MANUAL DE OPERACIÓN, POLÍTICA DE INFORMACIÓN, PROCEDIMIENTOS Y REGLAMENTOS

Departamento de Informática y nuevas Tecnologías

ÍNDICE DE CONTENIDO

INTRODUCCIÓN 11

LEYES, BASES Y NORMAS TÉCNICAS 13

MANUAL DE OPERACIÓN 14

Descripción de Funciones 14

DEPARTAMENTO DE INFORMATICA Y NUEVAS TECNOLOGÍAS 14

Organigrama 15

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 16

I. Alcance 17

II. Términos y Definiciones 17

2.1. Seguridad de la Información 17

2.2. Evaluación de Riesgos 18

2.3. Administración de Riesgos 18

2.4.Incidente de Seguridad 18

III. Política de Seguridad de la Información 18

Generalidades 18

Objetivo 18

Alcance 19

Responsabilidad 19

3.1. Aspectos Generales 19

3.2. Sanciones Previstas por Incumplimiento 20

IV Organización de la Seguridad 20

Generalidades 20

Objetivo 21

Alcance 21

4.1. Infraestructura de la Seguridad de la Información 21

4.1.1. Asignación de Responsabilidades en Materia de Seguridad de la Información 21

4.1.2. Proceso de Autorización para Instalaciones de Procesamiento de Información 21

4.1.3. Asesoramiento Especializado en Materia de Seguridad de la Información 21

4.1.4. Revisión Independiente de la Seguridad de la Información 22

4.2. Seguridad Frente al Acceso por Parte de Terceros 22

4.2.1. Identificación de Riesgos del Acceso de Terceras Partes 22

4.2.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros 22

4.3. Tercerización / Externalización / Outsourcing 24

4.3.1. Requerimientos de Seguridad en Contratos de Tercerización 24

V Clasificación y Control de Activos 24

Generalidades 25

Objetivo 25

Alcance 25

Responsabilidad 26
Política de Inventario de Activos 26
5.1. Inventario de activos 26
5.2. Clasificación de la información 26
5.3. Rotulado de la Información 27
VI Seguridad del Personal 28
Generalidades 28
Objetivo 28
Alcance 28
Responsabilidad 28
Política sobre la Seguridad de la Información y el Personal 29
6.1. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos 29
6.1.1. Incorporación de la Seguridad en los Puestos de Trabajo 29
6.1.2. Control y Política del Personal 29
6.1.3. Compromiso de Confidencialidad 29
6.1.4. Términos y Condiciones de Empleo 29
6.2. Capacitación del Usuario 30
6.2.1. Formación y Capacitación en Materia de Seguridad de la Información 30
6.3. Respuesta a Incidentes *y* Anomalías en Materia de Seguridad 30
6.3.1. Comunicación de Incidentes Relativos a la Seguridad 30
6.3.2. Comunicación de Debilidades en Materia de Seguridad 30
6.3.3. Comunicación de Anomalías del Software 31
6.3.4. Aprendiendo de los Incidentes 31
6.3.5. Procesos Disciplinarios 31
VII Seguridad Física y Ambiental 31
Generalidades 31
Objetivo 32
Alcance 32
Responsabilidad 32
Política sobre seguridad Física. 33
7.1. Perímetro de Seguridad Física 33
7.2. Controles de Acceso Físico 33
7.3. Protección de Oficinas, Recintos e Instalaciones 34
7.4. Ubicación y Protección del Equipamiento y Copias de Seguridad 35
7.5. Suministros de Energía 35
7.6. Seguridad del Cableado 35
7.7. Mantenimiento de Equipos 36
7.8. Seguridad de los Equipos Fuera de las Instalaciones. 36
7.9. Desafectación o Reutilización Segura de los Equipos. 37
7.10. Políticas de Escritorios y Pantallas Limpias 37

7.11. Retiro de los Bienes 37
VIII. Gestión de comunicaciones y operaciones 38
Política sobre la operación y las comunicaciones 38
8.1. Procedimientos y Responsabilidades Operativas 38
8.1.1. Documentación de los Procedimientos Operativos 38
8.1.2. Control de Cambios en las Operaciones 38
8.1.3. Procedimientos de Manejo de Incidentes 38
8.1.4. Separación de Funciones 39
8.1.5. Gestión de Instalaciones Externas 40
8.2. Planificación y Aprobación de Sistemas 40
8.2.1. Planificación de la Capacidad 40
8.2.2. Aprobación del Sistema 40
8.3. Protección Contra Software Malicioso 40
8.3.1. Controles Contra Software Malicioso 40
8.4. Mantenimiento 41
8.4.1. Resguardo de la Información 41
8.4.2. Registro de Actividades del Personal Operativo 42
8.4.3. Registro de Fallas 42
8.5. Administración de la Red 42
8.5.1. Controles de Redes 42
8.6. Administración y Seguridad de los Medios de Almacenamiento 42
8.6.1. Administración de Medios Informáticos Removibles 42
8.6.2. Eliminación de Medios de Información 43
8.6.3. Procedimientos de Manejo de la Información 43
8.6.4. Seguridad de la Documentación del Sistema 43
8.7. Intercambios de Información y Software 44
8.7.1. Acuerdos de Intercambio de Información y Software 44
8.7.2. Seguridad de los Medios en Tránsito 44
8.7.3. Seguridad del Gobierno Electrónico 44
8.7.4. Seguridad del Correo Electrónico 8.7.4.1. Riesgos de Seguridad 45
8.7.4.2. Política de Correo Electrónico 45
8.7.5. Seguridad de los Sistemas Electrónicos de Oficina 46
8.7.6. Sistemas de Acceso Público 46
IX. Control de Accesos 47
Generalidades 47
Objetivo 47
Alcance 47
Responsabilidad 47
Política sobre el Control de Acceso 49
9.1. Requerimientos para el Control de Acceso 49
9.1.1. Política de Control de Accesos 49

9.1.2. Reglas de Control de Acceso 49
9.2. Administración de Accesos de Usuarios 49
9.2.1. Registro de Usuarios 49
9.2.2. Administración de Privilegios 50
9.2.3. Administración de Contraseñas de Usuario 50
9.3. Responsabilidades del Usuario 51
9.3.1. Uso de Contraseñas 51
9.4. Control de Acceso a la Red 51
9.4.1. Política de Utilización de los Servicios de Red 51
9.4.2. Autenticación de Usuarios para Conexiones Externas 52
9.4.3. Autenticación de Nodos 52
9.4.4. Protección de los Puertos (Ports) de Diagnóstico Remoto 53
9.4.5. Subdivisión de Redes 53
9.4.6. Acceso a Internet 53
9.4.7. Control de Conexión a la Red 53
9.4.8. Control de Ruteo de Red 53
9.4.9. Seguridad de los Servicios de Red 54
9.5. Control de Acceso al Sistema Operativo 54
9.5.1. Identificación Automática de Terminales 54
9.5.2. Procedimientos de Conexión de Terminales 54
9.5.3. Identificación y Autenticación de los Usuarios 55
9.5.4. Sistema de Administración de Contraseñas 55
9.5.5. Uso de Utilitarios de Sistema 55
9.5.6. Desconexión de Terminales por Tiempo Muerto 56
9.5.7. Limitación del Horario de Conexión 56
9.6. Control de Acceso a las Aplicaciones 56
9.6.1. Restricción del Acceso a la Información 56
9.6.2. Aislamiento de los Sistemas Sensibles 57
9.7. Monitoreo del Acceso y Uso de los Sistemas 57
9.7.1. Registro de Eventos 57
9.7.2. Monitoreo del Uso de los Sistemas 57
9.7.2.1. Procedimientos y Áreas de Riesgo 57
9.7.2.2. Factores de Riesgo 58
9.7.2.3 Registro y revisión de Eventos 58
9.8. Computación Móvil *y* Trabajo Remoto 59
9.8.1. Computación Móvil 59
9.8.2. Trabajo Remoto 60
X. Desarrollo y mantenimiento de sistemas 61
Generalidades 61
Objetivo 61
Alcance 61
Responsabilidad 61

Política de Seguridad de los Sistemas 62
10.1. Requerimientos de Seguridad de los Sistemas 62
10.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad 62
10.2. Seguridad en los Sistemas de Aplicación....62
10.2.1. Validación de Datos de Entrada 62
10.2.2. Controles de Procesamiento Interno 63
10.2.3. Autenticación de Mensajes 63
10.2.4. Validación de Datos de Salidas 63
10.3. Seguridad de los Archivos del Sistema 63
10.3.1. Control del Software Operativo 63
10.3.2. Protección de los Datos de Prueba del Sistema 64
10.3.3. Control de Cambios a Datos Operativos 64
10.4. Seguridad de los Procesos de Desarrollo y Soporte 65
10.4.1. Procedimiento de Control de Cambios 65
10.4.2. Revisión Técnica de los Cambios en el Sistema Operativo 65
10.4.3. Restricción del Cambio de Paquetes de Software 65
10.4.4. Canales Ocultos y Código Malicioso 66
10.4.5. Desarrollo Externo de Software 66
Modelo de separación de ambientes 66
Ambiente de Desarrollo 66
Ambiente de Pruebas 67
Ambiente de Producción 67
XI. Gestión de la Continuidad de la organización 67
Generalidades 67
Objetivo 68
Alcance 68
Responsabilidad 68
Políticas relativas a la Continuidad de Negocio 69
11.1. Proceso de la Administración de la Continuidad del Organismo 69
11.2. Continuidad de las Actividades y Análisis de los Impactos 69
11.3. Elaboración e Implementación de los Planes de Continuidad de las Actividades de la Organización 69
XII. Cumplimiento 70
Generalidades 70
Objetivos 70
Alcance 71
Responsabilidad 71
Política sobre el cumplimiento de Requisitos Legales 71
12.1. Cumplimiento de Requisitos Legales 71
12.1.1. Identificación de la Legislación Aplicable 71
12.1.2. Derechos de Propiedad Intelectual 71

12.1.2.1. Derecho de Propiedad Intelectual del Software 71
12.1.3. Protección de los Registros de la Organización 72
12.1.4. Protección de Datos y Privacidad de la Información Personal 73
12.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información 73
12.1.6. Recolección de Evidencia 73
12.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica 74
12.2.1. Cumplimiento de la Política de Seguridad 74
12.2.2. Verificación de la Compatibilidad Técnica 74
12.3. Sanciones Previstas por Incumplimiento 74
PROCEDIMIENTOS DE EL DEPARTAMENTO DE MODERNIZACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN 75
Atención y Soporte Técnico a Usuarios 75
Creación de Cuenta de Correo electrónico 77
Acceso, Modificación *y* Eliminación de privilegios de acceso 77
Solicitud de informe para Adquisición de Hardware 80
REGLAMENTOS 82
Reglamento para el uso de recursos de tecnologías de la información y las comunicaciones 82
Objetivo 82
Ámbitos de aplicación y competencia 82
Acceso a los servicios 82
Reglamento de uso de los servicios 83
Servicio 1; Computadores, Notebooks, Netbooks, Tablets u otro recurso de cómputo 83
Sobre la asignación 83
Sobre el uso 83
Disposiciones Generales 83
Buenas Prácticas 83
Sobre los Reportes de Fallas. 84
Servicio 2: Internet, Intranet y Correo electrónico 84
Sobre la asignación 84
Sobre la solicitud 84
Sobre el uso 84
Disposiciones Generales 84
Buenas Prácticas; 86
Servicio 3; Otros Sistemas o servicios de Información 87
Sobre la asignación o autorización de acceso 87
Sobre la solicitud 87
Sobre el uso 87
Disposiciones Generales 87
Buenas Prácticas; 87
Sobre la Instalación Temporal para Eventos 87

Sobre los Reportes de Fallas. 87
Servicio 4; Telefonía Celular 88
Sobre la asignación 88
Sobre el uso 88
Disposiciones Generales 88
Sobre los Reportes de Fallas. 88
Servicio 5; Servicio de Telefonía Fija 88
Sobre la asignación de teléfonos 88
Sobre la solicitud 89
Sobre las llamadas de larga distancia y celular 89
Sobre el uso del Teléfono 90
Disposiciones Generales 90
Sobre los Reportes de Fallas telefónicas. 90
ANEXOS 91
Comunicados sobre seguridad de la información 91
1.- Sobre explotar vulnerabilidades o fallos en los Sistemas Informáticos. 91
2.- Sobre probar controles internos en los Sistemas Informáticos. 91
3.- Uso del correo electrónico 91
4.- Sobre la Instalación de Software 91
5.- Uso de medios de almacenamiento masivo (USB, Tarjetas de Memoria, DVD, etc.) 92

INTRODUCCIÓN

En atención al proceso de mejoramiento de los servicios de este municipio, tendiente a avanzar hacia la acreditación de ellos, el enfoque de esta unidad es hacia la gestión de sus procesos *y* orientarnos hacia la visión de la Organización

El aporte de que las Tecnologías de la Información y las comunicaciones es central, todos los macroprocesos de la organización están soportados por sistemas, herramientas y soluciones tecnológicas que contribuyen de manera significativa al logro de los objetivos institucionales.

Dado lo anterior y producto de los cambios, tanto en infraestructura tecnológica, como en la forma en que se entregan los servicios relacionados con tecnología al interior del Municipio, ha sido necesario adecuar las normas que regulan el uso de los r e c u r s o s del servicio de manera de establecer de forma clara las c o n d i c i o n e s y políticas de su uso.

Las tecnologías de la información y las comunicaciones (TIC) contribuyen a optimizar y elevar los niveles de productividad y eficiencia, correspondiéndole a el Departamento de Modernización y Tecnologías de la Información velar porque dichas tecnologías se integren a los procesos y actividades del servicio de manera tal de brindar al usuario el máximo apoyo en cuanto a su gestión y que este tenga a disposición todas las herramientas y facilidades que otorgan las plataformas, haciendo necesario que todos los usuarios conozcan de forma clara y precisa, por un lado las normas que regulan su uso y por otro los procedimientos y mecanismos establecidos para asistencia.

