;
C. requerimientos y restricciones operativos;
D. costo de implementación y operación en relación directa a los riesgos reducidos, y proporcionales a los requerimientos y restricciones del Organismo;
E. la necesidad de equilibrar las inversiones en la implementación y operación de los controles contra el daño que podría resultar de las fallas de seguridad.

Los controles a implementar pueden ser seleccionados del contenido de las cláusulas de esta política, o se pueden establecer nuevos controles para satisfacer necesidades específicas del

2. RESPONSABILIDADES

El Responsable de Seguridad de la Información tendrá a su cargo las siguientes tareas:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- 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 las redes del organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

El Responsable de Seguridad de la Información junto con el responsable del área legal evaluará los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados. Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

3. GESTIÓN DE PROVISIÓN DE SERVICIOS

Se deberá implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros. El organismo debe verificar la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con la tercera persona. Se verificará, además, que los servicios brindados por una tercera parte incluyan los acuerdos de seguridad arreglados, definiciones de servicio, y aspectos de la gestión del servicio. En el caso de acuerdos de tercerización, el organismo debe planificar las transiciones necesarias (de la información, de las instalaciones de procesamiento de información, y cualquier otro componente que necesite ser trasladado), y que asegure que la seguridad sea mantenida a lo largo del período de transición.

4. PROTECCIÓN CONTRA CÓDIGO MALICIOSO

El software malicioso es un 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. 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 mediante la utilización de una herramienta antivirus.

El Responsable de Seguridad de la Información definirá e implementará los controles de detección y eliminación de software malicioso (virus informáticos, troyanos, gusanos, malware en general; incluyendo código móvil), minimizando el riesgo de infección y propagación, e impidiendo los accesos no autorizados, robo o destrucción de información. Estos controles involucrarán:

- Verificar que no se esté utilizando software no autorizado.
- Verificar la instalación y actualización periódica del software antivirus.
- Verificar el mantenimiento de los sistemas con las últimas actualizaciones de seguridad disponibles. Dicha situación debe estar reflejada en los contratos con el proveedor.

5. PROCEDIMIENTOS DE RESGUARDO DE LA INFORMACIÓN

El Responsable de Seguridad de la Información junto a los Propietarios de Información determinará los requerimientos para resguardar cada software o dato en función de su criticidad. Sobre la base de ello, se definirá y se documentará un esquema de resguardo de la información. El

3. ADMINISTRACIÓN DE ACCESOS DE USUARIOS

Con el objetivo de impedir el acceso no autorizado a la información, se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información. Los procedimientos deberán abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. En la administración de accesos, deberán tomarse en cuenta los siguientes requisitos:

- Todos los usuarios deben disponer de un identificador único que permita asociar las actividades del sistema a un responsable individualizado.
- Los accesos deben seguir el principio de "menor privilegio", permitiendo al usuario escalar el acceso a los recursos de información, en función de sus necesidades definidas en su puesto de trabajo.
- El registro de usuario se deberá mantener actualizado con identificación de derechos de acceso.
- Cada usuario deberá ser notificado por escrito u otro medio fehaciente de sus derechos de acceso, sus restricciones y privilegios.
- El derecho de acceso de los usuarios deberá ser revisado en intervalos no inferiores a tres meses, así como las autorizaciones de privilegios especiales de derechos de accesos.
- Se recomiendo utilizar el protector de pantalla con contraseña para las estaciones de trabajo con activación automática a partir de los 15 minutos de inactividad en el sistema.

4. RESPONSABILIDADES DEL USUARIO

Se deberá evitar el acceso de usuarios no autorizados, poner en peligro la información y el robo de información y los medios de procesamiento de la información. La cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario. Asimismo, se deberán seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario y, consecuentemente, un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

5. CONTROL DE ACCESO A LA RED

Se debe controlar el acceso a los servicios de redes internas y externas, evitando el acceso no autorizado. El acceso del usuario a las redes y servicios de estas no debe comprometer la seguridad.

