ESCUELA POLITECNICA DEL EJERCITO

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

PLAN MAESTRO DE SEGURIDAD INFORMATICA PARA EL MINISTERIO PUBLICO DEL ECUADOR

Previa la obtención del Título de:

INGENIERO DE SISTEMAS E INFORMATICA

POR: LUIS ESTALIN CORTEZ CARTAGENA

SANGOLQUI, OCTUBRE DE 2005

CERTIFICACION

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. LUIS ESTALIN CORTEZ CARTAGENA como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS.

Quito, 31 de octubre del 2005

Dr. Vinicio Carrera	**Dr. Jaime Almeida**
DIRECTOR	**CODIRECTOR**

DEDICATORIA

El presente trabajo se lo dedico a mi Madre Emma Cartagena, mi Esposa Sandra Ayala, mi hija Nicole Cortez y mi hijo Sebastián Cortez, por la confianza, apoyo y amor que me han brindado.

Luis Estalin Cortez Cartagena

INDICE DE CONTENIDOS

SOBRE LA TESIS ____ *1*
OBJETIVO GENERAL ____ 1
OBJETIVOS ESPECIFICOS ____ 1
ALCANCE ____ 1
JUSTIFICACIÓN E IMPORTANCIA ____ 2

CAPITULO I ____ *3*

INFORME DE RELEVAMIENTO ____ *3*

1 - RELEVAMIENTO DE LA SEGURIDAD FÍ SICA ____ 6
1.1 EQUIPAMIENTO ____ 6
1.2 ACCESO FÍSICO AL CENTRO DE CÓMPUTO ____ 11
1.3 ACCESO FÍSICO A EQUIPOS ____ 11
1.4 ESTRUCTURA Y ACCESO A LOS EDIFICIOS ____ 12
1.5 DISPOSITIVOS DE SOPORTE ____ 14

2 - RELEVAMIENTO DE LA ADMINISTRACIÓN DEL CENTRO DE CÓMPUTO ____ 15
2.1 ADMINISTRACIÓN DEL CENTRO DE CÓMPUTO ____ 15
2.2 CAPACITACIÓN DE USUARIOS ____ 18
2.3 RESPALDO (BACKUP) ____ 19
2.4 DOCUMENTACION ____ 19

3 - RELEVAMIENTO DE LA SEGURIDAD DE LAS APLICACIONES ____ 21
3.1 SOFTWARE ____ 21
3.2 SEGURIDAD DE BASES DE DATOS ____ 22
3.3 CONTROL DE APLICACIONES EN ESTACIONES DE TRABAJO ____ 22
3.4 CONTROL DE DATOS EN LAS APLICACIONES ____ 25
3.5 CICLO DE VIDA DE LAS APLICACIONES ____ 25

4 - RELEVAMIENTO DE LA SEGURIDAD LÓGICA ____ 27
4.1 IDENTIFICACIÓN DE USUARIOS ____ 27
4.2 AUTENTICACIÓN DE LOS USUARIOS ____ 30
4.3 CONTRASEÑAS ____ 30
4.4 SEGREGACIÓN DE FUNCIONES ____ 31

5 - RELEVAMIENTO DE LA SEGURIDAD DE LAS COMUNICACIONES ____ 32
5.1 TOPOLOGÍA DE RED ____ 32
5.2 CONEXIONES EXTERNAS ____ 41
5.3 CONFIGURACIÓN LÓGICA DE RED ____ 42
5.4 MAIL ____ 43
5.5 ANTIVIRUS ____ 44
5.6 FIREWALL ____ 46

CAPÍTULO II ____ *47*

VULNERABILIDADES Y CONSECUENCIAS ____ *47*

1- VULNERABILIDADES DE LA SEGURIDAD FÍSICA ____ 47

2- VULNERABILIDADES DE LA ADMINISTRACIÓN DEL CENTRO DE CÓMPUTO **51**

3- VULNERABILIDAD DE LA SEGURIDAD DE LAS APLICACIONES **54**

4- VULNERABILIDADES DE LA SEGURIDAD LOGICA **55**

5- VULNERABILIDAD EN LA SEGURIDAD DE LAS COMUNICACIONES **58**

ANÁLISIS DE RIESGOS ***60***

1 - ACTIVOS **60**

2 - FACTORES DE RIESGO **61**

3- ACTIVOS POSIBLES CONSECUENCIAS Y MEDIDAS EXISTENTES **64**

4- ACTIVOS Y PROBABILIDAD DE OCURRENCIA **86**

CAPITULO III ***98***

PLAN MAESTRO DE SEGURIDAD ***98***

GENERALIDADES ***98***

1 - SEGURIDAD FÍSICA **101**
1.1 EQUIPAMIENTO 101
1.2 CONTROL DE ACCESO FÍSICO AL CENTRO DE COMPUTO 103
1.3 CONTROL DE ACCESO A EQUIPOS 104
1.4 DISPOSITIVOS DE SOPORTE 105

2 - ADMINISTRACIÓN DEL CENTRO DE COMPUTO **107**
2.1 ADMINISTRACIÓN DEL CENTRO DE COMPUTO 107
2.2 CAPACITACIÓN 110
2.3 RESPALDO 110
2.4 DOCUMENTACIÓN 112

3 - SEGURIDAD DE LAS APLICACIONES **114**
3.1 SOFTWARE DE SERVIDORES 114
3.2 SEGURIDAD DE BASES DE DATOS 116
3.3 CONTROL DE APLICACIONES EN ESTACIONES DE TRABAJO 119
3.4 CONTROL DE DATOS EN LAS APLICACIONES 122
3.5 CICLO DE VIDA DE LAS APLICACIONES 122

4 - SEGURIDAD LÓGICA **125**
4.1 ASPECTOS GENERALES 125
4.2 IDENTIFICACION DE USUARIOS 127
4.3 AUTENTICACIÓN 130
4.4 CONTRASEÑAS (PASSWORDS) 130
4.5 POLITICAS DE DOMINIO Y UNIDADES ORGANIZACIONALES 132
4.6 SEGREGACIÓN DE FUNCIONES 135

5 - SEGURIDAD DE COMUNICACIONES **136**
5.1 ASPECTOS GENERALES 136
5.2 CABLEADO ESTRUCTURADO 137
5.3 USO DE LOS SISTEMAS DE COMUNICACIÓN 139
5.4 TOPOLOGÍA DE RED 140
5.5 CONEXIONES EXTERNAS 140

5.6 CONFIGURACIÓN LÓGICA DE RED 142
5.7 MAIL 143
5.8 ANTIVIRUS 145
5.9 FIREWALL 145
5.10 ATAQUES DE RED 146
5.11 SISTEMAS ANTIINTRUSOS 147

6 - AUDITORÍAS Y REVISIONES 148
6.1 CHEQUEOS DEL SISTEMA 148
6.2 RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD 149
6.3 AUDITORÍAS DE REDES 150

7- PLAN DE CONTINGENCIAS 152
7.1 PLAN DE ADMINISTRACIÓN DE INCIDENTES 152
7.2 RESPALDO DE EQUIPAMIENTO 152
7.3 ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES 153

CAPITULO IV 156

PLAN DE CONTINGENCIAS 156

OBTETIVOS 156

1- PLAN DE EMERGENCIAS 157
1.1 ORGANIZACIÓN GENERAL ANTE EMERGENCIAS 157
1.2 ORGANIZACIÓN DEL SISTEMA DE CONTROL DE EMERGENCIAS 158

2- PLAN DE RECUPERACIÓN 158
2.1 CENTROS DE CÓMPUTO ALTERNATIVOS 158
2.2 FUNCIONES DE LOS MIEMBROS DE LA ORGANIZACIÓN PARA LAS CONTINGENCIAS 159
2.3 ACCIONES A TOMAR EN EL CENTRO DE CÓMPUTO ALTERNATIVO 161
2.4 PLAN DE RESPALDOS 161
2.5 ACCIONES A TOMAR EN EL CENTRO DE CÓMPUTO DE LA EMERGENCIA 162
2.6 SISTEMAS CRITICOS 163
2.7 FUNCIONARIOS RESPONSABLES DEL PLAN DE CONTINGENCIAS 164
2.8 DIRECTORIO PARA LLAMADAS DE EMERGENCIA (Autoridades del Ministerio Público) 164
2.9 DIRECTORIO PARA LLAMADAS DE EMERGENCIA (Notificación Externa) 165