¿Qué es la información?

Según la Real Academia Española: "Es la comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada".

En la actualidad la información es uno de los activos más importantes y preciados, es por esta razón que se invierte a nivel mundial gran cantidad de otros recursos (profesionales, tecnológicos, económicos, etc.) para protegerla, pero ¿es solo la protección de ella la que debe preocuparnos? La respuesta es no, existen otros factores igual de importantes que considerar, como, por ejemplo: la oportunidad, integridad, validez o contabilidad, de lo anterior surge la necesidad entonces de "Asegurar" el conjunto elementos que dan su valor.

¿Qué es la seguridad de la información?

La información es un bien que, como otros, tiene distinto valor para una organización y/o personas, consecuentemente, con ello, necesita ser protegida en forma apropiada. La segundad debe entenderse como un conjunto de conductas, acciones, procedimientos, tecnologías y otros que buscan "asegurar" su buen uso, integridad, confidencialidad, confiabilidad y oportunidad, es por lo anterior que no podemos observar a la seguridad o sistemas como un agente externo o distinto a nosotros ya que somos parte activa de ella, ningún sistema de seguridad será lo suficientemente bueno como para evitar, por ejemplo: que alguno de nosotros al salir a colación o a realizar algún trámite dejemos sobre nuestro escritorio el informe final de un caso, y que este pueda ser sustraído, copiado o adulterado, ningún sistema de control de acceso va a ser efectivo si permanentemente dejamos las puertas de acceso abiertas o colocamos trabas para facilitar nuestro transitar de un lado a otro, ningún sistema de auditoría va a servir si

entregamos nuestras credenciales (nombre de usuario y contraseña).

Recordar también lo indicado en nuestra propia Ley orgánica la que nos impone el "deber de sigilo" o como lo define la Real Academia Española "Secreto que se guarda de una cosa o noticia". La información puede existir de muchas formas, puede ser impresa, escrita, o almacenada o transmitida electrónicamente, mostrada en películas o hablada. Cualquier forma que tome la información, o los dispositivos por los cuales es compartida o almacenada, siempre deberán estar sujetos al mismo cuidado. La seguridad de la información se caracteriza aquí como la preservación de:

a) Confidencialidad: asegurar que la información sea accesible sólo por aquellos usuarios autorizados para tener acceso;
b) Integridad: salvaguardar que la información y los métodos de procesamiento sean exactos y completos;
c) Disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran.

La seguridad de la información se logra mediante la implementación de un adecuado conjunto de controles, los que podrían ser políticas, prácticas, procedimientos, estructuras Organizacionales y funciones. Es por lo anteriormente expuesto que en el siguiente documento se establecen los procedimientos y mecanismos básicos de resguardo de la información de la I. Municipalidad de Loncoche.

LEYES, BASES Y NORMAS TÉCNICAS

- Norma chilena NCh-ISO 27002-2009.
- Ley 17.336 sobre Propiedad Intelectual.
- Ley 19.628 sobre documentos Protección de la Vida Privada.
- Ley 19.799 sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma.
- Ley 19.880 sobre procedimientos administrativos que rigen los actos de los órganos de la administración del estado.
- Ley 19223 Delitos Informáticos.
- Ley 20.285 sobre acceso a la información pública.
- Instructivo Presidencial N° 008 – 2006 sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.
- Instructivo Presidencial N° 005 de Gobierno Electrónico.
- Decreto Supremo 100/2006 - Ministerio Secretaría General de la Presidencia sobre el desarrollo de sitios web de los órganos de la administración del estado.
- Decreto Supremo 93/2006 - Ministerio Secretaría General de la Presidencia sobre la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del estado y de sus funcionarios.
- Decreto Supremo 83/2004 - Ministerio Secretaría General de la Presidencia sobre la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto Supremo 81/2004 - Ministerio secretaria general de la Presidencia sobre interoperabilidad de documentos electrónicos.
- Decreto Supremo 77/2004 - Ministerio Secretaría General de la Presidencia sobre eficiencia de las comunicaciones electrónicas entre órganos de la administración del estado y entre estos y los ciudadanos
- Decreto Supremo 14/2014 - Ministerio secretaria general de la Presidencia sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica.
- Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma
- Manual sobre Procedimiento Administrativo Ley 19.88

Descripción de Funciones

La Sección Informática depende directamente de la Dirección de Administrador Municipal y le corresponde cumplir los objetivos y funciones según la siguiente estructura:

DEPARTAMENTO DE INFORMATICA Y NUEVAS TECNOLOGIAS

ARTÍCULO 16º: El Departamento de informática y nuevas tecnologías tiene por misión la gestión eficiente y eficaz de los recursos tecnológicos, su infraestructura y servicios institucionales, el mejoramiento continuo de los procesos y servicios municipales, y el desarrollo del personal municipal. Para ello considera el diseño de planes y políticas públicas orientadas a la administración, mantención y desarrollo de sistemas de información y servicios informáticos que apoyen la realización de los procesos municipales, así como el seguimiento y acompañamiento a las unidades municipales.

El Departamento de informática y nuevas tecnologías tendrá las siguientes funciones:

a) Analizar, diseñar y desarrollar los sistemas informáticos y supervisar aquellos que son de responsabilidad de contrapartes externas.
b) Administrar y asegurar la disponibilidad de las redes, comunicaciones, servidores y equipos tecnológicos en las distintas unidades municipales, de acuerdo a la disponibilidad de recursos.
c) Prevenir, mantener y corregir el hardware, software, conectividad y telecomunicaciones institucionales de manera oportuna, para así poder brindar un servicio continuo.
d) Estudiar los requerimientos de las diferentes unidades municipales, definiendo y ejecutando el Plan de asignación y renovación del equipamiento tecnológico.
e) Asesorar al Alcalde y al personal municipal en aspectos tecnológicos, gestión de calidad e innovación.
f) Establecer normas y políticas de seguridad institucional de acuerdo a la normativa vigente.
g) Generar y mantener actualizado el manual de Políticas, Seguridad y Procedimientos Informáticos Institucional.
h) Generar proyectos tecnológicos que busquen la mejora de los procesos municipales y los procedimientos administrativos no computacionales.
i) Entregar soporte a la gestión territorial a través de la innovación y mejoramiento continuo de los actuales procedimientos que sustenta el municipio en su conjunto.
j) Asesorar y apoyar la gestión del Comité de Calidad.
k) Coordinar el desarrollo e implementación de la gestión de calidad para resolver y satisfacer las múltiples problemáticas y necesidades que surgen en las unidades municipales en el desarrollo de sus funciones.
l) Definir e implementar acciones para la reingeniería y mejora continua de procesos de las diferentes unidades municipales.
m) Acompañar a las unidades municipales en la mejora de sus procesos, definiendo las metodologías y tecnologías requeridas.
n) Analizar y determinar los indicadores de calidad que permitan medir y trabajar en la mejora continua de los procesos y servicios municipales.
o) Promover y articular el diseño, implementación y evaluación de programas de capacitación, formación y profesionalización destinados al personal municipal, incorporando las mejoras prácticas en materia de gestión de calidad y gobierno digital, aplicadas en forma continua para favorecer las oportunidades de cambio y mejora organizacional.

p) Ejecutar otras funciones que le encomiende el Alcalde o la jefatura de la Dirección.

Organigrama

Las funciones, objetivos y dependencias antes descritos se estructuran en el siguiente organigrama.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

I. Municipalidad de Loncoche

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Organización.

I. Alcance

Debe ser conocida y cumplida por todos los funcionarios de la Municipalidad, cualquiera sea su relación contractual, y sea cual fuere su nivel jerárquico.

II. Términos y Definiciones

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

2.1. Seguridad de la Información

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

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

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:

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.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

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.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

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:

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.

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.

Tecnología de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Organización, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2. 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 Organización.

2.3. 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.

2.4.Incidente de Seguridad

Un incidente de segundad 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.

III. Política de Seguridad de la Información

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Organización.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la Organización y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información de la Organización 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, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales. Mantener la Política de Seguridad de la Organización actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se aplica en todo el ámbito de la Organización, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad

Todos los directores de la organización, tanto se trate de autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Organización, cualquiera sea su situación de contrato, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

El alcalde, es la autoridad que aprueba esta Política (y sus respectivas modificaciones).

El departamento de informática, cumplirá funciones relativas a la seguridad de los sistemas de información de la Organización, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política. Los Propietarios de la Información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El responsable del Área de Recursos Humanos o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continúan en materia de seguridad.

El responsable del Área Informática cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Organización. Por otra parte, 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.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente. La Unidad de Control Interno, es responsable de practicar auditorias periódicas sobre los sistemas y actividades vinculadas con la tecnología de información.

3.1. Aspectos Generales

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

Organización de la Seguridad PARTE IV
Orientado a administrar la seguridad de la información dentro de la Organización y establecer un marco gerencial para controlar su implementación.

Clasificación y Control de Activos PARTE V

Destinado a mantener una adecuada protección de los activos de la Organización.

Seguridad del Personal PARTE VI
Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Organismo o uso inadecuado de instalaciones.

Seguridad Física y Ambiental PARTE Vil
Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la Organización.

Gestión de las Comunicaciones y las Operaciones PARTE VIII
Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

Control de Acceso PARTE IX
Orientado a controlar el acceso lógico a la información.

Mantenimiento de los Sistemas PARTE X
Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información y su respectivo mantenimiento

Administración de la Continuidad de las Actividades de la Organización PARTE XI
Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Cumplimiento PARTEXII
Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, el Organismo identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes, como anexo a la presente Política. Lo expresado anteriormente no implicará necesariamente la asignación de partidas presupuestarias adicionales.

3.2. Sanciones Previstas por Incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

IV Organización de la Seguridad

Generalidades

La presente Política de Segundad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la Organización.
Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades. Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información. Por otro lado, debe tenerse en cuenta que ciertas actividades de la Organización pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

Administrar la seguridad de la información dentro de la Organización y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.
Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Organización.

Alcance

Esta Política se aplica a todos los recursos de la Organización y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

IV Política sobre infraestructura de Seguridad

4.1. Infraestructura de la Seguridad de la Información

4.1.1. Asignación de Responsabilidades en Materia de Seguridad de la Información

El alcalde de la Comuna, asigna las funciones relativas a la Seguridad Informática del Organismo al Depto. de Informática, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la Organización, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

A continuación, se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsable
Seguridad del Personal	Personal
Seguridad Física y Ambiental	Administrador Municipal
Seguridad en las Comunicaciones y las Operaciones	Informática
Control de Accesos lógicos	Informática
Seguridad en el Desarrollo y Mantenimiento de Sistemas	Informática
Planificación de la Continuidad Operativa	Cada Director

4.1.2. Proceso de Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el depto. de informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la Organización.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso está Prohibido

4.1.3. Asesoramiento Especializado en Materia de Seguridad de la Información

El responsable del depto. de informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos, privados o públicos, pudiendo en casos justificados adquirir asesoría vía contratación, de la capacidad a empresas o personas debidamente acreditadas.

4.1.4. Revisión Independiente de la Seguridad de la Información

La Unidad de informática podrá realizar revisiones sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de la Organización reflejan adecuadamente sus disposiciones.

4.2. Seguridad Frente al Acceso por Parte de Terceros

4.2.1. Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la Organización, el depto. de informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.

La incidencia de este acceso en la seguridad de la información de la Organización. En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Organización, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar. Se cita a modo de ejemplo:

a) Personal de mantenimiento y soporte de hardware y software.

b) Limpieza, guardia de seguridad y otros servicios de soporte tercerizados.

c) Pasantías y otras designaciones de corto plazo.

d) Consultores.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados que definan las condiciones para la conexión o el acceso.

4.2.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de seguridad de la información de la Organización.

b) Protección de los activos de la Organización, incluyendo:

   - Procedimientos para proteger los bienes de la Organización, abarcando los activos físicos, la información y el software.
   - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
   - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
   - Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.

g) Existencia de Derechos de Propiedad Intelectual.

h) Definiciones relacionadas con la protección de datos.

i) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

n) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

o) Proceso claro y detallado de administración de cambios.

p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

r) Controles que garanticen la protección contra software malicioso.

s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

t) Relación entre proveedores y subcontratistas.

Todo contrato debe incluir las siguientes clausulas:

- Al término de contrato el proveedor deberá entregar un certificado donde acredite que todos los datos sensibles para la organización hayan sido removidos en forma segura, este certificado deberá ser firmado por el representante legal de la empresa proveedora del servicio. El proveedor no podrá hacer uso o divulgación de ningún tipo de información utilizada o generada en la puesta en marcha, ejecución o cierre del proyecto o servicio. (en concordancia con Nch-ISO 27.002 sección 6.2.3, letra b))

- Ante una modificación de aplicación o rutina de proceso se deberá llevar un control de cambio donde se identifique al menos la siguiente información:

1.- Tipo de Fuente de cambio según los 4 tipos de fuentes fundamentales de la Gestión del Cambio (Nuevas condiciones en el negocio, Nuevas necesidades del cliente, Reorganización o crecimiento del negocio y Restricciones presupuestales)
2.- Identificación del cambio a realizar (modulo impactado, cambio realizado)
3.- identificación del impacto generado por el cambio
4.- Control de Versión, donde refleje el cambio realizado.