6. CONTROL DE ACCESO A INTERNET

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Responsable de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Propietario de la Información del organismo a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

7. CONTROL DE ACCESO AL SISTEMA OPERATIVO

Se deben utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios no autorizados. 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 contraseñas individuales para determinar responsabilidades.
- Efectuarse al azar, y cuando el usuario se registre por primera vez, el sistema deberá forzar un cambio de contraseña para mejorar la confiabilidad.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de estas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Generar un vencimiento periódico, para que deba ser cambiada al menos con una frecuencia de tres meses.
- 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 (por ejemplo, claves de impresoras, hubs, routers, etc.).

Organismo. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o a su ambiente, y podrían no ser aplicables en todos los Organismos.

Se debe recordar que ningún conjunto de controles puede alcanzar la seguridad absoluta. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.

3) RESPONSABILIDADES

1. BÁSICAS

La implementación de la presente política dentro de la estructura del organismo requiere del trabajo conjunto del Responsable de Seguridad Informática, de los Propietarios de la Información y del Responsable de Tecnología de la Información, quienes llevarán a cabo las siguientes funciones:

- Revisar y proponer a la máxima autoridad del organismo para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información.
- Garantizar que la seguridad de la información sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y el apoyo a la seguridad de la información dentro del organismo y coordinar el proceso de administración de la continuidad de las actividades del organismo.

COMITÉ DE SEGURIDAD DE INFORMACIÓN

Según las características del organismo, se podrá conformar un Comité de Seguridad de Información integrado por representantes de las distintas áreas del organismo, destinado a garantizar las iniciativas de seguridad.

2. COMPLEMENTARIAS

1. LOS PROPIETARIOS DE LA INFORMACIÓN Y PROPIETARIOS DE ACTIVOS

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 y sus principales responsabilidades serán:

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de esta.
- Documentar y mantener actualizada la clasificación arriba mencionada.
- Definir qué usuarios deben tener permisos de acceso a la información de acuerdo con sus funciones y su competencia.

2. CUSTODIO

Tiene la posesión de la información y administra técnicamente los sistemas que utilizan esta información. Esta responsabilidad deberá ser asignada al responsable de Tecnología de la Información (en adelante TI) .Sus funciones son:

- 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 de cualquier incidente o sospecha de violación de acceso a la información.

3. EL RESPONSABLE DE TECNOLOGÍA DE LA INFORMACIÓN

Cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del organismo Asimismo, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

4. EL RESPONSABLE DEL ÁREA LEGAL

Verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del organismo con sus empleados y con terceros. Asimismo, asesorará en materia legal al organismo, en lo que se refiere a la seguridad de la información.

5. ACTIVIDAD DE AUDITORÍA INTERNA

Deberá practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

4) SEGURIDAD DEL PERSONAL

1. AL MOMENTO DE LA INCORPORACIÓN DE UN AGENTE

Deberá notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de las pautas de seguridad de la información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación del presente manual a todo el personal de los cambios que en él se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

2. DURANTE EL EMPLEO

1. RESPONSABILIDADES DEL ÁREA DE RECURSOS HUMANOS

El área de Recursos Humanos solicitará a los empleados, contratistas y usuarios de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos cumpliendo con lo siguiente:

Estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a información sensible o a los sistemas de información.

- Estar provistos de guías para establecer las expectativas de seguridad de su rol dentro del organismo.
- Tener la suficiente motivación para cumplir con las políticas de seguridad del organismo.
- Cumplir con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del organismo y métodos adecuados de trabajo.

3. DESVINCULACIÓN O CAMBIO DE PUESTO

Al momento del cese de las actividades de un empleado en el organismo, deberá comunicar fehacientemente este hecho al Responsable de Seguridad de la Información y al responsable de TI, quien deberá bloquear todos los accesos de esa persona a la red y desafectar todos sus privilegios en caso de desvinculación. Si el agente sufriera un cambio de puesto dentro del organismo, se le deberán actualizar sus roles y permisos en función de la nueva asignación.