3- SIMULACIÓN DEL PLAN DE CONTINGENCIAS 165

4- MANTENIMIENTO DEL PLAN DE CONTINGENCIAS 165

CONCLUSIONES 167

RECOMENDACIONES 169

BIBLIOGRAFIA 175

ANEXO 1 176

ANEXO 2 180

*ANEXO 3*_____*180*

LISTADO DE TABLAS

Tabla 2.1: (Listado de activos) 60

Tabla 2.2: (Factores de riesgo) 61

LISTADO DE CUADROS

Cuadro 2.1: (Activos y factores de riesgos) 65
Cuadro 2.2: (Activos y factores de riesgos) 66
Cuadro 2.3: (Activos y factores de riesgos) 67
Cuadro 2.4: (Activos y factores de riesgos) 68
Cuadro 2.5: (Activos y factores de riesgos) 69
Cuadro 2.6: (Activos y factores de riesgos) 70
Cuadro 2.7: (Activos y factores de riesgos) 71
Cuadro 2.8: (Activos y factores de riesgos) 72
Cuadro 2.9: (Activos y factores de riesgos) 73
Cuadro 2.10: (Activos y factores de riesgos) 74
Cuadro 2.11: (Activos y factores de riesgos) 75
Cuadro 2.12: (Activos y factores de riesgos) 76
Cuadro 2.13: (Activos y factores de riesgos) 77
Cuadro 2.14: (Activos y factores de riesgos) 78
Cuadro 2.15: (Activos y factores de riesgos) 79
Cuadro 2.16: (Activos y factores de riesgos) 80
Cuadro 2.17: (Activos y factores de riesgos) 81
Cuadro 2.18: (Activos y factores de riesgos) 82
Cuadro 2.19: (Activos y factores de riesgos) 84
Cuadro 2.20: (Activos y factores de riesgos) 85
Cuadro 2.21: (Activos y factores de riesgos) 85
Cuadro 2.22: (Activos, factores de riesgo y probabilidad de ocurrencia) 86
Cuadro 2.23: (Activos, factores de riesgo y probabilidad de ocurrencia) 87
Cuadro 2.24: (Activos, factores de riesgo y probabilidad de ocurrencia) 87
Cuadro 2.25: (Activos, factores de riesgo y probabilidad de ocurrencia) 88
Cuadro 2.26: (Activos, factores de riesgo y probabilidad de ocurrencia) 88
Cuadro 2.27: (Activos, factores de riesgo y probabilidad de ocurrencia) 89
Cuadro 2.28: (Activos, factores de riesgo y probabilidad de ocurrencia) 89
Cuadro 2.29: (Activos, factores de riesgo y probabilidad de ocurrencia) 90
Cuadro 2.30: (Activos, factores de riesgo y probabilidad de ocurrencia) 90
Cuadro 2.31: (Activos, factores de riesgo y probabilidad de ocurrencia) 91
Cuadro 2.32: (Activos, factores de riesgo y probabilidad de ocurrencia) 91
Cuadro 2.33: (Activos, factores de riesgo y probabilidad de ocurrencia) 92
Cuadro 2.34: (Activos, factores de riesgo y probabilidad de ocurrencia) 92

Cuadro 2.35: (Activos, factores de riesgo y probabilidad de ocurrencia) 93
Cuadro 2.36: (Activos, factores de riesgo y probabilidad de ocurrencia) 93
Cuadro 2.37: (Activos, factores de riesgo y probabilidad de ocurrencia) 94
Cuadro 2.38: (Activos, factores de riesgo y probabilidad de ocurrencia) 94
Cuadro 2.39: (Activos, factores de riesgo y probabilidad de ocurrencia) 95
Cuadro 2.40: (Activos, factores de riesgo y probabilidad de ocurrencia) 96
Cuadro 2.41: (Activos, factores de riesgo y probabilidad de ocurrencia) 96
Cuadro 2.42: (Activos, factores de riesgo y probabilidad de ocurrencia) 97
Cuadro 4.1: (Funcionarios responsables del Plan de Contingencias) 164
Cuadro 4.2: (Directorio interno, para llamadas de emergencia) 164
Cuadro 4.3: (Directorio externo, para llamadas de emergencia).....165

LISTADO DE FIGURAS

Figura 4.1: (Organización del sistema control de emergencias) 158

SOBRE LA TESIS

OBJETIVO GENERAL

Proponer el Plan de Seguridad Informática, para el Ministerio Público del Ecuador.

OBJETIVOS ESPECIFICOS

Proponer un conjunto de normas y procedimientos para el Ministerio Público del Ecuador, que permitan garantizar la integridad, confidencialidad y disponibilidad de la información.

Optimizar los controles de seguridad para proteger la información la información.

Determinar las medidas que regulen el uso del Internet.

Recomendar los requerimientos de hardware y de software necesarios para la implementación de políticas de seguridad.

Proponer un plan de contingencias y recuperación de desastres.

Impulsar la toma de conciencia de seguridad informática en los usuarios.

ALCANCE

- Asegurar la información y los bienes informáticos tanto de hardware como de software, contra posibles intrusos internos o externos.
- Comprometer a todas las autoridades y funcionarios del Ministerio Público para difundir las normas que se establecerán en los diferentes niveles jerárquicos.
- Evitar accesos no autorizados.
- Proteger la integridad de la información.

- Eliminar la posibilidad de ataques a los distintos tipos de servidores.
- Garantizar la continuidad del servicio de Internet.
- Planificar las acciones y procedimientos destinados a mantener la continuidad de la actividad de la Institución en situaciones de desastre.
- Recuperar en el menor tiempo y al menor costo posible, la continuidad de las actividades en caso de que sean interrumpidas por una emergencia.
- Evitar la pérdida de información sensible o importante.

JUSTIFICACIÓN E IMPORTANCIA

Una gran dotación de estaciones de trabajo, sumada a una nueva infraestructura física y nuevos recursos tecnológicos como conexiones a Internet, cableado estructurado y nuevos requerimientos de comunicación de la información han creado la necesidad imperiosa para la Institución, de implementar un **Plan de Seguridad Informática.**

El propósito de establecer el Plan de Seguridad Informática para el Ministerio Público es determinar la tecnología que se requiere, los procesos que intervienen y el conocimiento que el personal técnico debe poseer, para proteger la información y los activos de la Institución, pretendiendo conseguir confidencialidad, integridad y disponibilidad de la información; como también definir las responsabilidades que debe asumir cada uno de los funcionarios mientras permanezcan en la Institución.

CAPITULO I

INFORME DE RELEVAMIENTO

MINISTERIO PUBLICO DEL ECUADOR

El Ministerio Público es una Institución gubernamental cuyo ámbito de funcionamiento es el campo de la justicia penal.

El Ministerio Público cuenta con aproximadamente 1000 funcionarios a nivel nacional, distribuidos en los Ministerios Fiscales Distritales de cada una de las provincias del Ecuador.

En Quito el Ministerio Público cuenta con dos edificios, el primero es el Edificio Tocuyo en el cual funciona el Ministerio Fiscal General, el segundo es el Edificio Roca en el cual funciona la parte administrativa del Ministerio Fiscal General y el Ministerio Fiscal Distrital de Pichincha.

La estructura jerárquica de la Institución se presenta en el siguiente organigrama.

El informe de relevamiento comprende fundamentalmente la planificación y ejecución de los siguientes aspectos:

1. Relevamiento de la seguridad física.
2. Relevamiento de la administración del centro de cómputo.
3. Relevamiento de la seguridad de las aplicaciones.
4. Relevamiento de la seguridad lógica.
5. Relevamiento de la seguridad en las comunicaciones.

ORGANIGRAMA |INISTERIO PUBLICO

1 - RELEVAMIENTO DE LA SEGURIDAD FÍ SICA

OBJETIVO

Evaluar el centro de cómputo, los equipos, los dispositivos, los medios de almacenamientos y las personas que conforman el área de sistemas, así como lo relativo a la infraestructura física y al mantenimiento de los recursos de la organización.

1.1 EQUIPAMIENTO

1.1.1 EQUIPAMIENTO CENTRO DE COMPUTO EDIFICIO TOCUYO

Características físicas:

- Puerta de seguridad.
- Piso falso de metal.
- Cielo raso.
- Extintor de incendios.

Equipamiento:

- Rack abierto de voz y datos.
- Sistema de precisión de aire acondicionado.
- Central telefónica.

- Servidor-1: Compaq Proliant ML570, adquirido en el año 2001. El servidor se desempeña como servidor multifunción y contiene las siguientes características técnicas:
    - 1 Procesador Pentium III xeon de 700 MHz
    - 3 Fuentes de poder (redundantes)
    - 2 Tarjetas de red (redundantes)
    - 1.56 GB de memoria RAM.
    - 3 discos con tecnología SCSI con 9 GB de capacidad cada uno.
    - Unidad de cd writer y unidad de disquete.
    - Sistema operativo Windows 2000 Advanced Server.

1.1.2 EQUIPAMIENTO CENTRO DE CÓMPUTO EDIFICIO ROCA

Características físicas:

- El piso de madera.
- Puerta y paredes de vidrio.
- Todo el vidrio que se encuentra instalado, no es vidrio de seguridad.
- No posee piso falso.
- No posee cielo raso.
- No existe ningún sistema de alarmas ni vigilancia.
- No posee un sistema de control de incendios.

Equipamiento:

- Rack 1 abierto de voz.

- Rack 2 abierto de datos.
- Sistema de precisión de aire acondicionado.
- Central telefónica.
- UPS, capaz de soportar todo el equipamiento del backbone.
- Servidor-2: Compaq Proliant ML570, adquirido en el año 2001. El servidor se desempeña como servidor antivirus, servidor de impresión y contiene las siguientes características técnicas:
    - 1 Procesador Pentium III xeon de 700 MHz
    - 3 Fuentes de poder (redundantes)
    - 2 Tarjetas de red (redundantes)
    - 2.56 GB de memoria RAM.
    - 3 discos con tecnología SCSI con 9 GB de capacidad cada uno.
    - Unidad de cd writer y unidad de disquete.
    - Sistema operativo Windows 2000 Advanced Server.