(en concordancia con Nch-ISO 27.002 sección 6.2.3, letra h))

- El proveedor deberá declarar una lista de personas autorizadas para utilizar los servicios, estos usuarios no podrán realizar cambios no autorizados expresamente por la Jefatura de la Unidad TI, por lo que en una primera instancia solo tendrán privilegio de invitado para el uso del software o el hardware involucrados (en concordancia con Nch-ISO 27.002 sección 6.2.3, letra i))

- El proveedor deberá informar al Inspector de Contrato Técnico y/o a la Jefatura de la Unidad TI de cualquier incidente de seguridad detectada. Estos informes de incidentes deberán contener como mínimo los siguientes datos: Nombre de persona que realiza el reporte de incidente, servicio afectado por el incidente, Fecha y hora del incidente, prioridad de incidente, breve descripción del incidente, tiempo estimado de recuperación de servicio. (en concordancia con Nch-ISO 27.002 sección 6.2.3, letra j))

- El proveedor deberá mantener en un estándar de funcionamiento los servicios que permita la continuidad fluida del mismo, asegurando la confiabilidad, disponibilidad y confidencialidad de la información, se determinará como nivel inaceptable de servicio cuando este influya en el normal funcionamiento y tenga una interrupción del mismo.
  El nivel de servicio estará sancionado de acuerdo a las bases administrativas en el apartado de multas (en concordancia con Nch-ISO 27.002 sección 6.2.3, letra l))

- La municipalidad tendrá el derecho discrecional a realizar auditorías del funcionamiento y operatividad de los servicios contratados, a través de personal propio, personal de la contraloría general o un tercero que debe ser debidamente individualizado y aprobado por decreto alcaldicio. Esta auditoría será informada por oficio al prestador de servicio con un plazo no superior a 5 días hábiles antes del comienzo de dicha auditoría.
  Los auditores tendrán derecho de acceso a los elementos auditados con perfil de auditor y podrán, si así lo estiman, en un ambiente controlado replicar las condiciones de explotación del servicio auditado.
  Los auditores tendrán derecho a realizar observaciones y/o recomendaciones fundadas de acuerdo a los resultados obtenidos en la auditoría, las que serán comunicadas al proveedor con el fin de realizar las mejoras en el servicio prestado.

  Los auditores No podrán realizar modificaciones de ningún tipo en la fuente de datos o en los códigos que tengan acceso
  Los auditores No podrán revelar a terceros información que se generen como resultado de la auditoría. Sin perjuicio de lo exigido por la ley de transparencia (en concordancia con Nch-ISO 27.002 sección 6.2.3, letra o))

- El término de relación contractual anticipada debe ser notificado y consensuado por ambas partes de tal forma que permita a la Ilustre Municipalidad de Loncoche garantizar la continuidad de servicio y realizar la contratación directa o nueva licitación según corresponda. Se considera como plazo mínimo de tres meses para la notificación de dicho evento con el fin de asegurar los intereses de la Ilustre Municipalidad de Loncoche (en concordancia con Nch-ISO 27.002 sección 6.2.3, letra v))

4.3. Tercerización / Externalización / Outsourcing

4.3.1. Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC de la Organización, contemplarán además de los puntos especificados en "Requerimientos de Seguridad en Contratos o Acuerdos con Terceros", los siguientes aspectos:

a) Forma en que se cumplirán los requisitos legales aplicables.

b) Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.

c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de la Organización.

d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la Organización.

e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.

f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.

g) Derecho a la auditoría por parte de la Organización sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc. Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

V Clasificación y Control de Activos

Generalidades

El Organismo debe tener un acabado conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

Recursos de 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, etc.

Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.

Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información. Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

- ✓ Garantizar que los activos de información reciban un apropiado nivel de protección.
- ✓ Clasificar la información para señalar su sensibilidad y criticidad.
- ✓ Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

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

Responsabilidad

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El depto. de informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplido de acuerdo a lo establecido en la presente Política.

Política de Inventario de Activos

5.1. Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 12 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es la unidad de Inventario de la municipalidad.

5.2. Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

Confidencialidad:

0 PUBLICO: Información que puede ser conocida *y* utilizada sin autorización por cualquier persona, sea empleado de la Organización o no.

1 RESERVADA - USO INTERNO: Información que puede ser conocida *y* utilizada por todos los empleados de la Organización *y* algunas entidades externas debidamente autorizadas, *y* cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo, o terceros.

2 RESERVADA- CONFIDENCIAL: Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo o a terceros.

3 RESERVADA SECRETA: Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Organización, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público o a terceros.

Integridad:

0 Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la Organización.
1 Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el Organismo o terceros.
2 Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.
3 Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Organismo, al Sector Público Nacional o a terceros.

Disponibilidad:

0 Información cuya inaccesibilidad no afecta la operatoria de la Organización.
1 Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.
2 Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas al Organismo o a terceros.
3 Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas al Organismo o a terceros.

Al referirse a pérdidas, se contemplan aquellas medibles (materiales) y no medibles (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

CRITICIDAD BAJA: ninguno de los valores asignados supera el 1.

CRITICIDAD MEDIA: alguno de los valores asignados es 2

CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) *y* los perfiles funcionales que deberán tener acceso a la misma.

En adelante se mencionará como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

5.3. Rotulado de la Información

Se definirán procedimientos para el rotulado *y* manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia
- Almacenamiento;
- Transmisión por correo, fax, correo electrónico;
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.)

VI Seguridad del Personal

Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes. En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos tomando acciones preventivas. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo

- ✓ Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.
- ✓ Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de segundad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Organización en el transcurso de sus tareas normales.
- ✓ Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
- ✓ Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Alcance

Esta Política se aplica a todo el personal de la Organización, cualquiera sea su situación de contrato, y al personal externo que efectúe tareas dentro del ámbito de la Organización.

Responsabilidad

El responsable del Área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El depto. de informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados.

El responsable del Área Legal participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal de la Organización es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

Política sobre la Seguridad de la Información y el Personal

6.1. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos

6.1.1. Incorporación de la Seguridad en los Puestos de Trabajo

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de segundad determinadas.

6.1.2. Control y Política del Personal

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que, a tal efecto, alcanzan al Organismo

6.1.3. Compromiso de Confidencialidad

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Organización. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente. Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

a) Suscripción inicial del Compromiso por parte de la totalidad del personal.

b) Revisión del contenido del Compromiso cada año.

c) Método de aprobación en caso de modificación del texto del Compromiso.

6.1.4. Términos y Condiciones de Empleo

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la Organización y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

6.2. Capacitación del Usuario

6.2.1. Formación y Capacitación en Materia de Seguridad de la Información

Todos los empleados de la Organización y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el organismo, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la Organización. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada año se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de producir el material de capacitación

Áreas Responsables del Material de Capacitación; Dirección de Personal

El personal que ingrese al Organismo recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

6.3. Respuesta a Incidentes *y* Anomalías en Materia de Seguridad

6.3.1. Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales gerenciales apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación *y* de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el depto. de informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación *y* resolución del incidente, *y se* encargará de su monitoreo.

Todos los empleados *y* contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, *y* deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

6.3.2. Comunicación de Debilidades en Materia de Seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

6.3.3. Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
c) Alertar inmediatamente al Responsable de Seguridad Informática o del Activo de que se trate.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

6.3.4. Aprendiendo de los Incidentes

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

6.3.5. Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias y reglamentarias que rigen al personal de la Administración Pública, para los empleados que violen la Política, Normas y Procedimientos de Seguridad de la Organización (Ver 12. Cumplimiento).

VII Seguridad Física y Ambiental

Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias *a* la información y a las operaciones de la Organización. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la Organización, 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 de las instalaciones de la Organización como en instalaciones próximas a la sede del mismo que pueda 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 de la Organizador

Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al Organismo, pero situado físicamente fuera del mismo ("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 utilizados. 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.

Objetivo

- ✓ Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones información de la Organización.

- ✓ Proteger el equipamiento de procesamiento de información crítica de la Organización ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad, controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslade permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

- ✓ Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento equipamiento informático que alberga la información de la Organización.

- ✓ Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

- ✓ Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la Organización: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

Responsabilidad

El depto. de informática definirá junto con los Propietarios de Información, según corresponda, las medidas de seguridad física *y* ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, *y* controlará su implementación.

Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física *y* ambiental indicadas en el presente Capítulo.

Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la Organización.

Los responsables de Unidades Organizativas definirán los niveles de acceso físico del personal de la Organización a las a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados de la Organización cuando lo crean conveniente.

Todo el personal de la Organización es responsable del cumplimiento de la política de pantallas *y* escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

Política sobre seguridad Física.

7.1. Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, *y* cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el depto. de informática, de acuerdo a la evaluación de riesgos efectuada.

a) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

b) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio, como credenciales, hoja de registro de visitas u otras que evidencien el acceso físico a las dependencias. El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

c) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, por incendio, humedad e inundación.

7.2. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el depto. de informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos: "Registro de Acceso a Sala de Servidores". Se mantendrá un registro protegido para permitir auditar todos los accesos.

c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

d) Revisar y actualizar cada 6 Meses los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el responsable de la Unidad Organizativa de la que dependa.

e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

7.3. Protección de Oficinas, Recintos e Instalaciones

Para la selección *y* el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, *y* otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones *y* normas (estándares) en materia de sanidad *y* segundad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios *y* zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas de la Organización **Áreas Protegidas**

- Oficinas del Departamento de informática.
- Sala de equipos edificio consistorial

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos *y* ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

c) Ubicar las funciones *y* el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

d) Establecer que las puertas *y* ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.

e) Implementar los siguientes mecanismos de control para la detección de intrusos: Alarmas *y* sistemas de detección de movimiento. Los mismos serán instalados según estándares profesionales *y* probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.

f) Separar las instalaciones de procesamiento de información administradas por el Organismo de aquellas administradas por terceros.

g) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.

h) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas de la Organización. Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.

i) Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

7.4. Ubicación y Protección del Equipamiento y Copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.

b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.

c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:

Amenazas Potenciales

- Robo o hurto
- Incendio
- Explosivos
- Humo
- Inundaciones o filtraciones de agua (o falta de suministro)
- Polvo
- Vibraciones
- Efectos químicos
- Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)
- Radiación electromagnética Derrumbes

e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada: 12 meses.

f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede de la Organización.

7.5. Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b) Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la Organización. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el depto. de informática conjuntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

7.6. Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes en Chile.

b) Utilizar ducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la siguiente protección alternativa: Canalización DLP Sobrepuesta - Legrand

c) Proteger el cableado de red contra intercepción no autorizada o daño mediante los siguientes controles:

- Evitando la instalación en espacios de acceso al público.
- Revisando las instalaciones de datos y eléctrica en los edificios de la organización.

d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias. Tal y como se señala en el reglamento VDI generado en el Departamento de Modernización y Tecnologías de la Información.

e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados o Subterráneos.

Para los sistemas sensibles o críticos, se implementarán los siguientes controles adicionales:

a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.

b) Utilizar rutas o medios de transmisión alternativos.

7.7. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del jefe del depto. de informatica. El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

d) Registrar el retiro de equipamiento de la sede de la Organización para su mantenimiento.

e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

7.8. Seguridad de los Equipos Fuera de las Instalaciones.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Organización, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma.

La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Organización para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de la Organización, cuando sea conveniente.

7.9. Desafectación o Reutilización Segura de los Equipos.

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo, discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda, se deberá llevar un registro exclusivo de estos dispositivos y las acciones ejercida sobre ellos en forma de una hoja de vida.

7.10. Políticas de Escritorios y Pantallas Limpias.

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo. Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

b) Guardar bajo llave la información sensible o crítica de la Organización (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.

c) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

d) Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.

e) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

7.11. Retiro de los Bienes

El equipamiento, la información *y* el software no serán retirados de la sede de la Organización sin autorización formal del jefe del Departamento de Informatica o quien el designe para este efecto. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la Organización, las que serán llevadas a cabo por un funcionario designado por el depto. de informatica. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

Política sobre la operación y las comunicaciones

8.1. Procedimientos y Responsabilidades Operativas

8.1.1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Jefe del depto. de informática. Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) Procesamiento y manejo de la información.

b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.

c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.

d) Restricciones en el uso de utilitarios del sistema.

e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.

f) Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.

8.1.2. Control de Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo *y* de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos *y* de seguridad. El depto. de informática controlará que los cambios en los componentes operativos *y* de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El depto. de informática evaluará el posible impacto operativo de los cambios previstos *y* verificará su correcta implementación. Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado. Los procedimientos de control de cambios contemplarán los siguientes puntos:

a) Identificación *y* registro de cambios significativos.
b) Evaluación del posible impacto de dichos cambios.
c) Aprobación formal de los cambios propuestos.
d) Planificación del proceso de cambio.
e) Prueba del nuevo escenario.
f) Comunicación de detalles de cambios a todas las personas pertinentes.
g) Identificación de las responsabilidades por la cancelación de los cambios fallidos *y* la recuperación respecto de los mismos.

8.1.3. Procedimientos de Manejo de Incidentes

Se establecerán funciones *y* procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz *y* sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

a) Contemplar *y* definir todos los tipos probables de incidentes relativos a seguridad, incluyendo

1. Fallas operativas
2. Código malicioso
3. Intrusiones
4. Fraude informático
5. Error humano

6. Catástrofes naturales

b) Comunicar los incidentes a través de canales gerenciales apropiados tan pronto como sea posible.

c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):

1. Definición de las primeras medidas a implementar
2. Análisis e identificación de la causa del incidente.
3. Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
4. Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
5. Notificación de la acción a la autoridad y/u Organismos pertinentes.

d) Registrar pistas de auditoría y evidencia similar para:

1. Análisis de problemas internos.
2. Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial (Ver 12.1. Cumplimiento de Requisitos Legales).
3. Negociación de compensaciones por parte de los proveedores de software y de servicios.

e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:

1. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
2. Documentación de todas las acciones de emergencia emprendidas en forma detallada.
3. Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
4. Constatación de la integridad de los controles y sistemas de la Organización en un plazo mínimo. En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Legal de la Organización en el tratamiento de incidentes de seguridad ocurridos.