4. PROCESOS DISCIPLINARIOS

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Municipalidad de la Ciudad de San Juan, para los empleados que violen la Política, Normas y Procedimientos de Seguridad del municipio.

5) SEGURIDAD FÍSICA Y AMBIENTAL

1. GENERALIDADES

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños, pérdidas e interferencias a la información y a las operaciones del organismo. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad. El establecimiento de perímetros de seguridad y de áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del organismo y de accesos físicos no autorizados. El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del organismo así como en instalaciones próximas a la sede, que puedan interferir con las actividades. El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del organismo. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. También se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al organismo pero situado físicamente fuera de este (housing) así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al organismo (hosting). La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento son susceptibles de ser recuperadas mientras no están siendo utilizadas. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados. Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación; y para su destrucción cuando así lo amerite.

2. RESPONSABILIDADES

El Responsable de Seguridad de la Información junto con el Propietario de la Información y la Unidad de Auditoría Interna definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos. El Responsable de Seguridad de la Información junto con el Propietario de la Información definirán, en función de la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad de la Información definirá junto con el responsable de TI los métodos de encriptación para ser utilizados. El Responsable de Seguridad de la Información, además, cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para el control de cambios a los sistemas, para la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas, para el control de código malicioso y para la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable de Seguridad de la Información propondrá para su aprobación, por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas. El responsable de TI propondrá quiénes realizarán la administración de las técnicas criptográficas y claves. El área legal incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software.

9) PLANIFICACIÓN DE LA CONTINUIDAD OPERATIVA

1. GENERALIDADES

Definición de "contingencia": situación que necesita ser controlada, mediante la ejecución de un plan de acción coordinado, a fin de evitar o minimizar daños. En tal sentido, el desarrollo del plan y tratamiento de las contingencias informáticas se debe focalizar en dar respuestas a dos preguntas claves:

- Cuáles son los recursos informáticos relacionados con los procesos críticos del organismo.
- Cuál es el período de tiempo de recuperación crítico de los recursos de información en el que deben activarse los mecanismos alternativos específicos, antes de que se experimenten pérdidas significativas.

2. RESPONSABILIDADES

El responsable de TI debe arbitrar los medios necesarios a los efectos de minimizar las interrupciones de las actividades del organismo y asegurar la continuidad de la operación de los procesos críticos, protegiendo los activos de información y de los equipos que los soportan de fallas imprevistas. Asimismo deberá redactar los procedimientos correspondientes que especifiquen claramente los pasos a seguir ante la ocurrencia de eventos no deseados. Ante la ocurrencia de un evento que provoque la discontinuidad del servicio (caída en el procesamiento de los equipos, interrupción en los servicios de comunicaciones, desastres naturales, atentados, etc.) deberá:

- Evaluar el impacto en el organismo (definir los perjuicios económicos, financieros, políticos, de imagen, legales, etc.).
- Desarrollar una estrategia de recupero (deben existir varias alternativas de recupero de la información).
- Documentar el plan de recupero (desarrollo de procedimientos técnicos e inventarios de hardware, software, redes, etc.).
- Testear y mantener el plan (ej.: testeo, desarrollo de pruebas, mantenimiento actualizado del plan).
- Identificar y aplicar controles preventivos.