- Servidor-3: Compaq HP ML370 de segunda generación, adquirido en el año 2003. El servidor se desempeña como servidor de correo, de aplicaciones, de dominio y contiene las siguientes características:
    - 1 Procesador Pentium III
    - 1 Fuentes de poder (no posee fuentes redundantes)
    - 2 Tarjetas de red (redundantes)
    - 3 GB de memoria RAM.
    - 3 discos con tecnología SCSI con 9 GB de capacidad cada uno.
    - Unidad de cd writer y unidad de disquete.
    - Sistema operativo Windows 2003 Estándar.

- Estación de trabajo configurada para administración de la central telefónica.

1.1.3 ESTACIONES DE TRABAJO

La Institución en el edificio Tocuyo posee alrededor de 50 estaciones de trabajo de las cuales un 80% se encuentran conectadas a la red. Entre las estaciones de trabajo existen computadores de marca y clones con variadas versiones de sistemas operativos, desde Windows 95, Windows 98, Windows Millenium, Windows 2000 profesional, Windows XP Home Edition hasta Windows XP Profesional.

En lo referente al mantenimiento de las estaciones de trabajo, analistas de la misma institución se encargan de dar mantenimiento, sin embargo las autoridades de la Dirección Nacional de Informática tienen la inclinación de contratar los servicios de una empresa para que realice estas funciones.

Así también la Institución cuenta con aproximadamente 150 estaciones de trabajo en el edificio Roca de las cuales un 90% se encuentran conectadas a la red. Entre las estaciones de trabajo existen computadores de marca y clones con variadas versiones de sistemas operativos, desde Windows 95, Windows 98, Windows Millenium, Windows 2000 profesional, Windows XP Home Edition hasta Windows XP Profesional.

1.1.4 IMPRESORAS DE RED

En total existen 37 impresoras de red, 5 en el edificio Tocuyo una por cada piso y las restantes 32 se encuentran instaladas en el edificio Roca.

Un 90% de las impresoras tienen las siguientes características técnicas:

- Bandeja de papel de 250 hojas
- Impresión de 25 hojas por minuto en tamaño carta y 24 páginas por minuto en tamaño A4.
- Full duplex automático (impresión en ambos lados).
- Resolución de 1200 x 1200 ppp.
- 10/100 Base-TX.
- 48 MB de memoria.
- Puerto USB y puerto paralelo.

El 10% restante posee las siguientes características técnicas:

- Bandeja de papel de 250 hojas
- Impresión de 20 hojas por minuto en tamaño carta y 19 páginas por minuto en tamaño A4.
- Full duplex manual.
- Puerto USB.
- Resolución de 1200 x 1200 ppp.
- 10/100 Base-TX.

1.2 ACCESO FÍSICO AL CENTRO DE CÓMPUTO

El centro de cómputo del edificio Tocuyo es una oficina totalmente independiente y se encuentra ubicada en la planta baja, no existe personal de la Dirección Nacional de Informática, que labore permanentemente en esa oficina.

El centro de cómputo del Edificio Roca se encuentra ubicado en el quinto piso, en el interior de las oficinas de la Dirección Nacional de Informática.

Los únicos funcionarios que tienen acceso **permitido a cualquiera de los centros de cómputo,** trabajan en la Dirección Nacional de Informática.

En caso de que cualquier **persona ajena a la Institución** necesite realizar una tarea de mantenimiento relativa al centro de cómputo, deberá anunciarse con la secretaría o coordinar con cualquier persona de la dirección. Luego de eso un funcionario de la dirección será el encargado de escoltarlo y acompañarlo durante el transcurso de su tarea, hasta que sea concluida.

1.3 ACCESO FÍSICO A EQUIPOS

En lo referente a las estaciones de trabajo, los equipos son entregados individualmente a cada usuario mediante actas de asignación de bienes. Por lo tanto son los únicos autorizados a utilizarlos.

Los equipos son revisados únicamente ante fallas reportadas por los usuarios. Por lo tanto no se realizan **controles periódicos** sobre los dispositivos de hardware instalados.

Un 70% de los equipos de la Institución disponen de **disqueteras y lectoras de CD**. Estos **dispositivos** están habilitados y no hay ningún control sobre ellos.

En cuanto se refiere a dispositivos y periféricos que posee la Dirección Nacional de Informática todos se encuentran fuera del alcance de cualquier otro usuario o personal de limpieza.

En el edificio Roca haciendo referencia a los gabinetes donde se ubican los switches de cada una de las unidades, están cerrados con llave, para evitar que el personal de limpieza o cualquier otra persona manipule los equipos. Las llaves de todos los gabinetes se encuentran situados en la Dirección Nacional de Informática en poder del analista que administra los racks y gabinetes.

1.4 ESTRUCTURA Y ACCESO A LOS EDIFICIOS

El edificio Tocuyo cuenta con la siguiente estructura:

- 4 pisos, planta baja y parqueadero.
- En todos los pisos existen divisiones modulares, para distribuir los espacios y ordenar los puestos de trabajo.

- Un 90% de los pisos son alfombrados.
- Existe un elevador.
- Existen escaleras peatonales.
- No existen escaleras exteriores para evacuar en caso de emergencia.
- No existen extintores de incendio en ningún lugar del edificio.

El edificio Roca cuenta con la siguiente estructura:

- 10 pisos, planta baja y parqueadero.
- Aproximadamente en un 50% del edifico existen divisiones modulares, para distribuir los espacios y ordenar los puestos de trabajo.
- Un 95% de los pisos son de madera el resto son de alfombra.
- Existen dos elevadores.
- Existen escaleras peatonales.
- No existen escaleras exteriores para evacuar en caso de emergencia.
- No existen extintores de incendio en ningún lugar del edificio.

La seguridad de los dos edificios es controlada por Policías Nacionales, ubicados en la planta baja, quienes vigilan únicamente el control del ingreso a las oficinas.

Todo el público tiene acceso libre a cualquier dependencia, no existe ninguna restricción de ingreso a ninguna de las áreas de los edificios.

En horarios no laborables, y en fines de semana o feriados, cualquier funcionario de la Institución puede ingresar a las instalaciones sin ninguna autorización previa.

1.5 DISPOSITIVOS DE SOPORTE

En la Institución se disponen de los siguientes **dispositivos para soporte** del equipamiento informático:

- **Generador de energía**: cuando el flujo normal de energía falle el Ministerio Público cuenta con generadores propios tanto en el edifico Tocuyo como en el edifico Roca, para evitar que se paralicen las actividades por largos espacios de tiempo. Debido a los escasos cortes de energía, pocas veces se han utilizado estos generadores.

- **UPS**: en el centro de cómputo del edifico Roca, existe un UPS que permite mantener funcionando todos los equipos de comunicaciones y servidores que se encuentran en el centro de cómputo y los dos gabinetes. El tiempo de respaldo es de aproximadamente de 30 minutos.

- **Descarga a tierra**: se construyó una malla en el parqueadero del edificio Roca para descarga a tierra, el circuito de instalaciones eléctricas que sirve exclusivamente al equipo computacional se conecta a esta malla para protección de los equipos.

2 - RELEVAMIENTO DE LA ADMINISTRACIÓN DEL CENTRO DE CÓMPUTO

2.1 ADMINISTRACIÓN DEL CENTRO DE CÓMPUTO

2.1.1 RESPONSABILIDAD DE LOS FUNCIONARIOS DE LA DIRECCIÓN NACIONAL DE INFORMÁTICA

La Dirección Nacional de Informática esta conformada por: el Director Nacional de Informática, un Jefe de Desarrollo de Sistemas dos analistas y una secretaria.

No existen responsabilidades puntuales asignadas a cada funcionario, tampoco existe un encargado para el control de la seguridad. Todos realizan de todo, por ejemplo desarrollo de aplicaciones, mantenimiento de software, mantenimiento de hardware, soporte al usuario, administración de cuentas de usuarios, etc.

2.1.2 PLANES DE SISTEMAS

Parte del Plan Estratégico del Ministerio Público es el Plan Estratégico de Informática. El cronograma de ejecución es de enero del 2002 a diciembre del 2005 y consta con la siguiente planificación:

- Renovación del equipo informático y telecomunicaciones

- Automatización de la información Local, Regional y Nacional.
- Establecer un programa de información gerencial como soporte para la toma de decisiones en las principales áreas.
- Implementar el Sistema de automatización del Ministerio Público.

2.1.3 IMPORTANCIA DE LA SEGURIDAD

Todo funcionario de la Dirección Nacional de Informática tiene plena conciencia de la importancia de la seguridad en la Institución, ya que son los nuevos lineamientos que se han venido implementando. Los demás funcionarios de la Institución recién están asimilando las nuevas políticas y adaptándolas a su trabajo diario.