8.1.4. Separación de Funciones

Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas. Si este método de control no se pudiera cumplir en algún caso, se implementarán controles como:

a) Monitoreo de las actividades.
b) Registros de auditoría y control periódico de los mismos.
c) Supervisión por parte de la Unidad de Auditoría Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.

Asimismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones. Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

a) Separar actividades que requieren connivencia para defraudar, por ejemplo, efectuar una orden de compra y verificar que la mercadería fue recibida.
b) Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

8.1.5. Gestión de Instalaciones Externas

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes cuestiones específicas.

a) Identificar las aplicaciones sensibles o críticas que convenga retener en el Organismo.
b) Obtener la aprobación de los propietarios de aplicaciones específicas.
c) Identificar las implicancias para la continuidad de los planes de las actividades del Organismo.
d) Especificar las normas de seguridad y el proceso de medición del cumplimiento.
e) Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad.
f) Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deberán ser acordadas entre el Jefe del depto. de informática y el Responsable del Área Legal del Organismo.

8.2. Planificación y Aprobación de Sistemas

8.2.1. Planificación de la Capacidad

El Depto. de informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la Organización para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

8.2.2. Aprobación del Sistema

El depto. de informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

a) Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
b) Garantizar la recuperación ante errores.
c) Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
d) Garantizar la implementación de un conjunto acordado de controles de seguridad.
e) Confeccionar disposiciones relativas a la continuidad de las actividades de la Organización.
f) Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
g) Considerar el efecto que tiene el nuevo sistema en la seguridad global de la Organización,
h) Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

8.3. Protección Contra Software Malicioso

8.3.1. Controles Contra Software Malicioso

El depto. de informática definirá controles de detección y prevención para la protección contra software malicioso. El depto. de informática, o el personal designado por éste, implementarán dichos controles.

El depto. de informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por el Organismo
b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Organización, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
h) Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

8.4. Mantenimiento

8.4.1. Resguardo de la Información

El depto. de informática *y* los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá *y* documentará un esquema de resguardo de la información.

El depto. de informática dispondrá *y* controlará la realización de dichas copias, así como la prueba periódica de su restauración en caso de que se requiera. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información *y* del software crítico del Organismo.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

a) 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.
b) 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 a lo indicado por el proveedor, *y* asegurando la destrucción de los medios desechados.
c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos *y* completos de las mismas *y* los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información *y* el software esenciales para el Organismo. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad (Ver 5.2. Clasificación de la información) *y* requisitos legales a los que se encuentre sujeta.
d) Asignar a la información de resguardo un nivel de protección física *y* ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.

8.4.2. Registro de Actividades del Personal Operativo

El depto. de informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Tiempos de inicio *y* cierre del sistema.
b) Errores del sistema *y* medidas correctivas tomadas.
c) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
d) Ejecución de operaciones críticas
e) Cambios a información crítica

8.4.3. Registro de Fallas

El depto. de informática verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
b) Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, *y* que las medidas tomadas fueron autorizadas.
c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

8.5. Administración de la Red

8.5.1. Controles de Redes

El depto. de informática definirá controles para garantizar la seguridad de los datos *y* los servicios conectados en las redes de la Organización, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto.

b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información. El depto. de informática implementará dichos controles.

8.6. Administración y Seguridad de los Medios de Almacenamiento

8.6.1. Administración de Medios Informáticos Removibles

El depto. de informática implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.

b) Requerir autorización para retirar cualquier medio de la Organización y realizar un control de todos los retiros a fin de mantener un registro de auditoría.

c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores. Se documentarán todos los procedimientos y niveles de autorización, en concordancia con el capítulo 5. Clasificación y Control de Activos.

8.6.2. Eliminación de Medios de Información

El depto. de informática definirán procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.
b) Voces u otras grabaciones.
c) Papel carbónico.
d) Informes de salida.
e) Cintas de impresora de un solo uso.
f) Cintas magnéticas.
g) Discos o cáseles removibles.
h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
i) Listados de programas.
j) Datos de prueba.
k) Documentación del sistema.

Asimismo, se debe considerar que podría ser más eficiente disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.

8.6.3. Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a la clasificación establecida en el capítulo 5 - "Clasificación y Control de Activos". En los procedimientos se contemplarán las siguientes acciones:

a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
b) Restringir el acceso solo al personal debidamente autorizado
c) Mantener un registro formal de los receptores autorizados de datos
d) Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.
e) Proteger los datos en espera ("colas").
f) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

8.6.4. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:

a) Almacenar la documentación del sistema en forma segura.
b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

8.7. Intercambios de Información y Software

8.7.1. Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre Organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la Organización involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
b) Procedimientos de notificación de emisión, transmisión, envío y recepción.
c) Normas técnicas para el empaquetado y la transmisión.
d) Pautas para la identificación del prestador del servicio de correo.
e) Responsabilidades y obligaciones en caso de pérdida de datos.
f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
g) Términos y condiciones de la licencia bajo la cual se suministra el software.
h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
i) Normas técnicas para la grabación y lectura de la información y del software.
j) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

8.7.2. Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar:

a) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
    1. Uso de recipientes cerrados.
    2. Entrega en mano.
    3. Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
    4. En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

8.7.3. Seguridad del Gobierno Electrónico

El depto. de informática verificará que los procedimientos de aprobación de Software del punto "Aprobación del Sistema" incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

a) **Autenticación:** Nivel de confianza recíproca suficiente sobre la identidad del usuario y el Organismo.
b) **Autorización:** Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica.
c) **Procesos de oferta y contratación pública:** Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.
d) **Trámites en línea:** Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.

e) **Verificación:** Grado de verificación apropiado para constatar la información suministrada por los usuarios.
f) **Cierre de la transacción:** Forma de interacción más adecuada para evitar fraudes.
g) **Protección a la duplicación:** Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
h) **No repudio:** Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.
i) **Responsabilidad:** Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

Las consideraciones mencionadas se implementarán mediante la aplicación de las técnicas criptográficas enumeradas en el punto "Política de Utilización de Controles Criptográficos." y tomando en cuenta el cumplimiento de los requisitos legales emanados de toda la normativa vigente.

8.7.4. Seguridad del Correo Electrónico

8.7.4.1. Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
c) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
d) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
e) El impacto de un cambio en el medio de comunicación en los procesos de la Organización.
f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
g) Las implicancias de la publicación externa de listados de personal, accesibles al público,
h) El acceso de usuarios remotos a las cuentas de correo electrónico,
i) El uso inadecuado por parte del personal.

8.7.4.2. Política de Correo Electrónico

El depto. de informática definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.
b) Protección de archivos adjuntos de correo electrónico.
c) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos.
d) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
e) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
f) Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
g) Definición de los alcances del uso del correo electrónico por parte del personal del Organismo.
h) Potestad de la Organización para auditar los mensajes recibidos o emitidos por los servidores de la Organización, lo cual se incluirá en el "Compromiso de Confidencialidad"

Estos dos últimos puntos deben ser leídos a la luz de las normas vigentes que no sólo prohíben a los empleados a hacer uso indebido o con fines particulares del patrimonio estatal, sino que también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento.

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el Organismo debe informar claramente a sus empleados:

a. cuál es el uso que el organismo espera que los empleados hagan del correo electrónico provisto por el organismo; y
b. bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

8.7.5. Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc. Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias de la Organización, incluyendo:

a) Vulnerabilidades de la información en los sistemas de oficina, por ejemplo, la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.
b) Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo, el uso de boletines electrónicos institucionales.
c) Exclusión de categorías de información sensible de la Organización, si el sistema no brinda un adecuado nivel de protección.
d) Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo, aquellas que trabaja en proyectos sensibles.
e) La aptitud del sistema para dar soporte a las aplicaciones de la Organización, como la comunicación de órdenes o autorizaciones.
f) Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.
g) Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.
h) Identificación de la posición o categoría de los usuarios, por ejemplo, empleados del Organismo o contratistas, en directorios accesibles por otros usuarios.
i) Retención y resguardo de la información almacenada en el sistema.
j) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

8.7.6. Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación de la Organización que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo, la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica.

Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación. Todos los sistemas de acceso público deberán prever que:

a) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales.
b) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
c) La información sensible sea protegida durante el proceso de recolección y su almacenamiento.

d) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.
e) Se registre al responsable de la publicación de información en sistemas de acceso público.
f) La información se publique teniendo en cuenta las normas establecidas al respecto.
g) Se garantice la validez y vigencia de la información publicada.

1. Control de Accesos

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 concientizar a los mismos 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.

Objetivo

- ✓ Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- ✓ Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- ✓ Controlar la seguridad en la conexión entre la red de la Organización y otras redes públicas o privadas.
- ✓ Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas. Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- ✓ Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la Organización, cualquiera sea la función que desempeñe.

Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad

El depto. de informática estará a cargo de:

Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la

activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.

- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo. Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
    - determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
    - definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.

- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
- Definir un cronograma de depuración de registros de auditoría en línea.

Los Responsable de las Unidades Organizativas, junto con el jefe del depto. de informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo, autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El depto. de informática cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de "enrutadores" o "gateways" adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.

- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

Política sobre el Control de Acceso

9.1. Requerimientos para el Control de Acceso

9.1.1. Política de Control de Accesos

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificar toda la información relacionada con las aplicaciones.
c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes.
d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

9.1.2. Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

a) Indicar expresamente si las reglas son obligatorias u optativas
b) Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".
c) Controlar los cambios en los rótulos de información que son iniciados automáticamente
d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
e) Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

9.2. 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.

9.2.1. Registro de Usuarios

El depto. de 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 multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando 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.
b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la Organización, por ejemplo,

que no compromete la separación de tareas.

d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Organismo o sufrieron la pérdida/robo de sus credenciales de acceso.
i) Efectuar revisiones periódicas con el objeto de:

- cancelar identificadores y cuentas de usuario redundantes
- inhabilitar cuentas inactivas por más de 30 días
- eliminar cuentas inactivas por más de 60 días

En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

9.2.2. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo, el requerimiento mínimo para su rol funcional.
c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el depto. de informática.

9.2.3. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad (Ver 6.1.3. Compromiso de Confidencialidad)
b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.

d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
e) Configurar los sistemas de tal manera que:

- las contraseñas tengan al menos 8 caracteres, debiendo contener símbolos y alfanuméricos
- suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda),
- la contraseña caducara cada 30 días, y el usarlo deberá realizar su cambio.
- impedir que las últimas 10 contraseñas sean reutilizadas,

9.3. Responsabilidades del Usuario

9.3.1. Uso de Contraseñas

Los usuarios deben 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.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Realizar el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el depto. de informática:

1. Sean fáciles de recordar.
2. 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.
3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").
f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

9.4. Control de Acceso a la Red

9.4.1. Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, por lo tanto, 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 depto. de informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal según el procedimiento declarado respecto de personal de su incumbencia. Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que

están fuera de la administración y del control de seguridad de la Organización.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.
b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

9.4.2. Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la Organización. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El depto. de informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso. La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:

    - Asignación de la herramienta de autenticación.
    - Registro de los poseedores de autenticadores.
    - Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
    - Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.

b) Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:

    - Establecimiento de las reglas con el usuario.
    - Establecimiento de un ciclo de vida de las reglas para su renovación.

c) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos *y* controles de re-llamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información de la Organización. Al aplicar este tipo de control, el Organismo no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no será posible aplicar el control de re-llamada. Asimismo, es importante que el proceso de re-llamada garantice que se produzca a su término, una desconexión real del lado de la Organización.

9.4.3. Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Organización. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad de la Organización. En el punto anterior se mencionan algunos ejemplos de autenticación *y* de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro *y* compartido.

9.4.4. Protección de los Puertos (Ports) de Diagnóstico Remoto

Muchas computadoras *y* sistemas de comunicación son instalados *y* administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto "Autenticación de Usuarios para Conexiones Externas". También para este caso deberá tenerse en cuenta el punto "Camino Forzado".

9.4.5. Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán *y* documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios. La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos *y* los requerimientos de acceso (Ver 9.1. Requerimientos para el Control de Acceso), el depto. de informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados, para subdividir la red. Luego decidirá, junto con el depto. de informática, el esquema más apropiado a implementar.

9.4.6. Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El depto. de informática definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el jefe del depto. de informática y la jefatura directa del solicitante. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares.

9.4.7. Control de Conexión a la Red

Se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios de la red. Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a) Correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a la red fuera del horario laboral.

9.4.8. Control de Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del Organismo, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otra autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

9.4.9. Seguridad de los Servicios de Red

El depto. de informática definirá las pautas para garantizar la seguridad de los servicios de red de la Organización, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de segundad. Dicha configuración será revisada periódicamente por el depto. de informática.

9.5. Control de Acceso al Sistema Operativo

9.5.1. Identificación Automática de Terminales

El depto. de informática realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

a) El método de identificación automática de terminales utilizado.
b) El detalle de transacciones permitidas por terminal.

9.5.2. Procedimientos de Conexión de Terminales

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 deberá:

a) Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.
b) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.
c) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
d) 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.
e) Limitar el número de intentos de conexión no exitosos permitidos y:

    - Registrar los intentos no exitosos.
    - Impedir otros intentos de identificación, una vez superado el límite permitido. Desconectar conexiones de comunicaciones de datos.

f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
g) 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.

9.5.3. Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para el Organismo, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

9.5.4. Sistema de Administración de Contraseñas

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:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.
b) 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.
c) Imponer una selección de contraseñas de calidad
d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas.
e) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
f) Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
g) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
h) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional,
j) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo, claves de impresoras, hubs, routers, etc.).
k) 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.