El plan debe contar con procedimientos de resguardo de datos (back-ups) conteniendo una planificación detallada con la cantidad, frecuencia, lugares apropiados de almacenamiento tanto internos como externos, inventarios detallados, etc. Estos procedimientos deben prever, como mínimo, la generación de copias de resguardo, con frecuencia diaria, de toda la información de los equipos centrales. A su vez, se deben realizar pruebas formales y debidamente documentadas de recuperación y de integridad de los resguardos de datos. Las prácticas y procedimientos que se desarrollen, alineados con la Política de Continuidad de Negocios, deberán ser evaluados por el Responsable de la Información junto a los Propietarios de la Información y podrán ser auditados por la Unidad de Auditoría Interna. Los planes, procedimientos y prácticas que se implementen deberán ser aprobados por la máxima autoridad del organismo y actualizados periódicamente a fin de garantizar que se encuentran al día y que continúan siendo efectivos en el tiempo.

Lic. SERGIO MORDACCI
COORDINADOR DE GABINETE
MUNICIPALIDAD DE LA CIUDAD DE SAN JUAN

Dr. Emilio Baistrocchi
Intendente
Municipalidad de la Ciudad de San Juan

2. RESPONSABILIDADES

El Responsable de Seguridad de la Información tendrá a su cargo las siguientes tareas:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- 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 las redes del organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

El Responsable de Seguridad de la Información junto con el responsable del área legal evaluará los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados. Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

3. GESTIÓN DE PROVISIÓN DE SERVICIOS

Se deberá implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros. El organismo debe verificar la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con la tercera persona. Se verificará, además, que los servicios brindados por una tercera parte incluyan los acuerdos de seguridad arreglados, definiciones de servicio, y aspectos de la gestión del servicio. En el caso de acuerdos de tercerización, el organismo debe planificar las transiciones necesarias (de la información, de las instalaciones de procesamiento de información, y cualquier otro componente que necesite ser trasladado), y que asegure que la seguridad sea mantenida a lo largo del período de transición.

4. PROTECCIÓN CONTRA CÓDIGO MALICIOSO

El software malicioso es un 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. 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 mediante la utilización de una herramienta antivirus.

El Responsable de Seguridad de la Información definirá e implementará los controles de detección y eliminación de software malicioso (virus informáticos, troyanos, gusanos, malware en general; incluyendo código móvil), minimizando el riesgo de infección y propagación, e impidiendo los accesos no autorizados, robo o destrucción de información. Estos controles involucrarán:

- Verificar que no se esté utilizando software no autorizado.
- Verificar la instalación y actualización periódica del software antivirus.
- Verificar el mantenimiento de los sistemas con las últimas actualizaciones de seguridad disponibles. Dicha situación debe estar reflejada en los contratos con el proveedor.

5. PROCEDIMIENTOS DE RESGUARDO DE LA INFORMACIÓN

El Responsable de Seguridad de la Información junto a los Propietarios de Información determinará los requerimientos para resguardar cada software o dato en función de su criticidad. Sobre la base de ello, se definirá y se documentará un esquema de resguardo de la información. El

responsable de TI dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración e integridad. Para esto se debe contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del organismo Los sistemas de resguardo deben probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del organismo. A continuación, se detallarán procedimientos para el resguardo de la información, que deben considerar los siguientes puntos:

- Definir un esquema de rótulo de las copias de resguardo que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo con lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
- Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de estas, y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deben retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el organismo.
- Probar periódicamente los medios de resguardo.
- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Las prácticas y procedimientos se evaluarán con la participación de la Unidad de Auditoría Interna.

6. USO DEL CORREO ELECTRÓNICO

El responsable de TI deberá garantizar la provisión de una casilla de correo electrónico a cada agente del organismo. La casilla de correo otorgada al usuario es propiedad del organismo, independientemente del nombre y clave de acceso que sean necesarios para su utilización, por lo que su utilización debe relacionarse con fines laborales, vinculados a las actividades del organismo.

Los nombres de las casillas de correo electrónico los otorgará el responsable de TI. Entre las actividades prohibidas se encuentran:

- Leer, interceptar o revelar comunicaciones electrónicas pertenecientes a otro usuario sin su autorización previa y expresa.
- Divulgar las claves o contraseñas de acceso personales.