2.1.4 MANTENIMIENTO

- **Solicitud de mantenimiento:** cada vez que un usuario requiere el asesoramiento o ayuda se comunica telefónicamente con cualquiera de las extensiones de la Dirección Nacional de Informática, si es posible se soluciona el problema vía telefónica, caso contrario se acude al puesto de trabajo. Cada una de las peticiones de asistencia realizadas, son registradas en una hoja de control de asistencia técnica. De esta manera queda constancia de las tareas desarrolladas por los funcionarios de la Dirección y

de las solicitudes de los usuarios. Este registro se podrá utilizar además para realizar estadísticas de atención al usuario, tipos de peticiones, tiempo de asistencia, etc.

- **Mantenimiento preventivo:** por el momento no se realiza mantenimiento preventivo de las estaciones de trabajo, pero si se realiza mantenimiento a ciertos dispositivos estratégicos como impresoras y servidores.
- **Inventario:** No existe un inventario completo de hardware ni de software con suficientes detalles, como para determinar que software pertenece a cada equipo o determinar estadísticamente tipo de equipo, sistemas operativos, aplicaciones instaladas, tipos de acceso, etc. Tampoco existe un procedimiento formal para rotular o identificar a cada equipo.

2.1.5 INSTALADORES

Los instaladores de las aplicaciones utilizadas en la Institución se encuentran en CD's originales almacenados en un armario del centro de cómputo.

Los instaladores de uso más frecuente como versiones de Windows, antivirus y otras aplicaciones se ejecutan desde copias de los CD's originales[1], para evitar posibles daños o pérdidas de los medios originales.

[1] El artículo 30 en su literal a), de la Ley de Propiedad Intelectual, faculta faculta a quien ha adquirido un programa de ordenador a reproducir una copia con fines de seguridad o resguardo. Ver texto de la ley en el anexo 3.

2.1.6 LICENCIAS

Como se enunció anteriormente en la Dirección Nacional de Informática se encuentran las licencias de los programas instalados en las estaciones de trabajo y servidores como son:

- Windows en diferentes versiones.
- Microsoft Office en diferentes versiones.
- Winzip.
- Norton Antivirus corporativo en diferentes versiones.
- Entre otros.

También se poseen aplicaciones propietarias y aplicaciones gratuitas que no requieren licenciamiento.

2.2 CAPACITACIÓN DE USUARIOS

La capacitación de parte de la Dirección Nacional de Informática hacia el resto de funcionarios de la Institución ha sido muy pobre en lo que se refiere a las políticas nuevas que se están implementado, las políticas únicamente han sido aplicadas y se han realizado breves explicaciones de los cambios realizados en el sistema.

2.3 RESPALDO (BACKUP)

- **Respaldo de datos y configuración del servidor:** por el momento no se está realizando respaldos de la configuración de los servidores, ni respaldo de la información que contienen, se han solicitado los dispositivos para obtener los respaldos pero ha habido inconvenientes con los proveedores que no han cumplido con los pedidos.

- **Respaldo de las estaciones de trabajo:** los usuarios han sido instruidos para que almacenen todos los datos en la carpeta Mis Documentos.

- **Respaldo de los logs:** no se realiza respaldo total de los logs generados, son leídos y se respalda aquellos que se consideran importantes, el resto es eliminado para que se sobrescriban.

2.4 DOCUMENTACION

2.4.1 DOCUMENTACIÓN DEL CENTRO DE CÓMPUTO

En el centro de cómputo se posee la siguiente documentación:

- Licencias del software.
- Registro de red.

- Registro de la central telefónica.
- Planos del cableado estructurado y cableado eléctrico.
- Número de IP fijos, de impresoras de red, switches y lector biométrico

2.4.2 MANUALES

Los siguientes manuales están almacenados en la Dirección Nacional de Informática:

- Manuales de equipamiento como impresoras, servidores, estaciones de trabajo, UPS, etc.
- Manuales técnicos de software.
- Manuales con estándares para el desarrollo de aplicaciones.
- Manuales de usuario de las aplicaciones desarrolladas en la Institución.

3 - RELEVAMIENTO DE LA SEGURIDAD DE LAS APLICACIONES

OBJETIVO

Evaluar la seguridad de las aplicaciones utilizadas en la Institución, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento.

3.1 SOFTWARE

La Institución cuenta con servidores de plataforma Windows, los servidores 1 y 2 con sistema operativo Windows 2000 Advanced Server y el servidor-3 con sistema operativo Windows 2003 estándar; se ha mantenido la misma plataforma por las siguientes razones:

- Alto grado de confiabilidad.
- Interoperatibilidad.
- Compatibilidad con el resto de versiones de sistemas operativos Windows existentes en la Institución.
- Usuarios están muy familiarizados con la plataforma Windows.
- Soporte técnico y capacitación especializada.

3.2 SEGURIDAD DE BASES DE DATOS

La Institución cuenta con aplicaciones desarrollas y adquiridas en SQL server 2000.

Existen controles lógicos que restringen el acceso a las bases de datos, de esta manera obtienen acceso exclusivamente los funcionarios que manejan los sistemas, además como se explicó anteriormente también existen controles de seguridad física a los servidores.

Los únicos funcionarios que tienen autorización de uso y modificación de los archivos de las bases de datos son los administradores y programadores.

Se controla además en las aplicaciones que los registros eliminados solo sean marcados como borrados y no sean borrados físicamente de los registros de las bases de datos.

3.3 CONTROL DE APLICACIONES EN ESTACIONES DE TRABAJO

Solamente los funcionarios de la Dirección Nacional de Informática son los encargados y autorizados de realizar **instalaciones de software** en las estaciones de trabajo, sin embargo esta premisa no se ha cumplido cabalmente, puesto que gran cantidad de usuarios han instalado y modificado el software que poseen sus computadores sin autorización alguna. Esto se debía a que anteriormente los

usuarios con sistemas operativos como Windows 2000 y Windows XP técnicamente tenían todos los privilegios que el sistema operativo les brinda sobre sus estaciones de trabajo.

Actualmente las estaciones de trabajo que han ingresado a la red del Ministerio Público han sido depuradas de tal manera que cada una posee una cuenta de administrador y una cuenta de usuario, validadas por un nombre de usuario y una contraseña. La cuenta de administrador es manejada por los funcionarios de la Dirección Nacional de Informática y posee todos los privilegios y permisos que el sistema operativo les brinda, en cambio la cuenta de usuario es usada por el funcionario a cargo y es una cuenta limitada, en el sentido principalmente de no poder instalar software alguno, aunque con los suficientes permisos para usar todo el software instalado y para almacenar y modificar su propia información.

A la par de realizar estas configuraciones, se evaluó cada equipo con la finalidad de que cada uno cuente con el software original y únicamente con el software licenciado que le pertenece. Todavía un porcentaje mínimo de estaciones de trabajo permanece sin realizar estas auditorias, la meta es realizar estos procedimientos en el ciento por ciento de las estaciones de trabajo.

En sistemas operativos como Windows 98, Windows 95 no se pueden efectuar las configuraciones antes mencionadas, aunque se realizó la misma evaluación de software de cada una de las estaciones de trabajo antes de ingresarlas en la red.

No existen **estándares** definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la **instalación y actualización** de la configuración de las estaciones de trabajo. Sin embargo, en todos los computadores se encuentran instalados, el sistema operativo que viene preinstalado de fábrica, el Microsoft Office, el Norton Antivirus y los sistemas adquiridos o desarrollados por la Institución, en algunos casos el sistema legal, así también para quien lo requiere se da el acceso a las aplicaciones de las áreas jurídicas y/o administrativo-financieras.

En el caso de que una estación de trabajo presente errores en su configuración, se trata de reparar a toda costa el sistema operativo, con las propias opciones que prestan las diferentes versiones. Si el caso lo amerita se procede a formatear el disco duro y a reinstalar todos los programas.

Se realizan actualizaciones de software, especialmente del sistema operativo, del Microsoft Office y todos los productos de Microsoft.

En lo referente a los servidores, no se documenta ni se guardan las configuraciones del servidor, tampoco se guarda configuraciones anteriores a cualquier cambio, para restaurar el sistema en caso de fallos.

3.4 CONTROL DE DATOS EN LAS APLICACIONES

Quienes utilizan las aplicaciones desarrolladas o adquiridas tienen exclusivos permisos para el ingreso, modificación e impresión de la información únicamente del sistema sobre el cual tienen autorización.

El servidor-2, es un servidor de tiempo, lo que le permite sincronizar la fecha y hora de cada una de las estaciones de trabajo. De esta manera se logra que los logs y los datos ingresados en los sistemas se generen con la fecha del servidor.

3.5 CICLO DE VIDA DE LAS APLICACIONES

La Institución cuenta con pocas **aplicaciones propias** desarrolladas por el departamento de desarrollo de sistemas. Este desarrollo sigue una metodología estándar basada en estándares IEEE 830.

Análisis: el procedimiento es iniciar con una entrevista con el usuario final, recabando la información necesaria para obtener los requerimientos iniciales y luego proceder con el desarrollo de la aplicación que se requiera.

Desarrollo: la implementación de las aplicaciones se las realiza en Visual Fox 5.0 y en Visual Basic, se tiene mucho interés en empezar a desarrollar aplicaciones en Visual Basic Dot Net.