9.5.5. Uso de Utilitarios de Sistema

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a) Utilizar procedimientos de autenticación para utilitarios del sistema.
b) Separar entre utilitarios del sistema y software de aplicaciones.
c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
d) Evitar que personas ajenas al Organismo tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
e) Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
f) Limitar la disponibilidad de utilitarios de sistema, por ejemplo, durante el transcurso de un cambio autorizado.
g) Registrar todo uso de utilitarios del sistema.
h) Definir y documentar los niveles de autorización para utilitarios del sistema.
i) Remover todo el software basado en utilitarios y software de sistema innecesarios.

9.5.6. Desconexión de Terminales por Tiempo Muerto

El depto. de informática, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo, áreas públicas o externas fuera del alcance de la gestión de seguridad de la Organización, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal. Para las PC's, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

9.5.7. Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo, áreas públicas o externas que estén fuera del alcance de la gestión de seguridad del Organismo. Entre los controles que se deben aplicar, se enuncian:

a) Utilizar lapsos predeterminados, por ejemplo, para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.
b) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
c) Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

9.6. Control de Acceso a las Aplicaciones

9.6.1. Restricción del Acceso a la Información

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 Organización para el acceso a la información. Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) 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. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.
b) 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.
c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
d) 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.
e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

9.6.2. Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

a) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación.
b) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.
c) Coordinar con el depto. de informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.
d) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

9.7. Monitoreo del Acceso y Uso de los Sistemas

9.7.1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:

a) Identificación del usuario.
b) Fecha y hora de inicio y terminación.
c) Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma.
d) Registros de intentos exitosos y fallidos de acceso al sistema.
e) 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.

9.7.2. Monitoreo del Uso de los Sistemas

9.7.2.1. Procedimientos y Áreas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente. Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.

El alcance de estos procedimientos deberá corresponderse a la evaluación de riesgos que realice el depto. de informática.

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

a) Acceso no autorizado, incluyendo detalles como:

1. Identificación del usuario.
2. Fecha y hora de eventos clave.
3. Tipos de eventos.
4. Archivos a los que se accede.
5. Utilitarios y programas utilizados.

b) Todas las operaciones con privilegio, como:

1. Utilización de cuenta de supervisor.
2. Inicio y cierre del sistema.
3. Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.
4. Cambio de fecha/hora.
5. Cambios en la configuración de la seguridad.
6. Alta de servicios.

c) Intentos de acceso no autorizado, como:

1. Intentos fallidos.
2. Violaciones de la Política de Accesos y notificaciones para "gateways" de red y "firewalls".
3. Alertas de sistemas de detección de intrusiones.

d) Alertas o fallas de sistema como:

1. Alertas o mensajes de consola.
2. Excepciones del sistema de registro.
3. Alarmas del sistema de administración de redes.
4. Accesos remotos a los sistemas.

9.7.2.2. Factores de Riesgo

Entre los factores de riesgo que se deben considerar se encuentran:

a) La criticidad de los procesos de aplicaciones.
b) El valor, la sensibilidad o criticidad de la información involucrada.
c) La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
d) El alcance de la interconexión del sistema (en particular las redes públicas).

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

9.7.2.3 Registro y revisión de Eventos

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 depto. de informática, de acuerdo a la evaluación de riesgos efectuada. Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.

Por otra parte, el depto. de informática, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los registros. En la asignación de funciones en materia de seguridad de la información, se deberá separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de

garantizar que no ocurra:

a) La desactivación de la herramienta de registro.
b) La alteración de mensajes registrados.
c) La edición o supresión de archivos de registro.
d) La saturación de un medio de soporte de archivos de registro.
e) La falla en los registros de los eventos.
f) La sobre escritura de los registros.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control *y* efectuar recomendaciones sobre modificaciones a los aspectos de seguridad. Adicionalmente podrían evaluar las herramientas de registro, pero no tendrán libre acceso a ellas.

9.8. Computación Móvil *y* Trabajo Remoto

9.8.1. Computación Móvil

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la Organización. Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil *y/o* removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares *y* sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Tapes, *y* cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc. Esta lista no es taxativa, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial de la Organización y por lo tanto, ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo. Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria
b) El acceso seguro a los dispositivos
c) La utilización de los dispositivos en lugares públicos.
d) El acceso a los sistemas de información y servicios de la Organización a través de dichos dispositivos.
e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
f) Los mecanismos de resguardo de la información contenida en los dispositivos.
g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia, deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

a) Permanecer siempre cerca del dispositivo.
b) No dejar desatendidos los equipos.
c) No llamar la atención acerca de portar un equipo valioso.
d) No poner identificaciones de la Organización en el dispositivo, salvo los estrictamente necesarios.
e) No poner datos de contacto técnico en el dispositivo.
f) Mantener cifrada la información clasificada.

Por otra parte, 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 de la Organización, los que incluirán:

a) Revocación de las credenciales afectadas
b) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

9.8.2. Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al Organismo.

El trabajo remoto sólo será autorizado por el responsable de la Unidad Organizativa, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios de la Organización, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
b) El ambiente de trabajo remoto propuesto.

Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la Organización, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.

a) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
b) Evitar la instalación / desinstalación de software no autorizada por el Organismo. Los controles y disposiciones comprenden:
c) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.
d) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
e) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
f) Incluir seguridad física.
g) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
h) Proveer el hardware y el soporte y mantenimiento del software.
i) Definir los procedimientos de backup y de continuidad de las operaciones,
j) Efectuar auditoría y monitoreo de la seguridad.

k) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.
l) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

10. Desarrollo y mantenimiento de sistemas

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 a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán 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.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los sistemas y en la infraestructura de base en la cual se apoyan. Definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tantos desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

Responsabilidad

El depto. de informática junto con el Propietario de la Información, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos. El depto. de informática, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos.

Asimismo, el depto. de informática 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; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

Política de Seguridad de los Sistemas

10.1. Requerimientos de Seguridad de los Sistemas

10.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen. Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo. Se deben tener en cuenta las siguientes consideraciones:

a) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.
b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

10.2. Seguridad en los Sistemas de Aplicación

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

a) La validación de datos de entrada.
b) El procesamiento interno.
c) La autenticación de mensajes (interfaces entre sistemas)
d) La validación de datos de salida.

10.2.1. Validación de Datos de Entrada

Se definirá un procedimiento que, durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros. Este procedimiento considerará los siguientes controles:

a) Control de secuencia.
b) Control de monto límite por operación y tipo de usuario.
c) Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.
d) Control de paridad.
e) Control contra valores cargados en las tablas de datos.
f) Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

a) Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.
b) Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.
c) Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

10.2.2. Controles de Procesamiento Interno

Se definirá un procedimiento para que, durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores. Para ello se implementarán:

a) Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
b) Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
c) Procedimientos que establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.
d) Procedimientos que realicen la validación de los datos generados por el sistema.
e) Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
f) Procedimientos que controlen la integridad de registros y archivos.
g) Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
h) Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

10.2.3. Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto "Controles Criptográficos".

10.2.4. Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

a) Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.
b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
c) Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
d) Procedimientos para responder a las pruebas de validación de salidas.
e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

10.3. Seguridad de los Archivos del Sistema

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

10.3.1. Control del Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único responsable designado formalmente por el depto. de informática.

Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida. Otros controles a realizar son:

    a) Guardar sólo los ejecutables en el ambiente de producción.
    b) Llevar un registro de auditoría de las actualizaciones realizadas.
    c) Retener las versiones previas del sistema, como medida de contingencia.
    d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
    e) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
    f) Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

10.3.2. Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

a) Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
b) Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
c) Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

10.3.3. Control de Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El depto. de informática definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

a) Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
b) El Propietario de la Información afectada y el depto. de informática aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
c) Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
d) Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales.
e) Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho

registro será revisado posteriormente por el depto. de informática.

10.4. Seguridad de los Procesos de Desarrollo y Soporte

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto, se controlarán los entornos y el soporte dado a los mismos.

10.4.1. Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de segundad y control, respetando la división de funciones. Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

a) Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
b) Mantener un registro de los niveles de autorización acordados.
c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
d) Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
e) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
f) Obtener aprobación formal por parte del depto. de informática para las tareas detalladas, antes que comiencen las tareas.
g) Solicitar la revisión del depto. de informática para garantizar que no se violen los requerimientos de segundad que debe cumplir el software.
h) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
i) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
j) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
k) Mantener un control de versiones para todas las actualizaciones de software.
l) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
m) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
n) Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en "Control del Software Operativo".

10.4.2. Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad. Para ello, se definirá un procedimiento que incluya:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
c) Asegurar la actualización del Plan de Continuidad de las Actividades de la Organización.

10.4.3. Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del depto. de informática se deberá:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Determinar la conveniencia de que la modificación sea efectuada por el Organismo, por el proveedor o por un tercero.
c) Evaluar el impacto que se produce si el Organismo se hace cargo del mantenimiento.
d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

10.4.4. Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario. En este sentido, se redactarán normas y procedimientos que incluyan:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.
b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
c) Controlar el acceso y las modificaciones al código instalado.
d) Utilizar herramientas para la protección contra la infección del software con código malicioso.

10.4.5. Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos.
b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
d) Verificación del cumplimiento de las condiciones de seguridad.
e) Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

Modelo de separación de ambientes

Para cumplir con esta Política, en lo referente a los puntos "Seguridad de los Archivos del Sistema y "Seguridad de los Procesos de Desarrollo y Soporte", se sugiere implementar un modelo de separación de funciones entre los distintos ambientes involucrados.

Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

A continuación, se presenta un modelo ideal formado por tres ambientes que debe ser adaptado a las características propias de cada Organismo, teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

Ambiente de Desarrollo

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir alguna fuente para modificar, quedando registrado en el sistema de control de versiones que administra el "administrador de programas fuentes".

El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera

que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

Ambiente de Pruebas

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible. El testeador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctas de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

Ambiente de Producción

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El "implementador" compila el programa fuente dentro del ambiente de producción en el momento de realizar el pasaje para asegurar de esta forma que hay una correspondencia bi-unívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

Deberían aplicarse procedimientos de la misma naturaleza y alcance para las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, Productos middleware) deberían cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores.

Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

11. Gestión de la Continuidad de la organización

Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles de la Organización.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades de la Organización puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la Organización y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales de la organización (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro. Maximizar la efectividad de las operaciones de contingencia de la Organización con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) ***Notificación / Activación:*** Consistente en la detección y determinación del daño y la activación del plan.
b) ***Reanudación:*** Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
c) ***Recuperación:*** Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal de la Organización y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

Esta Política se aplica a todos los procesos críticos identificados de la Organización.

Responsabilidad

El depto. de informática participará activamente en la definición, documentación, prueba *y* actualización de los planes de contingencia.

Los Propietarios de la Información las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos *y/o* las actividades de la Organización.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Organización.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Organización.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en los planes de continuidad. Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

- Asegurar que todos los integrantes de la Organización comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
- Elaborar y documentar una estrategia de continuidad de las actividades de la organización consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades de la Organización de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la Organización.
- Proponer las modificaciones a los planes de contingencia.

Políticas relativas a la Continuidad de Negocio

11.1. Proceso de la Administración de la Continuidad del Organismo

Este tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la Organización frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

a) Identificar y priorizar los procesos críticos de las actividades de la Organización.
b) Asegurar que todos los integrantes de la Organización comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
c) Elaborar y documentar una estrategia de continuidad de las actividades de la organización consecuente con los objetivos y prioridades acordados.
d) Proponer planes de continuidad de las actividades de la Organización de conformidad con la estrategia de continuidad acordada.
e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
f) Coordinar actualizaciones periódicas de los planes y procesos implementados.
g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la Organización.
h) Proponer las modificaciones a los planes de contingencia.

11.2. Continuidad de las Actividades y Análisis de los Impactos

Con el fin de establecer un Plan de Continuidad de las Actividades de la Organización se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el depto. de informática, considerando todos los procesos de las actividades de la Organización y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad de la Organización para su aprobación.

11.3. Elaboración e Implementación de los Planes de Continuidad de las Actividades de la Organización

Los propietarios de procesos y recursos de información, con la asistencia del depto. de informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Organización. Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a

implementaren cada caso.

c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
d) Documentar los procedimientos y procesos acordados.
e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
f) Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

    1. Objetivo del plan.
    2. Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
    3. Procedimientos de divulgación.
    4. Requisitos de la seguridad.
    5. Procesos específicos para el personal involucrado.
    6. Responsabilidades individuales.

g) Probar y actualizar los planes.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades del Organismo requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

12. Cumplimiento

Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales. Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

El Área Legal de la Organización, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo. Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Organización.

Alcance

Esta Política se aplica a todo el personal de la Organización, cualquiera sea su situación de revista. Asimismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas de la Organización y a las auditorías efectuadas sobre los mismos.

Responsabilidad

El depto. de informática cumplirá las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
- Realizar revisiones periódicas de todas las áreas de la Organización a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política,normas y procedimientos de seguridad establecidos.
- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

Los responsables de Unidades Organizativas velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

Política sobre el cumplimiento de Requisitos Legales

12.1. Cumplimiento de Requisitos Legales

12.1.1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

12.1.2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual. Los empleados únicamente podrán utilizar material autorizado por el Organismo. El Organismo solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente. La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales. Se deberán tener presentes las siguientes normas:

Ley de Propiedad Intelectual, LEY 17336 DE PROPIEDAD INTELECTUAL

12.1.2.1. Derecho de Propiedad Intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la Ley 17336 de Propiedad Intelectual.

Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción. Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen

limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El depto. de informática, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
c) Mantener un adecuado registro de activos.
d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.
f) Verificar que sólo se instalen productos con licencia y software autorizado.
g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
i) Utilizar herramientas de auditoría adecuadas.
j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

12.1.3. Protección de los Registros de la Organización

Los registros críticos de la Organización se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la Organización. Los registros se clasificarán en diferentes tipos, por ejemplo, registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo, papel.