Con el objeto de minimizar el riesgo de violación a la seguridad a través del uso incorrecto del servicio de correo electrónico, se recomienda:

- Analizar los archivos adjuntos descargados con la herramienta antivirus instalada en las estaciones clientes.

- No adjuntar archivos mayores a 5 MB. Es conveniente utilizar herramientas de compresión, para minimizar el tamaño de los adjuntos.

Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información adjunta en él.

7) CONTROL DE ACCESO

1. GENERALIDADES

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información, se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso. La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizarlos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

2. RESPONSABILIDADES

El Responsable de la Seguridad de la Información será quien administre los niveles de acceso definidos por el máximo responsable del organismo junto con los propietarios de la Información. A su vez, deberá crear, implementar y verificar el cumplimiento de las pautas relacionadas con el control de accesos, registración de usuarios, administración de privilegios, otorgamiento de contraseñas, utilización de servicios de red, registro de eventos, protección de puertos, control de conexiones a la red, etcétera.
El responsable del área de Recursos Humanos es el responsable de efectuar un control mensual de las modificaciones de puestos de trabajo y/o baja de personal, y/o modificación de equipos de trabajo, y notificar al responsable de TI para que efectúe las acciones correspondientes.
Los usuarios serán responsables de concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, como ser un protector de pantalla protegido por contraseña. Al terminar la jornada laboral o al dejar de utilizar la PC, los usuarios deberán apagarla con todos los periféricos asociados (ej.: impresoras, monitores, etc.). La Unidad de Auditoría Interna tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

- Garantizar que el medio utilizado para acceder o utilizar el sistema de contraseñas asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.
- Denegar el acceso al sistema luego de tres intentos fallidos.
- Mantener un registro, como mínimo, de las últimas tres contraseñas utilizadas por el usuario y evitar la reutilización de estas.

8. MONITOREO DEL ACCESO y USO DE LOS SISTEMAS

Se deberá verificar la existencia de procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, asegurando que se registren y se evalúen todos los eventos significativos para la seguridad de accesos. Se generarán, además, registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad, incluyendo la siguiente información:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Identidad o ubicación de la terminal, si se hubiera dispuesto su identificación automática.
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros. Los Propietarios de la Información junto con el Responsable de la Seguridad de la Información, deberán definir un cronograma de depuración de registros en línea en función de normas vigentes y de sus propias necesidades.
Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados. La periodicidad de dichas revisiones será definida por los Propietarios de la Información y el Responsable de Seguridad de la Información, de acuerdo con la evaluación de riesgos efectuada.

9. DISPOSITIVOS MÓVILES

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura del organismo. Se debe tener en cuenta, en este sentido, cualquier dispositivo móvil o removible, teléfonos celulares y sus tarjetas de memoria, dispositivos de almacenamiento removibles tales como CD o DVD, dispositivos de almacenamiento de conexión USB, tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc. La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo, hurto e

ingreso de software malicioso. En consecuencia, debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales por observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención acerca de portar un equipo valioso.
- No poner identificaciones del organismo en el dispositivo, salvo los estrictamente necesarios.
- No poner datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.

Asimismo, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del organismo, los que incluirán:

- Revocación de las credenciales afectadas.
- Notificación a grupos de trabajo donde potencialmente se pudieran haber comprometido recursos.

8) SEGURIDAD EN EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS

1. GENERALIDADES

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad e incorporarlos en las etapas de desarrollo e implementación. Adicionalmente, se deben diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos. Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer/ alterar la integridad de las bases de datos), y en el caso de que se lleven a cabo, identificar rápidamente al responsable. Asimismo, es necesaria una adecuada administración de la infraestructura de base, sistemas operativos y software de base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software. Se debe asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información. También se deben definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

2. RESPONSABILIDADES

El Responsable de Seguridad de la Información junto con el Propietario de la Información y la Unidad de Auditoría Interna definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos. El Responsable de Seguridad de la Información junto con el Propietario de la Información definirán, en función de la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad de la Información definirá junto con el responsable de TI los métodos de encriptación para ser utilizados. El Responsable de Seguridad de la Información, además, cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para el control de cambios a los sistemas, para la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas, para el control de código malicioso y para la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable de Seguridad de la Información propondrá para su aprobación, por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas. El responsable de TI propondrá quiénes realizarán la administración de las técnicas criptográficas y claves. El área legal incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software.