Prueba: para probar las aplicaciones se generan casos de prueba, donde se definen tablas con valores de entrada y de salida a las aplicaciones.

Cuando se hagan modificaciones en los programas fuente, los casos de prueba que se usen sobre el software modificado deberán ser los mismos que se usaron antes, de manera de comprobar que los valores obtenidos en las últimas pruebas sean los mismos que los que surgieron de las primeras.

Instalación y modificación: una vez hecha la instalación, las únicas modificaciones que se realizan son a pedido del usuario final a través de su director o jefe de unidad. No se lleva a cabo ningún control de versiones ni gestión de configuración de las modificaciones.

Documentación: en lo posible cada aplicación posee un manual de usuario, en la actualidad se están confeccionando los manuales de usuario de algunas de las aplicaciones que han sido desarrolladas y no se posee su documentación.

Terceros: la Institución ha adquirido varias aplicaciones, especialmente para las áreas administrativo y financieras, en este caso la empresa contratada se encarga de dar la capacitación a los usuarios finales y del soporte que se requiera en el momento que se solicite. Adicionalmente las empresas contratadas deben realizar la instalación del software adquirido en las estaciones de trabajo y en el servidor de aplicaciones.

4 - RELEVAMIENTO DE LA SEGURIDAD LÓGICA

OBJETIVO

Evaluar los controles de acceso de los usuarios a los recursos informáticos y a los datos que se producen en las aplicaciones desarrolladas, con el fin de señalar las irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información.

4.1 IDENTIFICACIÓN DE USUARIOS

4.1.1 INGRESO DE USUARIOS A LA RED (ALTAS)

La asignación, creación y modificación de las cuentas de usuario de la red, es administrada por los funcionarios de la Dirección Nacional de Informática.

La creación o modificación de las cuentas de usuarios de la red, se basa en la necesidad de cada unidad operativa o de apoyo.

Cuando en una unidad a un usuario se le ha asignado una estación de trabajo, el Jefe departamental o Director de la unidad solicita el ingreso en la red del usuario a la Dirección de Informática, donde se genera el alta en el sistema. Los datos que se requieren son nombres y apellidos y unidad a la que pertenece.

4.1.2 SALIDA DE USUARIOS DE LA RED (BAJAS)

Las cuentas de los usuarios que no se utilizan no son eliminadas del sistema, solo son deshabilitadas. De esta forma se mantiene un registro de todas las cuentas de usuario.

No hay ningún **procedimiento** formal para dar de baja a un usuario del sistema.

4.1.3 MANTENIMIENTO DE LAS CUENTAS DE USUARIO

Existe considerable traslado de personal entre diferentes unidades especialmente en el Distrito de Pichincha, muchas veces no es posible registrar ni realizar todos los cambios debido a que la Dirección de Recursos Humanos no emite la información respectiva a la Dirección de Informática.

No se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.

4.1.4 PERMISOS ASIGNADOS A LAS CUENTAS DE USUARIO

El control de acceso a la red de la Institución se basa en los perfiles de los usuarios.

La asignación de permisos a los diferentes sistemas que se utilizan en la Institución, se realiza de acuerdo a las necesidades de cada dirección o área operativa, la asignación o negación de permisos a los usuarios son dados por los administradores que pueden ser el Jefe de Desarrollo de Sistemas o cualquiera de los Analistas. De esta manera, los usuarios solo pueden interactuar con los sistemas y los datos a los que se les permite acceder.

No se tiene en cuenta ninguna **restricción horaria** para el uso de los recursos.

4.1.5 INACTIVIDAD DE LAS CUENTAS DE USUARIO

Si las cuentas de usuarios permanecen varios días sin actividad, por licencia o por vacaciones del usuario, estas no pasan a un estado de suspensión.

4.1.6 CUENTAS DE USUARIO

En algunos de los departamentos o direcciones, los usuarios no son identificados en forma personal, permitiendo que varios usuarios utilicen el mismo nombre de usuario y contraseña para ingresar a la red.

Las cuentas de usuarios que vienen por default en el sistema operativo de las estaciones de trabajo, como son las cuentas “Guest”, permanecen inactivas en el sistema sin ser utilizadas.

4.2 AUTENTICACIÓN DE LOS USUARIOS

En la **pantalla de ingreso a la red (login)** de los sistemas operativos se muestran los siguientes datos:

- Nombre de usuario.
- Contraseña (a completar por el usuario),
- Dominio.

Cuando los usuarios ingresan su contraseña al sistema, solo se visualizan asteriscos en lugar del dato ingresado.

En cuanto a la configuración de las estaciones de trabajo en el sistema BIOS, existe una contraseña de administrador y una contraseña de usuario, con la contraseña de usuario se permite el arranque del sistema, y no se tiene acceso a modificar las opciones de configuración.

4.3 CONTRASEÑAS

4.3.1 GENERACIÓN DE CONTRASEÑAS

Las contraseñas que existen en la Institución son generadas por cada uno de los usuarios, sin ningún procedimiento automático de generación.

Cuando se da de alta a un usuario en la red, se inicializa con una misma contraseña y con la opción de que el usuario cambie su contraseña la próxima vez que ingrese a la red.

4.3.2 CAMBIOS DE CONTRASEÑA

La edad máxima de la contraseña es de treinta días, esto es controlado automáticamente por el sistema operativo del servidor-3 a través de una política de grupo. Una vez cumplidos 30 días desde el último cambio de contraseña ésta caduca y el sistema obliga a los usuarios a ingresar una nueva contraseña para ingresar a la red.

4.4 SEGREGACIÓN DE FUNCIONES

Se está intentado implantar un plan de separación de funciones, con el propósito especialmente de que no todos los usuarios tengan los mismos permisos para realizar la totalidad de las funciones de administración.

En lo relativo a la administración y soporte a los usuarios, todos los analistas conocen de todo, esto se aprovecha como una gran ventaja, ya que si un analista sale de vacaciones otro puede cubrir sus tareas.

5 - RELEVAMIENTO DE LA SEGURIDAD DE LAS COMUNICACIONES

OBJETIVO

Evaluar la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro.

5.1 TOPOLOGÍA DE RED

5.1.1 COMPONENTES DE RED

La red informática del Ministerio Público cuenta con el siguiente equipamiento:

Edificio Roca

- Dos servidores, el primer servidor (servidor-2) es de impresión y antivirus el segundo servidor (servidor-3) es servidor de correo y aplicaciones.
- Aproximadamente 150 estaciones de trabajo.
- Backbone de Fibra óptica.
- Cableado horizontal UTP categoría 5e.
- Un switch central 3 Com 4900 SX con 12 salidas de fibra óptica.
- Conexión ADSL de 256 KBPS.
- paneles de 48 puertos
- paneles de 24 puertos
- paneles de 16 puertos

- switch 4228G de 24 puertos
- switch 4226T de 24 puertos
- switch 4250T de 48 puertos
- firewall 3com.

Edificio Tocuyo

- Un servidor (servidor-1), que se lo utiliza como servidor de impresión, antivirus, correo y aplicaciones.
- Aproximadamente 50 estaciones de trabajo.
- Cableado horizontal y vertical UTP categoría 5e.
- Hubs de 100 MB.
- Conexión ADSL de 128 KBPS.
- Paneles de 48 puertos
- Paneles de 24 puertos
- 1 firewall 3com.

5.1.2 DESCRIPCIÓN DE LA RED

Edificio Tocuyo

- **UTP en conexiones internas**: el tendido horizontal y vertical esta realizado con cable UTP CAT5e, capaz de soportar velocidades de transmisión de datos de hasta 155 Mbps.
- **Hubs:** todos los hubs están conectados en cascada.

El diseño del sistema de cableado estructurado, posee todo el equipamiento y equipos activos (hubs, servidor, central telefónica, etc) en el Centro de Cómputo, ubicado en la planta baja.

En el Centro de Cómputo se encuentra un rack abiertos de 44" que cumple con todos los estándares de cableado en el cual están montados los hubs.

El diagrama del rack de voz y datos del centro de cómputo se presenta en el Anexo2[2].

Edificio Roca

- **Backbone de fibra óptica**: el backbone central del edificio está realizado con cable de fibra óptica multimodo y es capaz de soportar velocidades de transmisión de datos de hasta 1Gb. También posee un respaldo en UTP en caso de que el backbone principal falle.
- **UTP en conexiones internas**: el tendido horizontal esta realizado con cable UTP CAT5e, capaz de soportar velocidades de transmisión de datos de hasta 155 Mbps.
- **Switch**: sobre los switches se han configurado dos Vilans (vilan-1 y vilan-2), en el segmento de la vilan-1 se encuentran conectadas las estaciones de trabajo del distrito de Pichincha (desde la planta baja al cuarto piso) y en la vilan-2 se encuentran conectadas las estaciones de trabajo de la parte de

[2] Los racks de piso, los gabinetes y equipo activo del edificio Tocuyo se pueden visualizar en el Anexo 2.

apoyo del Ministerio Fiscal General (desde el quinto piso hasta el décimo piso).

El diseño del sistema de cableado estructurado, posee todo el equipamiento y equipos activos (switches, servidores, central telefónica, etc) en el Centro de Cómputo, en la Dirección Nacional de Informática, ubicada en el quinto piso.