Se debe considerar que la generación y el resguardo contra pérdida, destrucción y falsificación los registros en papel generados por cada Dirección/Departamento/Sección son de responsabilidad del encargado de cada área y según los plazos y condiciones que indique la ley.

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento *y* manipulación se implementarán de acuerdo con las recomendaciones del fabricante.

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo, que todos los registros requeridos puedan recuperarse en un plazo *y* un formato aceptable.

El sistema de almacenamiento *y* manipulación garantizará una clara identificación de los registros *y* de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para el Organismo. A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.

c) Mantener un inventario de programas fuentes de información clave.
d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

12.1.4. Protección de Datos y Privacidad de la Información Personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del responsable del Activo de que se trate.

Se debe mantener la vigilancia legal de la presente política, teniendo en cuenta todas las leyes de la república relativas a la Información y sus derechos de acceso.

12.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información de la Organización se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido. Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

12.1.6. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.
Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, el Organismo garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida. Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

a) Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.
b) Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

Se deberá tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, procedimiento administrativo especial, de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las responsabilidades impuestas a los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley 19880 de Procedimientos Administrativos y por toda otra normativa aplicable, incluido el Código Penal, los artículos competentes

12.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica

12.2.1. Cumplimiento de la Política de Seguridad

Cada responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad. El depto. de informática, realizará revisiones periódicas de todas las áreas de la Organización a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Propietarios de información.
d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

12.2.2. Verificación de la Compatibilidad Técnica

El depto. de informática verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico. La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema. Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

12.3. Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias y reglamentarias convencionales que rigen al personal de la Administración Pública, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables. Amén de las sanciones disciplinarias o administrativas, el agente que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial - cuando ocasiona un daño que debe ser indemnizado- y/o en responsabilidad penal -cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

PROCEDIMIENTOS DE EL DEPARTAMENTO DE INFORMATICA Y NUEVAS TECNOLOGIAS

DESCRIPCIÓN PROCEDIMIENTO	
Nombre	**Atención y Soporte Técnico a Usuarios**
Objetivo	Establecer los mecanismos que permitan la ejecución de acciones orientadas a mantener en condiciones de operatividad y funcionalidad la infraestructura TIC (Tecnologías de Información y Comunicación) de la Ilustre Municipalidad de Loncoche, facilitando con ello el cumplimiento de sus objetivos
Alcance	Todos los usuarios de la plataforma Informática de la Ilustre Municipalidad de La Loncoche
Frecuencia	Diaria

NORMAS
Para los servicios de la I. Municipalidad de Loncoche los usuarios deberán solicitar soporte técnico vía telefónica con respaldo de la misma a correo electrónico soporte@muniloncoche.cl Las Solicitudes de atención serán tramitadas y ejecutadas de acuerdo al orden de ingreso de las mismas, o en su defecto de acuerdo al nivel de urgencia de las mismas.

DESCRIPCION DEL PROCEDIMIENTO		
	Actividad	**Responsable**
1	Recibe vía telefónica o mediante correo electrónico soporte@muniloncoche.cl, solicitud de asistencia. Ninguna solicitud será atendida si no se realiza por los medios mencionado	Depto. Informática
2	Se realiza el análisis de la urgencia o premura de la solicitud	Depto. Informática
3	Solucionar en forma remota o telefónicamente la incidencia reportada	Depto. Informática
4	Personal del depto. de informática realiza visita a terreno a revisar el dispositivo, cuando la falla no pudiese resolverse vía telefónica o remota	Depto. Informática

DESCRIPCIÓN PROCEDIMIENTO	
Nombre	**Creación de Cuenta de Correo electrónico**
Objetivo	El objetivo de este Procedimiento es otorgar un ordenamiento en el uso del servicio de correo electrónico, definiendo de manera general, no limitativa, las actuaciones consideradas como abusivas y prohibidas

Alcance	Funcionarios de la MUNICIPALIDAD, autorizados por Jefatura o superior jerárquico
Frecuencia	Eventual

NORMAS

POLÍTICAS: El servicio de correo electrónico es una plataforma de comunicación brindada por la Organización, la que permite a los usuarios enviar y recibir mensajes a todo el mundo electrónicamente. Este servicio se utiliza para mejorar la comunicación entre los funcionarios y entre entidades públicas o privadas. Este servicio bajo ninguna circunstancia debe ser considerado como un medio privado y personal de comunicación sino como uno institucional.

A) Es responsabilidad del usuario mantener la confidencialidad de la clave de acceso.
B) La cuenta de correo es personal e intransferible no permitiéndose que segundas personas hagan uso de ella.
C) Cada usuario es el responsable de las acciones efectuadas en su cuenta.
D) Es responsabilidad del usuario limpiar su cuenta de correo periódicamente para que exista espacio de almacenaje disponible y realizar sus respaldos de correspondencia electrónica.
E) Se prohíbe expresamente utilizar el servicio en cualquier actividad distinta a las relacionadas con el trabajo, asumiendo (el usuario) la responsabilidad por daños o perdidas de información atribuibles a este hecho.
f) El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión y cierre de la misma.
g) Se prohíbe expresamente inscribirse en listas de correos o de servidores, las cuales no estén relacionadas directamente con su trabajo. Algunas listas de correo o servidores generan cantidades masivas de correos a los suscriptores. Esto no solamente satura el espacio disponible en el disco duro de la estación de trabajo, sino que también degrada el funcionamiento del sistema de e-mail completo.
h) El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no mandar SPAMS (correos masivos no autorizados) de información, ni mandar archivos adjuntos que pudieran contener información nociva para otro usuario como virus o pornografía
1) La contraseña del correo electrónico es intransferible y no debe ser confiada a ninguna otra persona. No compartirla de modo que algún extraño pueda usarla para enviar mensajes con otros propósitos. La ILMS no se hace responsable por el uso que el usuario final le dé a esta cuenta de correo electrónico
m) Está prohibido descargar archivos con extensión .exe, .vbs, avi, protectores de pantalla, etc. que no provenga de un usuario conocido, pues, aunque es probable que no sean virus, pueden ser programas dañinos. En estos casos, se les recomienda borrar inmediatamente el mensaje y en caso de recibir un mensaje bajo sospecha de virus, contacte al depto. de informática.

DESCRIPCIÓN PROCEDIMIENTO	
Nombre	**Acceso, Modificación *y* Eliminación de privilegios de acceso**
Objetivo	Restringir *y* controlar la asignación *y* el uso de privilegios de acceso a los sistemas de información
Alcance	Jefaturas o superior jerárquico
Frecuencia	Eventual

NORMAS

Para mantener un control efectivo del acceso a los datos *y* servicios de información, los jefes de unidades o departamentos o direcciones, deberán informar a el Departamento de Informática sobre asignación de funciones que signifiquen que el usuario deba utilizar sistemas de información así como también es responsable de los cambios relativos a esas atribuciones, con el fin de proteger la integridad de la información *y* revocar o modificar oportunamente los accesos a la información de la cual *ya* no tenga responsabilidad el usuario.

POLÍTICAS

REVOCACIÓN O BAJA DE CUENTAS Y ACCESOS.
Revocación por conducta inapropiada
El uso de las computadoras, red *y* sistemas de acceso a información de la municipalidad puede ser temporalmente o incluso permanentemente revocado en cualquier momento por conducta inapropiada.
Dicha conducta incluye;

- la introducción de información ilegal al sistema

DEFINICIONES

Mensajes Adjuntos: El servicio de correo permite enviar archivos anexados (attachments) de hasta 15 MB
Interface web: El usuario podrá acceder al correo institucional, desde cualquier punto con acceso a internet, ingresando a la siguiente dirección http://www.gmail.com.
Cuota: Los buzones tienen una cuota máxima de hasta 30 GB por usuario, por lo tanto, el usuario deberá eliminar periódicamente los mensajes leídos de modo tal que no exceda esa cuota.

DESCRIPCION DEL PROCEDIMIENTO

	Actividad	Responsable
1	Recibe vía correo electrónico soporte@muniloncoche.cl o bien solicitud mediante un ordinario. Se debe definir el nombre, rut y dependencia del usuario que requiera la cuenta. Ninguna solicitud será atendida si no se realiza por los medios mencionados	Depto Informát
2	Recibe correo u ordinario se verifica validación	Depto. Informática
3 a	Aprueba solicitud y asigna para su ejecución	Depto. Informática
3 b	No aprueba solicitud y envía ordinario de notificación al solicitante especifica motivos	Depto. Informática
5	Realiza ejecución de solicitud, comprueba correcto funcionamiento	Mesa de Ayuda

- el transporte de "software" con derechos de autor de un sistema de información a otra (ya sea por medios físicos, mecánicos o electrónicos) sin el consentimiento del autor.
- El uso de lenguaje abusivo o cuestionable tanto en mensajes públicos como en privados
- El envío de mensajes que puedan ocasionar la pérdida de datos o sistemas del destinatario.
- El envío de "cadenas", listas de mensajes o individuos ("mailing lists")
- El envío de mensajes no solicitados ("spamming"), o cualquier otro uso que pueda provocar la congestión de la red o que de alguna otra forma interfiera con el trabajo de otros usuarios de la red de municipalidad.
- No cumplimiento del presente reglamento.
- Uso inapropiado del servicio internet (paginas obscenas, pornografía, descarga de aplicaciones p2p)

Revocación de cuentas por desvinculación con municipalidad.

Con el fin de mantener un control efectivo del acceso o la información, el Departamento de Informática está facultado para revocar cuentas de correo, dominio, privilegios de acceso, etc., de los usuarios que ya no pertenezcan a esta institución, previo documento enviado por el Departamento de Recursos humanos o departamento de personal. Sin perjuicio de lo anterior es responsabilidad de las jefaturas o encargados de unidades y/o departamentos de la municipalidad, entregar oportunamente información con la desvinculación de funcionarios dependientes de su área.

Revocación o baja de cuentas y accesos. Modificación de privilegios de acceso.
Se realizará la modificación de los permisos y acceso a la información en los siguientes casos;

- Cuando el jefe del departamento, superior jerárquico directo o encargado del sistema solicite modificación.
- Cuando un usuario deje de cumplir funciones en un Departamento o unidad determinado (para este caso el usuario quedará sin acceso a los sistemas Informáticos de la municipalidad.)
- El Departamento de Informática está facultado para modificar permisos o accesos en los siguientes casos:

    1. El usuario haya incurrido en actos ilegales.
    2. Requerimiento expreso de Autoridades competentes.
    3. Requerimiento expreso de jefatura o superior jerárquico del usuario.
    4. Para identificar o resolver problemas técnicos.
    5. El acceso comprometa el normal funcionamiento del servicio.

Revocación o baja de cuentas y accesos.
Seguridad y privacidad
El uso de instrumento informático y acceso a información está cubierto y detallado actualmente en la Ley 19223 del Ministerio de Justicia, donde se tipifican y *detallan* sanciones judiciales por uso mal intencionado de la información (ver pág. 3, Ley de delitos informáticos). La violación de dichas leyes puede conllevar encarcelamiento o el pago de costosas multas. La política de seguridad a la que se adhieren los sistemas de Informática de la municipalidad es la siguiente:

- Todos los usuarios son responsables de cumplir con las políticas de seguridad y privacidad establecidas por la municipalidad.
- El privilegio de uso de los sistemas de informática e información será revocado en caso de violación de estas políticas, sin importar cuan necesario sea el uso de computadores para completar las tareas asignadas a dicha persona.
- Cualquier usuario implicado en infracciones de esta política, políticas del servicio, leyes civiles o criminales con relación a la privacidad y seguridad computacional de la municipalidad será sujeto a acción disciplinaria incluyendo, pero no limitada a, revocación de privilegios a recursos de informática, suspensión de equipamiento computacional, eliminación de cuentas y accesos.

Todos los usuarios deben cooperar con las autoridades policiales, judiciales u otros que ejerzan auditorias, en la investigación y convicción de cualquier sospecha de infracción a la seguridad y privacidad que involucren a personal de municipalidad y/o los recursos de TIC de MUNICIPALIDAD.

DESCRIPCION DEL PROCEDIMIENTO		
	Actividad	**Responsable**
1	Recibe vía telefónica o mediante correo electrónico soporte@muniloncoche.cl o bien envía notificación de creación de acceso, desvinculación o traslado de funcionario a otro Departamento o unidad Ninguna solicitud será atendida si no se realiza por los medios mencionados	Depto. Informática
1 a	Si es desvinculación, se realiza revocación de todos los accesos, cuentas y privilegios	Depto. Informática
1 b	Si es creación de accesos se valida la información y se realiza la configuración de accesos solicitados	Depto. Informática
2	Recibe solicitud y realiza modificación de privilegios de acceso	Depto. Informática
4	Realiza ejecución de solicitud, comprueba correcto funcionamiento	Depto. Informática
5	Una vez solucionada la incidencia, el funcionario derivara una copia al usuario mediante correo electrónico	Depto. Informática

DESCRIPCIÓN PROCEDIMIENTO	
Nombre	**Solicitud de informe técnico para adquisición de Hardware o software**
Objetivo	Establecer los pasos necesarios que deberán seguir las áreas y Departamento del MUNICIPALIDAD, para solicitar la adquisición de equipamiento TIC.
Alcance	Direcciones de la MUNICIPALIDAD
Frecuencia	Eventual

NORMAS

POLÍTICAS

Las solicitudes para la generación de informes técnicos para adquisición de cualquier equipo TIC (impresora, escáner, monitor, radios, antenas, partes y piezas, etc.) deben ser enviadas por el Director y/o Unidades respectivo vía Ordinario o correo electrónico al Departamento de informática, quien determinara los planes y prioridad para el equipamiento computacional dependiendo de las necesidades y requerimiento del usuario.