9) PLANIFICACIÓN DE LA CONTINUIDAD OPERATIVA

1. GENERALIDADES

Definición de "contingencia": situación que necesita ser controlada, mediante la ejecución de un plan de acción coordinado, a fin de evitar o minimizar daños. En tal sentido, el desarrollo del plan y tratamiento de las contingencias informáticas se debe focalizar en dar respuestas a dos preguntas claves:

- Cuáles son los recursos informáticos relacionados con los procesos críticos del organismo.
- Cuál es el período de tiempo de recuperación crítico de los recursos de información en el que deben activarse los mecanismos alternativos específicos, antes de que se experimenten pérdidas significativas.

2. RESPONSABILIDADES

El responsable de TI debe arbitrar los medios necesarios a los efectos de minimizar las interrupciones de las actividades del organismo y asegurar la continuidad de la operación de los procesos críticos, protegiendo los activos de información y de los equipos que los soportan de fallas imprevistas. Asimismo deberá redactar los procedimientos correspondientes que especifiquen claramente los pasos a seguir ante la ocurrencia de eventos no deseados. Ante la ocurrencia de un evento que provoque la discontinuidad del servicio (caída en el procesamiento de los equipos, interrupción en los servicios de comunicaciones, desastres naturales, atentados, etc.) deberá:

- Evaluar el impacto en el organismo (definir los perjuicios económicos, financieros, políticos, de imagen, legales, etc.).
- Desarrollar una estrategia de recupero (deben existir varias alternativas de recupero de la información).
- Documentar el plan de recupero (desarrollo de procedimientos técnicos e inventarios de hardware, software, redes, etc.).
- Testear y mantener el plan (ej.: testeo, desarrollo de pruebas, mantenimiento actualizado del plan).
- Identificar y aplicar controles preventivos.

El plan debe contar con procedimientos de resguardo de datos (back-ups) conteniendo una planificación detallada con la cantidad, frecuencia, lugares apropiados de almacenamiento tanto internos como externos, inventarios detallados, etc. Estos procedimientos deben prever, como mínimo, la generación de copias de resguardo, con frecuencia diaria, de toda la información de los equipos centrales. A su vez, se deben realizar pruebas formales y debidamente documentadas de recuperación y de integridad de los resguardos de datos. Las prácticas y procedimientos que se desarrollen, alineados con la Política de Continuidad de Negocios, deberán ser evaluados por el Responsable de la Información junto a los Propietarios de la Información y podrán ser auditados por la Unidad de Auditoría Interna. Los planes, procedimientos y prácticas que se implementen deberán ser aprobados por la máxima autoridad del organismo y actualizados periódicamente a fin de garantizar que se encuentran al día y que continúan siendo efectivos en el tiempo.

Lic. SERGIO MORDACCI
COORDINADOR DE GABINETE
MUNICIPALIDAD DE LA CIUDAD DE SAN JUAN

Dr. Emilio Baistrocchi
Intendente
Municipalidad de la Ciudad de San Juan

Certifico que la Presente es Fotocopia Fiel del Original
Dpto. de Administración
16/03/2021

Dra. ROSANA ISABEL GOMEZ
Sub Directora de Despacho
y Boletín Oficial
MUNICIPALIDAD DE LA CIUDAD DE SAN JUAN

Firmado digitalmente por GIL PEREZ Marcelo Adrian
Fecha: 2021.03.18 12:42:04 -03'00'