Se posee una red en estrella con un backbone de fibra óptica capaz de soportar transmisión de voz y datos hasta 2 gabinetes para administración remota, desde los cuales se alimentan las distintas dependencias y pisos asignados en cada uno de estos.

En el Centro de Cómputo se encuentran dos racks abiertos de 84" que cumplen con todos los estándares de cableado en el cual está montado el switch principal para manejar los equipos remotos.

- ***Gabinete 1 (G 1),*** de voz y datos está ubicado en el Departamento de Asesores del Distrito de Pichincha, en el Séptimo Piso, ala SUR.
  Perímetro de acción: planta baja, primer piso, segundo piso y tercer piso.

- ***Gabinete 2 (G 2),*** de voz y datos está ubicado en la Unidad de Delitos Automotores, en el Primer Piso, ala SUR.
  Perímetro de acción: séptimo piso, octavo piso, noveno piso y décimo piso

- ***Rack 1 (R 1),*** de voz está ubicado en el Centro de Cómputo de la Dirección Nacional de Informática, en el Quinto Piso, ala SUR.

  Perímetro de acción: cuarto piso, quinto piso y sexto piso.

- ***Rack 2 (R 2),*** de datos está ubicado en el Centro de Cómputo de la Dirección Nacional de Informática, en el Quinto Piso, ala SUR.

  Perímetro de acción: cuarto piso, quinto piso y sexto piso.

Hacia los dos Gabinetes se llega con un **backbone de fibra óptica de 4 hilos más dos cables UTP como respaldo de datos**, considerando que dos hilos de fibra son usados para la alimentación de los switches y que otros dos hilos son de reserva.

Los diagramas de los racks de voz y datos de los gabinetes y del centro de cómputo se presentan en el Anexo1[3].

5.1.3 CABLEADO ESTRUCTURADO

El cableado estructurado contempla la integración en una sola red de servicios integrados de Voz y Datos, montada sobre una configuración en estrella, ordenada y lo suficientemente flexible para permitir una ágil administración del sistema. Este aspecto logra que la red estructurada sea de arquitectura abierta, de modo que se adapte a los sistemas que a ella se conecten. Permite tener computación distribuida a través de la red a velocidades de hasta 155 Mbps con su cable CAT5e.

[3] En el Anexo 1 se presenta el rack del edificio Roca y su equipo activo.

El cableado estructurado está configurado de tal manera que permite se “centralice” la ubicación de los sistemas de transmisión (Central Telefónica, Servidores, Switches, etc) al mismo tiempo que se “descentraliza” la aplicación final de cada uno de ellos.

La Red Horizontal de Voz y Datos y la Red Vertical de Datos cumplen fundamentalmente con el estándar ANSI/EIA/TIA para Categoría 5e, de acuerdo a las siguientes normas: 568A normas para el cableado de telecomunicaciones, 569 normas para la ruta y espacios de telecomunicaciones, y 606 normas para la administración del cableado.

Se pueden ubicar los siguientes subsistemas de cableado:

- Subsistema de trabajo: tomas de información (I/O´s) y cable de enlace a computador.
- Subsistema de Centro de Cómputo: elementos encargados de enlazar y distribuir los servicios de Voz y Datos.
- Subsistema de Administración: equipos de enlace entre backbone y red horizontal.
- Subsistema de Backbone: cable de enlace o alimentación desde el Centro de Cómputo hasta el subsistema de Administración.
- Subsistema horizontal: cable UTP desde la zona de trabajo hasta el Centro de Cómputo.

SUBSISTEMA DE TRABAJO

Este subsistema de cableado está conformado por los elementos terminales en el lado de la estación de trabajo.

Se tienen las siguientes características:

- En las estaciones de trabajo se encuentran conectores (jacks) montados sobre un cajetín rectangular. Los jacks se han colocado sobre la parte superior de la canaleta de acceso y/o al final de la misma. Se ha realizado una diferenciación por color para los puntos de voz (blanco) y datos (azul).

- Los jacks se han conectado bajo la característica de la Norma 568B, se puede utilizar indiferentemente cada punto como servicio de voz o datos.

- La misma norma es cumplida por los cables de enlace (patch cord).

SUBSISTEMA DE EQUIPOS

Este subsistema es el área utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El subsistema de Equipos se encuentra ubicado en el Centro de Cómputo. En esta área se encuentran los racks de

telecomunicaciones principales, desde el cual se alimentan a los gabinetes uno y dos.

El Centro de Cómputo posee instalaciones eléctricas exclusivas para los equipos de telecomunicaciones, así también alimentadas por un UPS, en caso de cortes de energía.

En este subsistema se tienen los siguientes elementos principales:

- Distribuidor Óptico Principal (ODF) compuesto por un panel de 12 puertos ubicado en el Sexto Piso en el RACK 2 ; (ODF I) compuesto por un panel de 12 puertos ubicado en el Octavo Piso y (ODF II) compuesto por un panel de 12 puertos ubicado en el Segundo Piso con una capacidad instalada de 4 fibras.

- Los acopladores ópticos utilizados en los paneles son del tipo ST-ST.

- En este subsistema de equipos se encuentra instalada la central telefónica.

SUBSISTEMA DE ADMINISTRACIÓN

Está formado por los equipos y elementos utilizados en la administración de la red que realizan el enlace entre el Centro de Cómputo y los Gabinetes distribuidos.

Se tienen los siguientes elementos:

- Paneles RJ45 de voz y datos para servicio de las distintas áreas. Dependiendo de la densidad del área se tienen paneles de 24 y/o 48 puertos.

- En este subsistema se tiene los patch cord para habilitar los puntos de red.

- Distribuidores ópticos secundarios para recibir 4 hilos de fibra óptica provenientes del centro de cómputo. El panel óptico ODF tiene capacidad para 12 puertos de los cuales se encuentran habilitados 4 con acopladores ST-ST.

- En cada gabinete se encuentran instalados los Switches remotos para la red de datos y los distribuidores telefónicos para la red de voz.

SUBSISTEMA DE BACKBONE

Está conformado por fibra óptica multimodo de 62,5 / 125 micrones a 4 hilos.

SUBSISTEMA HORIZONTAL

Implica el cableado existente entre el Centro de Cómputo y los puntos terminales (subsistema de trabajo) y entre los Gabinetes de Administración y los puntos terminales. El cableado realiza su recorrido mediante canaletas en las áreas en

donde no existe cielo falso y se completa el recorrido mediante tubería PVC para los sitios con cielo falso.

5.1.4 ANCHO DE BANDA DE LA RED

El cableado UTP soporta hasta 155 Mbps con su cable CAT5e.
El backbone central soporta hasta 1Gb con su cable de fibra óptica.

5.1.5 FALLA EN LA RED ELÉCTRICA

Cuando hay un corte de luz, en caso de poseer un UPS conectado a la estación de trabajo, se graban los trabajos que se están ejecutando y se apaga el computador hasta que el generador principal entre en funcionamiento.

5.2 CONEXIONES EXTERNAS

- **Conexión entre los dos edificios**: para conectarse entre los dos edificios se posee una configuración de POP3, esta conexión es utilizada únicamente para la transmisión del correo electrónico.
- **Servidor de Internet**: el servidor-3 tiene una salida al exterior a través de una conexión ADSL de 512 Kbps y el servidor-1 tiene una salida al exterior a través de una conexión ADSL de 256 Kbps suministradas por el mismo ISP.

- **Hosting**: se tiene contratado un espacio de 10 Mb, en nuestro proveedor de Internet para almacenar la página web de la Institución. El contenido de la página WEB que se almacena en el espacio contratado es actualizado en forma remota por un analista de la Dirección Nacional de Informática, cada vez que es requerido.

5.3 CONFIGURACIÓN LÓGICA DE RED

5.3.1 INTEROPERATIVIDAD WINDOWS

La plataforma Windows que se posee permite, la comunicación entre todos los usuarios de la red, facilitando así las comunicaciones y el acceso a recursos y servicios que brinda la red.

El servidor-3, a través de su sistema operativo Windows 2003 permite:

- Autenticación de los usuarios.
- Administración de perfiles de usuarios.
- Administración de los recursos compartidos.
- Administración de los niveles de seguridad de los recursos de red.

5.3.2 RECURSOS COMPARTIDOS

El entorno de red de cada una de las estaciones de trabajo se encuentra deshabilitado, el personal que presta el soporte técnico se encarga de realizar las

configuraciones necesarias para acceder a los recursos compartidos y los servicios de red que cada usuario debe acceder.

Ninguno de los usuarios puede compartir sus datos con otro usuario, solo los funcionarios que brindan el soporte técnico pueden ayudarlos a compartir sus archivos o recursos a través de su perfil de administrador en cada terminal.

Sobre los servidores 2 y 3 (Edificio Roca) se tienen compartidas:

- En el servidor-3, se comparten todas las carpetas de las aplicaciones que son utilizadas por los usuarios de las distintas unidades.
- En el servidor-2 se encuentran instaladas y compartidas todas las impresoras de red.

Sobre el servidor-1 (Edificio Tocuyo) se encuentran compartidas:

- Todas las carpetas de las aplicaciones que son utilizadas por los usuarios de las distintas unidades.
- Instaladas y compartidas todas las impresoras de red.