Toda solicitud debe ser fundada y remitida a el Departamento de informática que evaluara los costos y beneficios que el solicitante incluya en la solicitud que respalda su pedido.

Es responsabilidad de los usuarios cuidar y mantener el buen estado de los equipos entregados a su custodia.

Todo equipo TIC (impresora, scanner, monitor, etc.) ya sea propiedad de la empresa externa o de la MUNICIPALIDAD, deberá permanecer en el lugar asignado de acuerdo a lo indicado en la solicitud enviada por la unidad, ya que frente a una auditoria debe saberse el lugar físico donde se encuentran.

Normas Generales de uso

Los usuarios deberán cuidar física y lógicamente los recursos computacionales existentes; pensando que estos están al servicio de todos.

No manipular alimentos sobre los equipos teniendo especial cuidado de no derramar líquidos sobre ellos.

No está permitida la utilización de equipos con fines recreativos, ni fines particulares.

El usuario debe mantener la limpieza externa de los equipos computacionales.

Normas de hardware

El usuario no deberá abrir los equipos computacionales, como tampoco sacar o cambiar componentes de los equipos

Está prohibido instalar equipos sin la autorización expresa del Departamento de informática.

Normas de Software

El equipo que sea entregado al usuario contendrá en el disco duro el software básico, siendo estos todos los definidos por el Departamento de informática, como mínimo para su operación.

Configuración Base:

- Sistema operativo Windows 10 o similar
- Herramienta administrativa Microsoft Office
- Browser (Chrome)
- Acrobat Reader
- Win Rar
- Antivirus

DESCRIPCION DEL PROCEDIMIENTO		
	Actividad	**Responsable**
1	Solicita por oficio, memorándum o correo electrónico a soporte@muniloncoche.cl al Departamento de informática (se debe especificar nombre y RUT del usuario final)	Director o jefatura que solicita
2	Recibe solicitud, determina las necesidades y genera informe técnico respectivo.	Depto. informática
3	Remite informe al funcionario solicitante.	Depto. informática

REGLAMENTOS

Reglamento para el uso de recursos de tecnologías de la información

Objetivo

Regular el uso de los servicios de TIC, con el fin de racionalizar y optimizar el uso de dichos recursos y servicios y asegurar una mayor calidad en el desarrollo de las funciones propias de la Ilustre Municipalidad de Loncoche, este reglamento se fundamentan en la normativa vigente y la política de seguridad de la Información de la Ilustre Municipalidad de Loncoche, buenas prácticas comúnmente utilizadas, así como también en el ejercicio ético de las actividades funcionarías por cuanto gestionamos recursos Públicos.

Ámbitos de aplicación y competencia

El uso de los Activos de TIC de la MUNICIPALIDAD, está determinado por la calidad de funcionario, independiente del tipo de contrato y que en las funciones de su contrato esté previsto el uso de este tipo de recurso, o en su defecto a solicitud del director Responsable del funcionario. Los recursos que son parte del alcance de esta regulación son:

1. Computadores, Notebooks, Netbooks, Tablets u otro recurso de cómputo.
2. Internet, Intranet y Correo electrónico.
3. Otros Sistemas o servicios de Información.
4. Telefonía Celular
5. Equipos de Radio Comunicaciones.
6. Telefonía Fija
7. Internet Móvil
8. Servicio de Impresión

Los activos de TIC, corresponden a un activo estratégico de la organización por lo que el presente reglamento establece con claridad cómo se ejerce el acceso y baja de los servicios.

Los funcionarios de la MUNICIPALIDAD, podrán emplear los servicios en la medida que cumplan el presente reglamento, en los términos previsto. El usuario deberá leer y observar estas normas y el desconocimiento de las mismas no le exime de las responsabilidades y sanciones a que se haga acreedor.

La aplicación del presente documento rige a partir de su promulgación por decreto alcaldicio y estará sujeta a cualquier tipo de modificación que estime el Departamento de informática y nuevas tecnologías. El Departamento de informática y nuevas tecnologías es la dependencia encargada de proporcionar y garantizar el servicio de acceso institucional a los servicios listados. La interacción de ésta con los usuarios, deberá realizarse siempre a través de las siguientes vías:

IMPORTANTE:
Queda estrictamente prohibido intentar resolver problemas en los equipos y/o sistemas sin estar en contacto con algún profesional del depto. informática.
Cualquier falla o daño en los equipos y/o servicios originados por acciones no autorizadas serán informadas a los superiores jerárquicos y dependiendo de la envergadura del daño se solicitarán las acciones que contemple la regulación de la organización

Acceso a los servicios

Solo serán consideradas las solicitudes de acceso a los servicios emanadas de los Directores o jefaturas de la MUNICIPALIDAD, solicitud que, si bien es posible realizarla vía llamado telefónico, debe ser respaldada con el envío de un correo electrónico a soporte@muniloncoche.cl u ordinario dirigido a la Unidad

En este mismo sentido es responsabilidad de los Directores y jefaturas, informar de los cambios de funciones o traslados o desvinculaciones de funcionarios para que el Departamento de informatica pueda dar de baja los accesos que pudiese tener, para mantener la seguridad de los activos de TIC de la organización. Sin perjuicio de lo anterior es el Departamento de Personal quien validará la información mediante un oficio, ordinario o correo electrónico.

Reglamento de uso de los servicios

Servicio 1; Computadores, Notebooks, Netbooks, Tablets u otro recurso de computo

Sobre la asignación

En cada Dirección Municipal, el director es el único que puede solicitar la asignación de un Computador (dependiendo de la disponibilidad de los recursos), pues es quien conoce la operación y necesidades de la misma, y su consumo repercute en gastos generados por su departamento.

El Director informará a la Unidad las funciones a desempeñar para la evaluación del perfil del equipo a asignar. Además, Indicara los niveles de acceso a aplicaciones.

El estándar utilizado en la Organización para la asignación de Computadores y equipos afines será determinado por el Depto. de informática bajo las siguientes premisas y con el visto bueno del director de División:

- Cada secretaria y director de departamento contará con un Computador de Perfil Básico, adecuado a sus funciones.
- Cada Profesional o Administrativo que cumpla funciones que requieran el uso de PC, se le asignara un equipo, si esto no ocurre, solamente se explica por falta de recursos. Sin embargo, es posible que más de un funcionario utilice un equipo, En el caso de computador compartido, se debe declarar a cada uno de los usuarios, puesto que se les creará una clave personal para uso.

Sobre el uso

Disposiciones Generales:

- Cada Computador es de responsabilidad del funcionario que lo tiene asignado.
- Las claves de acceso son personales e intransferibles.
- Está prohibido facilitar el equipo a personas ajenas al servicio o a quien no se le ha asignado privilegios de acceso a algún servicio de TIC.
- El acceso a los servicios siempre estará respaldado por una solicitud hecha por el director del servicio.
- La información contenida en los computadores es de propiedad del servicio. Y en ningún caso podrá utilizarse para fines personales.
- Desde cada computador será posible acceder a los servicios, y aplicaciones que estén asociados a su perfil, quedando estrictamente prohibido intentar ingresar a sistemas o servicios de manera no autorizada.
- Está prohibido instalar aplicaciones sin la autorización del Depto. de informática
- Está prohibido desinstalar aplicaciones sin la autorización del Depto. de informática.
- La limpieza exterior del equipo es de responsabilidad del usuario
- La utilización de medios extraíbles de información debe ser autorizada por el Depto. de informática.
- Los recursos de computación se deben usar exclusivamente para propósitos relacionados con la actividad desempeñada en la MUNICIPALIDAD.
- Está prohibido trasladar de ubicación los equipos.

Buenas Prácticas

- Mantenga su escritorio o estación de trabajo despejada y en orden si no está utilizando el Computador, apáguelo.
- Si está trabajando y se retira a una reunión o salida a terreno, bloquee el acceso a él o simplemente apáguelo.

Sobre los Reportes de Fallas.

El reporte de fallas se debe realizar vía correo electrónico (soporte@muniloncoche.cl), área encargada de recibir TODAS las necesidades de la organización, siendo esta responsable de realizar la derivación de las mismas.

Servicio 2: Internet, Intranet y Correo electrónico.

Sobre la asignación

El servicio de Internet e Intranet estará disponible para todos los equipos de la organización, sin embargo, si un Director establece que este servicio no agrega valor al desempeño de un funcionario, podrá solicitar el bloqueo del mismo. Es importante entender que el acceso al servicio de Intranet e Internet se entrega al Equipo y el servicio de correo electrónico es asignado al funcionario. Respecto al Correo electrónico, existen dos vías para asignar este recurso a un funcionario; Personal al momento de ingresar a un nuevo RRHH, por funciones podrá solicitar una cuenta de correo a el Departamento de informática, y si este no es cursado desde Personal, el director, superior jerárquico del funcionario podrá solicitar la asignación de este recurso.

Cabe señalar que la asignación de correos es a PERSONAS y no a Unidades Organizativas o a Funciones.

Sobre la solicitud

La Solicitud de Restricción de Internet se debe realizar por los medios de correo electrónico a soporte@muniloncoche.cl, entregando los siguientes Antecedentes:

- Nombre del Funcionario
- Rut
- Funcionario
- Ubicación física del equipo,

La información aquí señalada es requisito para cursar la solicitud, es decir, si esta no está completa, faltando alguno de estos antecedentes, la solicitud no ingresará al flujo de trabajo.

La petición de un Correo Electrónico (nombre@muniloncoche.cl) se realizará por los medios ya definidos; entregando los siguientes Antecedentes:

- Nombre del Funcionario
- Rut Funcionario
- Tipo de Contrato
- Fecha Inicio Contrato
- Sección/Departamento/Dirección de dependencia
- Ubicación Física,
- Superior Jerárquico

La información aquí señalada es requisito para cursar la solicitud, es decir, si esta no está completa, faltando alguno de estos antecedentes, la solicitud no ingresara al flujo de trabajo.

Sobre el uso

Disposiciones Generales:

Queda prohibido acceder a sitios de Internet en donde se incite o promueva Pornografía, segregación racial, sexual, religiosa, social, política etc. Piratería de cualquier tipo de material multimedia con derechos de propiedad intelectual, fabricación de cualquier material o dispositivo que pueda ser utilizado para dañar la integridad o propiedad de cualquier persona o institución, actividades encaminadas a acceder ilícitamente a otros sistemas de información con fin de recabar dañar o manipular la información de tales sistemas para obtener provecho personal, por diversión o para beneficiar o perjudicar a terceros.

Queda terminantemente prohibido la instalación de cualquier software adicional al oficialmente instalado por la MUNICIPALIDAD, en cualquier computadora utilizada para acceder a Internet, no importando el tipo ni origen del mismo.

Queda prohibido el envió de Chain Letters (cartas de cadena), en virtud de que él envió simultáneo de mensajes puede fácilmente escalar a miles de mensajes enviados e interferir con la recepción de mensajes legítimos y propios de trabajo.

Se prohíbe realizar a través de Internet cualquier actividad ilegal o maliciosa que causa molestias o daños a segundas o terceras personas dentro o fuera de la MUNICIPALIDAD.

En el envió de mensajes electrónicos, se prohíbe el uso de lenguaje abusivo, soez, vulgar, obsceno o cuestionable.

Está prohibido el uso de sitios de conversación (Chat).

Está prohibido el uso de sitios de streaming (youtube, radios online, televisión online, etc.) con el fin de mantener la calidad de servicio en la red

Está prohibido el uso de redes sociales. Si se requiere utilizar redes sociales por motivos laborales, el director de la unidad debe solicitar mediante correo electrónico la habilitación de un solo equipo.

En cualquier actividad realizada a través de Internet, se prohíbe lesionar o desacreditar el prestigio de la MUNICIPALIDAD

Igualmente se prohíbe terminantemente la transmisión de cualquier tipo de información confidencial o propia de la MUNICIPALIDAD bajo cualquier medio.

Respetar la protección legal otorgada a programas, textos, artículos y bases de datos según legislación sobre propiedad intelectual y derecho de autor.

Respetar la integridad de los sistemas de computación. Esto significa que ningún usuario podrá adelantar acciones orientadas a infiltrarse, dañar o atacar la seguridad informática de la MUNICIPALIDAD, a través de medio físico o electrónico alguno.

No obtener ni suministrar información sin la debida autorización, no dar a conocer códigos de seguridad tales como contraseñas a otras personas, o entorpecer por ningún medio el funcionamiento de los sistemas de información y telecomunicaciones de la MUNICIPALIDAD.

No está permitido acceder a Internet con fines diferentes a los propios de las actividades de la MUNICIPALIDAD.

La creación de nuevas redes, configuración o bien modificación de las existentes, solo podrá ser realizada por personal autorizado del Departamento de informática.

La MUNICIPALIDAD asignará una cuenta de correo electrónico a los funcionarios según sea solicitado por la Dirección de personal, o del Director respectivo. Dicha cuenta es personal e intransferible.

En el uso del correo electrónico no está permitido:

- Atentar contra la integridad de la organización y de su autoridad Máxima. Divulgar información que incite a la discriminación o la violencia.
- Enviar contenidos con fines publicitarios y comerciales de bienes y servicios en beneficio propio, de familiares o de terceros, salvo en los casos en los cuales el Departamento de Modernización y Tecnologías de la Información lo autorice expresamente.
- Enviar correo tipo SPAM, es decir "correo basura", relacionado con falsos virus, con publicidad de empresas, cadenas de mensajes, etc.
- Usar la cuenta de correo electrónico de otro usuario o entregar a un tercero la contraseña propia.
- Falsificar mensajes de correo electrónico.
- Leer, borrar, copiar o modificar mensajes de correo electrónico de otras personas, sin su autorización.