5.4 MAIL

Todo funcionario que se encuentra conectado a la red, posee una cuenta de correo electrónico, este medio de comunicación es interno y externo.

La administración de las cuentas de correo electrónico se lleva a cabo mediante **Microsoft Exchange 2000**, instalado en el servidor-3.

Para que cada funcionario pueda acceder a sus mensajes de correo electrónico en cada una de las estaciones de trabajo se ha instalado **Microsoft Outlook**.

Los mensajes de correo electrónico, no son considerados ni utilizados como **documentos formales,** así tampoco se ha manifestado a los usuarios que se deben respetar todos los lineamientos referentes al uso inapropiado de este medio de comunicación.

No existe ningún tipo de configuración respecto ha la encriptación de los mensajes.

Cada buzón tiene asignado una **capacidad fija de almacenamiento de 4Mb** por cuenta de correo electrónico.

5.5 ANTIVIRUS

En la Institución se posee una versión corporativa de una herramienta antivirus, en los dos edificios tanto en el servidor-1 como en el servidor-2 está instalada una versión de servidor y en cada una de las estaciones de trabajo una versión cliente.

Una versión corporativa de esta naturaleza enlaza el servidor con cada una de las estaciones de trabajo permitiendo:

Instalación remota, se puede realizar instalaciones remotas del antivirus en estaciones de trabajo que poseen versiones de sistema operativo Windows XP o Windows 2000.

Control de desinstalación del antivirus, la desinstalación del antivirus de cada una de las estaciones de trabajo, puede llevarse a cabo si se conoce la clave de acceso.

Actualización automática, se tiene programada la tarea de actualización de las definiciones de virus en cada uno de los servidores por la noche, permitiendo realizar las actualizaciones vía Internet. Una vez que las definiciones han sido actualizadas en los servidores, las estaciones de trabajo son actualizadas en forma automática.

Búsqueda de virus, se pueden realizar búsquedas de virus localmente en cada estación de trabajo, como también se puede realizar una búsqueda desde el servidor por medio de números de IP o por el nombre de la estación de trabajo.

Contenido de mensajes de correo, esta herramienta tiene la capacidad de verificar el contenido de cada uno de los mensajes de correo electrónico sean entrantes o salientes.

5.6 FIREWALL

Los firewalls que existen en la Institución están configurados de tal manera que se habilitan aquellos requeridos por las actividades de cada unidad y se han restringido los que prestan riesgos a la seguridad del sistema.

Como política de aplicación de los firewalls en los dos edificios, se verifica todo tipo de tráfico, entrante, saliente y en tránsito, de esta manera se protegen las redes internas de cada edificio.

CAPÍTULO II

VULNERABILIDADES Y CONSECUENCIAS

En este capítulo se detallan las debilidades encontradas en el informe de relevamiento del Ministerio Público, siempre con la premisa de crear y mantener un ambiente seguro para la información y los recursos. Este estudio apoyará en el desarrollo del análisis de riesgos.

1- VULNERABILIDADES DE LA SEGURIDAD FÍSICA

- **Equipamiento centro de cómputo edificio Tocuyo**

  El extintor del que dispone el centro de cómputo del edificio Tocuyo, se encuentra descargado, no se realizado el mantenimiento respectivo para la recarga del equipo.

  Consecuencia

  Si el fuego se hiciera presente en el centro de cómputo, sería imposible detenerlo ya que el equipo extintor no posee carga.

- **Centro de cómputo edificio Roca**

  Las paredes y puerta del centro de cómputo fueron construidas con **vidrio convencional**, esto se convierte en un riesgo, por no poseer características técnicas acordes a especificaciones y estándares técnicos.

Consecuencia

En caso de un incidente como un incendio las paredes por no soportar el calor podrían estallar, convirtiéndose en una amenaza para los funcionarios y equipamiento de la Dirección de Informática.

- **Centro de cómputo edificio Roca**

  Las seguridades físicas no brindan completa seguridad a toda el área de la Dirección de Informática. La puerta de acceso es de vidrio sin ninguna otra protección y esta montada sobre un panel de aglomerado.

Consecuencia

Como las protecciones son muy frágiles, son muy fáciles de violentar permitiendo el acceso a todos los equipos de la Dirección de Informática y al centro de cómputo.

- **Centro de cómputo edificio Roca**

  No se dispone de ningún medio de extinción de incendios en el centro de cómputo del edificio Roca.

Consecuencias

Si el fuego se hiciera presente en el centro de cómputo, sería imposible detenerlo por no poseer ningún dispositivo de soporte que permita mitigarlo o extinguirlo.

- **Dispositivos instalados**

No se realizan controles sobre los dispositivos instalados en las estaciones de trabajo, tales como disqueteras, cd rom, etc.

Consecuencia

Cualquier funcionario podría poner, sacar o reemplazar los dispositivos pasando por desapercibido el cambio o modificación realizada.

- **Control de acceso a los edificios**

  El control de la seguridad solo se realiza en la entrada al edificio, ya en el interior del edificio, el público puede acceder a cualquier dependencia sin ninguna restricción.

  Consecuencia

  Podría cualquier persona aprovecharse de esta debilidad para acceder a cualquier tipo de recurso o información.

- **Control de acceso a los edificios**

  Los funcionarios pueden ingresar a los edificios en horarios no laborables, fines de semana o feriados sin ninguna autorización.

  Consecuencia

  Esta vulnerabilidad se presta para dar facilidades para que los funcionarios usen o abusen de los recursos a ellos asignados, por no estar sujetos a ningún control.

- **Salida de equipo informático**

Cualquier equipo informático sea o no de la Institución puede ingresar o salir libremente de las instalaciones del Ministerio sin ningún control.

Consecuencia

Como todo el público puede circular libremente en el interior de los edificios, esta falla en la seguridad podría permitir el robo de equipamiento.

2- VULNERABILIDADES DE LA ADMINISTRACIÓN DEL CENTRO DE CÓMPUTO

- **Asignación de responsabilidades**

  No se asignan responsabilidades para cada tarea a cada funcionario del área de sistemas.

  Consecuencia

  El no asignar responsabilidades puntuales, permitiría la generación de malas interpretaciones respecto a las tareas a desarrollar.

- **Falta de planes formales de la Dirección de Informática**

  No se han desarrollado planes formales de la dirección de Informática.

  Consecuencia

  La falta de planes recae directamente en la ausencia de administración de tiempo, y recursos tanto humanos como tecnológicos.

- **Conciencia de la seguridad**

  Aun los funcionarios no han tomado plena conciencia sobre el tema de seguridad y su importancia.

  Consecuencia

  El no adquirir una cultura de seguridad impedirá a los funcionarios cumplir con las normas y procedimientos de seguridad implementados.

- **Inventario de los sistemas**

  No existe un inventario de los sistemas de información y sus características principales.

  Consecuencia

  Generar un inventario exacto permitirá designar los posibles responsables de la información que maneja cada sistema, como también las áreas en las que interviene y la prioridad en caso de emergencia.

- **Inventarios de hardware**

  No existe un único y completo inventario de hardware de los equipos.

  Consecuencia

  El mantener esta información actualizada facilita las actividades de mantenimiento y las actividades del plan de contingencias.

- **Publicación de las normas**

  Se debe realizar un procedimiento para publicar y dar a conocer las nuevas normas de seguridad que se están implementando.

  Consecuencia

  En la Institución se torna fundamental el difundir las normas de seguridad que se están implementando, con el fin de que cada funcionario tome conciencia sobre la importancia de la seguridad.

- **Consentimiento de los usuarios**

  No existe consentimiento por parte de los usuarios a que se auditen sus actividades en el sistema , ni declaraciones de que conocen las normas de buen uso del sistema.

  Consecuencia

  No existe una garantía de que el usuario ha comprendido las normas y que sabe de cómo hacer un buen uso del sistema y sus dispositivos y que está dispuesto a cumplirlas.

- **Respaldo de la información**

  No se está realizando ningún respaldo de información ni de la configuración de los servidores, ni de la información de los sistemas en funcionamiento.

  Consecuencias

  Siendo el respaldo el principal método de recuperación de información es imposible volver a poner en funcionamiento la red, los sistemas y servidores en caso de una contingencia.

3- VULNERABILIDAD DE LA SEGURIDAD DE LAS APLICACIONES

- **Clasificación de la información**

  Los datos de la Institución no se clasifican formalmente de acuerdo a su importancia.

  Consecuencia

  La clasificación de la información permite asignar diferentes niveles de control de seguridad. La falta de clasificación permitiría errar en la asignación de accesos.

4- VULNERABILIDADES DE LA SEGURIDAD LOGICA

- **Estación de trabajo abandonada**

  Los usuarios luego de encender sus estaciones de trabajo por descuido pueden dejarlas abandonadas.

  Consecuencia

  Cualquier persona que tenga acceso físico a la estación de trabajo puede apoderarse de la misma y hacer uso de la información o de los recursos en forma inadecuada.

- **Restricción de horario**

  No existe un control de acceso a las estaciones de trabajo, de acuerdo al horario de trabajo ni días laborables.