- Enviar mensajes de correo electrónico, alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse.
- Iniciar o continuar cadenas de mensajes pues éstas tienden a congestionar innecesariamente la red.
- Usar el servidor de correos como medio para archivar los mensajes, los cuales se recomienda borrar una vez leídos. Si hay necesidad de conservarlos, los mensajes se deberán grabar en un sitio destinado para su almacenamiento; esto también se aplica a los correos enviados y a la papelera de reciclaje. Así mismo, cuando las unidades requieran compartir un archivo, se sugiere hacerlo utilizando las herramientas pertinentes, en vez de enviarlo por correo.

IMPORTANTE: La MUNICIPALIDAD no asume responsabilidad alguna por los contenidos emitidos a través del correo electrónico o por el uso ilegal y mal intencionado por parte de los usuarios.

Buenas Prácticas;

El correo electrónico no es mensajería instantánea, por lo tanto, no envíe un correo electrónico para comunicar un hecho que requiere inmediatez en la comunicación.

- No pida confirmación de lectura de ningún tipo, el correo electrónico fue diseñado para informar si el correo NO LLEGA.
- Busque correos en la bandeja de SPAM, es posible que algún remitente este clasificado de tal forma y los correos lleguen a la casilla SPAM.
- No responder correos en cadena.
- No abrir correos con adjuntos si no han sido solicitados.
- No imprima correos electrónicos a menos que sea estrictamente necesario

IMPORTANTE el Departamento de Informática y nuevas tecnologías en virtud de la continuidad de los servicios y operaciones, registra los accesos a los servicios de internet, Intranet y correo electrónico, por lo que las actividades de los usuarios, que no cumplan lo aquí estipulado serán informadas a los superiores jerárquicos para las acciones pertinentes.

Servicio 3; Otros Sistemas o servicios de Información.

Sobre la asignación o autorización de acceso

Cada sistema de Información tiene un Director o Jefe de Departamento que ejerce el Rol de "Propietario"; esto es, existe un responsable que colabora con el Departamento de informática para cumplir los requisitos de la información relativos al sistema. Teniendo esto definido, las autorizaciones o revocaciones de Acceso a los sistemas de información debe ser enviada por el Propietario del sistema a el Departamento de informatica.

Sobre la solicitud

La petición de acceso a un Sistema de Información, se realizará por los medios ya definidos y además se enviará un Ordinario o Memo dirigido a el Departamento de informática, entregando los siguientes Antecedentes:

- Nombre del Funcionarios Responsable, indicando si tiene o no responsabilidad administrativa.
- Rut Funcionario
- Sistemas a Utilizar
- Nivel de acceso

La información aquí señalada es requisito para cursar la solicitud, es decir, si esta no está completa, faltando alguno de estos antecedentes, la solicitud no ingresará al flujo de trabajo.

Sobre el uso

Disposiciones Generales:

- Las Claves de sistemas y/o accesos son PERSONALES e INSTRANSFERIBLES
- La responsabilidad asociada a uso de las claves recae en cada funcionario.

Buenas Prácticas;

- Si se aleja del equipo del que hace uso el sistema, cierre su sesión.
- No anote sus credenciales de acceso en papeles u otro soporte físico.

Sobre la Instalación Temporal para Eventos

Si es necesario este servicio se evaluará caso a caso y debe ser presentado en las planificaciones anuales, debido a la complejidad de estos las evaluaciones deben realizarse con la anticipación necesaria

Sobre los Reportes de Fallas.

El reporte de fallas se debe realizar vía correo electrónico a soporte@muniloncoche.cl, vía telefónica, al área informática encargada de recibir TODAS las necesidades de la organización, siendo esta responsable de derivar en caso de ser necesario.

IMPORTANTE el Departamento de informatica en virtud de la continuidad de los servicios y operaciones, registra los accesos a los sistemas de información o aplicaciones, por lo que las actividades de los usuarios, que no cumplan lo aquí estipulado serán informadas a los superiores jerárquicos para las acciones pertinentes.

Servicio 4; Telefonía Celular

Sobre la asignación

Los Teléfonos Móviles o Celulares se entregan a los Directores y funcionarios determinados por el Sr. Administrador Municipal.

Sobre el uso

Disposiciones Generales:

- El equipo y sus accesorios son proveídos por el municipio, cualquier falla atribuible al usuario, robo, o pérdida del aparato, la renovación será costo del usuario, así como también la renovación de cargadores y manos Libres.
- En caso de pérdida o robo, es responsabilidad del usuario, avisar al depto. de informática con la mayor prontitud posible y dejar la constancia en Carabineros de Chile o fiscalía, entregando una copia de dicha constancia a mesa de ayuda.
- El fin del aparato es comunicar al funcionario para cumplir funciones de trabajo y no para su uso personal, las labores y horarios de cada funcionario están estipuladas en sus respectivos contratos y decretos de nombramiento.
- A cada usuario se le asignara un MÁXIMO de minutos y de datos a utilizar cada mes, siendo responsabilidad de él procurar un buen uso del tiempo.
- La solicitud de minutos o datos extras en el mes debe ser mediante un correo a administración@muniloncoche.cl con copia a soporte@muniloncoche.cl.

Sobre los Reportes de Fallas.

El reporte de fallas se debe realizar vía telefónica o correo electrónico a soporte@muniloncoche.cl, siendo el depto. de informática la responsable de derivar la petición en caso de ser necesario.

IMPORTANTE el Departamento de informativa virtud de la continuidad de los servicios y operaciones, registra los accesos a los sistemas de información o aplicaciones, por lo que las actividades de los usuarios, que no cumplan lo aquí estipulado serán informadas a los superiores jerárquicos para las acciones pertinentes.

Servicio 5; Servicio de Telefonía Fija

Sobre la asignación de teléfonos

En cada Dirección Municipal, el director es el único que puede solicitar la asignación de un anexo telefónico (dependiendo de la disponibilidad de los recursos), pues es quien conoce la operación y necesidades de la misma, y su consumo repercute en gastos generados por su división.

El director decidirá si el teléfono asignado será un número directo o no, esto es si el anexo puede ser llamado directamente del exterior o no.

El estándar utilizado en la Organización para la asignación de aparatos telefónicos y/o líneas será determinado por el depto. de Informática bajo las siguientes premisas y con el visto bueno del Director de División:

Cada secretaria y director de departamento contará con un aparato telefónico adecuado a sus funciones.

En cada área compartida ocupada existirá un anexo telefónico, ya que no existe capacidad para habilitar un anexo por funcionario.

En el caso de teléfonos compartidos, se debe declarar a cada uno de los usuarios, puesto que se les creará una clave personal para uso.

Todas las solicitudes se atenderán dependiendo de los recursos tecnológicos disponibles, y se informara al director si se aprueba o no esta solicitud, teniendo como argumento dicha disponibilidad.

Sobre la solicitud

La petición de una línea telefónica se hará vía correo electrónico, a la cuenta soporte@muniloncoche.cl, desde el correo del director o vía Ordinario o Memo dirigido a el Departamento de informática.

Se debe indicar si requiere acceso al exterior según la siguiente tabla:

CODIGO	SALIDAS
0	SOLO ANEXOS, NUMEROS EMERGENCIA
1	LOCAL, CELULAR, NUMEROS EMERGENCIA
2	LOCAL, NUMEROS EMERGENCIA
3	LOCAL, CELULAR, RURAL, NUMEROS EMERGENCIA
4	LOCAL, CELULAR, RURAL, LARGA DISTANCIA NACIONAL, NUMEROS EMERGENCIA
5	LOCAL, RURAL, LARGA DISTANCIA NACIONAL E INTERNACIONAL, NUMEROS EMERGENCIA
6	LOCAL, CELULAR, RURAL, LARGA DISTANCIA NACIONAL E INTERNACIONAL, NUMEROS EMERGENCIA
7	TODAS LAS LLAMADAS

La modificación de los accesos de un anexo de acceso por ejemplo a larga distancia o celular, se hará vía correo electrónico a la cuenta soporte@muniloncoche.cl desde el correo del director o vía Ordinario o Memo dirigido a el Departamento de informática, incluyendo los siguientes datos:

- Anexo
- Código de Servicio
- Nombre del funcionario responsable de dicha línea.

Sobre las llamadas de larga distancia y celular

El director es el encargado de determinar a qué persona, por la naturaleza de sus funciones, se le dará una clave de larga distancia, celular o local, quedando esto registrado en un documento.

Existen 7 tipos de Códigos de Servicio para que se adecúen a sus necesidades:

CODIGO	SALIDAS
0	SOLO ANEXOS, NUMEROS EMERGENCIA
1	LOCAL, CELULAR, NUMEROS EMERGENCIA
2	LOCAL, NUMEROS EMERGENCIA
3	LOCAL, CELULAR, RURAL, NUMEROS EMERGENCIA
4	LOCAL, CELULAR, RURAL, LARGA DISTANCIA NACIONAL, NUMEROS EMERGENCIA
5	LOCAL, RURAL, LARGA DISTANCIA NACIONAL E INTERNACIONAL, NUMEROS EMERGENCIA
6	LOCAL, CELULAR, RURAL, LARGA DISTANCIA NACIONAL E INTERNACIONAL, NUMEROS EMERGENCIA
7	TODAS LAS LLAMADAS

Sobre el uso del Teléfono

Disposiciones Generales

Es responsabilidad de la persona a la cual se le ha asignado un aparato telefónico, o clave personal, su buen uso.

Se entiende por buen uso:

- el utilizar el teléfono como medio de comunicación para asuntos de la Organización y no personales.
- el realizar un uso medido del mismo no excediéndose en el tiempo de llamada ni en el número de llamadas
- se considera un tiempo excesivo llamadas de más de 4 minutos, siendo responsabilidad de cada director informar si un funcionario bajo su cargo por funciones propias, debe realizar llamadas con tiempos de duración mayores.
- el no permitir que personas ajenas al servicio realicen llamadas, el cuidar físicamente el aparato telefónico.

El no utilizar adecuadamente los recursos (teléfono, buzón, clave) será motivo de suspensión de los mismos. Específicamente en el caso de buzón de voz, se aplicará lo anterior, si no se accede a este servicio en un tiempo igual o mayor a 20 días o se satura el mismo.

Nota: Cualquier daño ocasionado por mal uso o descuido será responsabilidad del usuario y el departamento correspondiente absorberá los gastos generados por la reparación o reemplazo del aparato telefónico.

Sobre los Reportes de Fallas telefónicas.

El reporte de fallas se debe realizar vía correo electrónico a soporte@muniloncoche.cl o vía telefónica.

IMPORTANTE El Departamento de informática en virtud de la continuidad de los servicios y operaciones, registra los accesos a los sistemas de información o aplicaciones, por lo que las actividades de los usuarios, que no cumplan lo aquí estipulado serán informadas a los superiores jerárquicos para las acciones pertinentes.

ANEXOS

Comunicados sobre seguridad de la información

Importante comunicado sobre la seguridad de la Información y los recursos tecnológicos de la Ilustre Municipalidad de Loncoche.

1.- Sobre explotar vulnerabilidades o fallos en los Sistemas Informáticos.

La Ilustre Municipalidad de Loncoche precisa que los funcionarios no deben explorar vulnerabilidades, fallos o deficiencias en la seguridad del software para la gestión municipal, ya sea, para obtener recursos mayores a los que han sido autorizados, para tomar recursos de otros usuarios, para alterar la información que manejan los sistemas o para tener acceso a otros recursos a los cuales no se les ha otorgado una autorización apropiada. Todas estas vulnerabilidades y deficiencias deben ser reportadas inmediatamente.

2.- Sobre probar controles internos en los Sistemas Informáticos.

La I. Municipalidad de Loncoche precisa que los funcionarios no deben comprobar o intentar arreglar controles internos de los sistemas a menos que anticipadamente y por escrito haya sido específicamente aprobado por el jefe de la sección de informática.

3.- Uso del correo electrónico

El correo electrónico institucional es personal e intransferible, cada usuario mantiene su propia cuenta y está prohibido el utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo.

Los mensajes enviados por correo electrónico se consideran como una comunicación privada y directa entre el emisor y el receptor.

El usuario debe utilizar el correo electrónico exclusivamente para desempeñar las funciones que le fueron asignadas por su cargo, empleo o comisión; cualquier otro uso del correo electrónico está prohibido.

Queda prohibido suplantar, falsear o suprimir la identidad de un usuario de correo electrónico.

Queda prohibido el interceptar, revelar o ayudar a interceptar o revelar a terceros las comunicaciones por correo electrónico.

El empleo del correo electrónico considera el uso de lenguaje apropiado, evitando palabras ofensivas o altisonantes que afecten la honra y estima de terceros.

4.- Sobre la Instalación de Software

Todos los usuarios que debido a sus actividades requieran el uso de software propietario, deberán justificar el uso del mismo y solicitar la autorización a la sección de Informática a través de un oficio firmado por el Director de la unidad del usuario, indicando en que equipo o equipos (de existir varias licencias adquiridas) deberá instalarse el programa en cuestión.

La instalación de cualquier tipo de programa en computadores, servidores o cualquier otro equipo conectado a la red sin la autorización de la sección de Informática está prohibida.

5.- Uso de medios de almacenamiento masivo (USB, Tarjetas de Memoria, DVD, etc.)

La información constituye uno de los principales activos de la institución, por tanto, el manejo adecuado de la misma es responsabilidad de todos los funcionarios, así como la correcta utilización de los dispositivos que el mercado ofrece para la administración y respaldo de información. Por lo tanto, todos los usuarios de tecnologías de información que manipulen dispositivos como: CD, DVD, USB, discos duros externos, entre otros, deben utilizarlos considerando la importancia de la información que contienen, buscando mecanismos seguros para su almacenamiento o distribución.