  Consecuencia

  Al no tener establecido una restricción horaria, los usuarios pueden hacer uso de los bienes y servicios sin ningún control, especialmente en horarios fuera de los establecidos. Esta debilidad puede permitir que funcionarios ingresen a la red en horarios no laborables y utilicen los recursos para beneficio propio.

- **Suspensión de cuentas de usuario**

  Las cuentas de los usuarios que han permanecido inactivas por varios días no pasan a un estado de suspensión.

Consecuencia

Una persona no autorizada que conozca la contraseña de ingreso, puede tener acceso a una cuenta de usuario que no le corresponde, permitiéndosele ver información para la que no tiene autorización.

- **Identificación personal**

  En algunos departamentos los usuarios no son identificados en forma personal, utilizando la misma estación de trabajo con el mismo nombre y contraseña de ingreso a la red.

  Consecuencia

  Ante un posible robo, fraude o abuso, sería imposible identificar qué persona fue la causante, por lo tanto no se puede rastrear las acciones de los usuarios en el sistema. Además no existe privacidad de la información.

- **Baja de usuarios de la red**

  No existe un procedimiento para efectuar las bajas de las cuentas de los funcionarios del sistema.

  Consecuencia

  Es posible que funcionarios próximos a salir de la Institución, realicen acciones de sabotaje o vandalismo, por rechazo o insatisfacción con las decisiones tomadas por las autoridades.

- **Contraseñas de los servidores edificio Tocuyo**

Las palabras claves de los dos servidores son iguales.

Consecuencia

Se incrementa el riesgo de acceso a los servidores, si alguien por cualquier circunstancia descubre la contraseña, tendrá acceso a los dos servidores.

- **Separación de funciones**

  No se implementa ningún régimen de separación de tareas.

Consecuencia

Pueden cometerse errores y librarse de responsabilidades.

5- VULNERABILIDAD EN LA SEGURIDAD DE LAS COMUNICACIONES

- **Diseño de la red**

  Los gabinetes 1 y 2 se encuentran ubicados en oficinas que no pertenecen a la Dirección Nacional de Informática, con demasiado tráfico de personas y en espacios completamente reducidos.

  Consecuencia

  Un intruso o una persona mal intencionada podría forzar las puertas de los gabinetes y provocar un daño muy grave en las comunicaciones o el robo del equipamiento.

- **Uso del mail**

  El uso del mail no solo se emplea para funciones laborales, sino también con fines personales.

  Consecuencia

  El utilizar el servicio de mail indiscriminadamente puede bajar el rendimiento de la red y se puede incrementar el riesgo de infección con virus.

- **Asignación automática de IP a cualquier equipo que se conecte a la red**

  Cualquier equipo que se conecte a la red automáticamente se le asigna un número de IP, y podría ingresar a la red o acceder a los servicios que ésta brinda.

Consecuencia

Puede provocar el acceso a la red de posibles atacantes.

ANÁLISIS DE RIESGOS

1 - ACTIVOS

La información, las funciones y actividades de la Institución y la infraestructura tecnológica son elementos indiscutibles que se deben mantener y proteger, es por ello que se ha realizado un listado de los distintos activos reconocidos, asignando un valor a la importancia que tienen en la Institución, ponderada en una escala del 1 al 10. Esta importancia es un valor relativo que refleja el nivel de impacto que puede tener la Institución si un incidente afecta a los activos.

Tabla 2.1: (Listado de activos)

N°	Activos a proteger	Importancia (1-10)
1	Servidor 1	10
2	Servidor 2	10
3	Servidor 3	10
4	Switch principal 4900SX	10
5	Switch 4228G	10
6	Switch 4226T	10
7	Switch 4250T	10
8	Hubs	10
9	UPS del centro de cómputo	7
10	Sistema de aire acondicionado edificio Roca	4
11	Sistema de aire acondicionado edificio Tocuyo	4
12	Equipo ADSL	6
13	Firewall	9
14	Central telefónica	8
15	Gabinete 1	10
16	Gabinete 2	10
17	Bases de datos	9
18	Software de aplicación, programas fuente, sistemas operativos	6
19	Backup	9
20	Datos de configuración	8
21	Administración del centro de cómputo (Departamento de sistemas).	9
22	Red, cableado red LAN.	8
23	Red eléctrica	8
24	Usuarios.	5
25	Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	4
26	Hardware (estaciones de trabajo impresoras de red)	4
27	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	3
28	Información procesada de usuarios.	6

2 - FACTORES DE RIESGO

Los factores de riesgo son las amenazas que pueden afectar a los activos, se ha realizado un estudio de los posibles riesgos a los cuales se les ha calificado, indicando la probabilidad de que estas contingencias ocurran, en una escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en la organización y acontecimientos ocurridos.

Tabla 2.2: (Factores de riesgo)

N°	Factores de riesgo	Probabilidad
1	Abuso de puertos para el mantenimiento remoto	1
2	Acceso a datos no autorizado[4]	2
3	Acceso físico no autorizado	3
4	Administración impropia de los recursos dependiendo de los roles y las responsabilidades	1
5	Almacenamiento de contraseñas negligente	1
6	Backups (Mala configuración del schedule)	1
7	Backups desactualizados	3
8	Backups perdidos o inexistentes	2
9	Borrado, modificación o revelación desautorizada o inadvertida de información [5]	1
10	Condiciones de trabajo adversas	1
11	Conexión de cables inadmisible	2
12	Conexiones todavía activas	3
13	Configuración inadecuada de componentes de red	2
14	Conocimiento insuficiente de los documentos de requerimientos en el desarrollo	2
15	Copia no autorizada de un medio de datos	2

[4] El primer artículo innumerado, agragado después del Art. 202, del Código Penal, mediante reforma contenida en el Art. 58, Título V, de La Ley de Comercio Electrónico, Firmas y Mensajes de Datos, publicada en el Registro Oficial No. 557, de 17 de abril del 2002, tipifica como infracción informática el acceso no autorizado a información protegida. Ver texto legal en el anexo 3.

[5] Este punto tiene relación directa con lo determinado en los Art2. 262 reformado en el Código Penal; primer y segundo artículos innumerados agregados después del Art. 415 del Código Penal; y, primer artículo innumerado agregado después del Art. 202 del Código Penal, mediante reforma contenida en los Arts. 59, 61 y 58, Título V, de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 557, de 17 de abril del 2002, que tipifica la destrucción maliciosa y fraudulenta de mensajes de datos e información; los daños informáticos; y, delitos contra la información protegida respectivamente. Ver texto de la ley en el anexo 3.

16	Corte de luz	1
17	Daño de cables inadvertido	1
18	Denial of service	1
19	Destrucción o mal funcionamiento de un componente	2
20	Desvinculación del personal	1
21	Documentación deficiente o faltante	3
22	Entrenamiento de usuarios inadecuado	2
23	Equipos informáticos con escasos medios físicos de protección	2
24	Equipos informáticos con recursos escasos de hardware	1
25	Errores de configuración y operación	1
26	Errores de software	1
27	Factores ambientales	1
28	Falla de las bases de datos	1
29	Falta de auditorías	3
30	Falta de compatibilidad	1
31	Falta de confidencialidad	1
32	Falta de espacio de almacenamiento	1
33	Incumplimiento con las medidas de seguridad del sistema	2
34	Límite de vida útil - Máquinas obsoletas	1
35	Longitud de los cables de red excedida	1
36	Mal uso de derechos de administrador	3
37	Configuración impropia del servicio de Mail	2
38	Mala evaluación de datos de auditoría	3
39	Mala integridad de los datos	1
40	Manipulación de los tableros de los circuitos eléctricos	3
41	Mantenimiento ausente en el equipamiento informático	2
42	Mantenimiento mal realizado en el equipamiento informático	1
43	Medios de datos no están disponibles cuando son necesarios	1
44	Modificación de datos no autorizada	1
45	Pérdida de confidencialidad[6] en datos privados	1
46	Pérdida de datos	1
47	Pérdida de datos en tránsito	1
48	Poca adaptación a cambios del sistema	1
49	Procesos no documentados	3
50	Registro de red desactualizado	2
51	Reglas insuficientes o ausencia de ellas	2
52	Riesgo por el personal de limpieza o personal externo	1
53	Robo	1
54	Rótulos inadecuados en medios magnéticos	1
55	Sabotaje	1
56	Seguridad de base de datos deficiente	1
57	Software desactualizado	1
58	Software sin licencia [7]	2
59	Spoofing y sniffing	1

[6] Quién vulnere la confidencialidad de la información será reprimido con sanción y multa según lo indica el artículo 58 de las Reformas del Código Penal, de la Ley de Comercio Electrónico, Firmas y mensajes de Datos. Ver texto de la ley en el anexo 3.

[7] La Ley de Propiedad Intelectual contempla normas especiales relativas a los programas de ordenador, en los Arts. 28, 29 y 30. Ver texto legal en el anexo 3.

60	Transferencia de datos incorrectos o no deseados	1
61	Transporte inseguro de archivos	1
62	UPS de cada equipo descargado	2
63	UPS del centro de cómputo descargado	2
64	Uso sin autorización del equipamiento	1
65	Variaciones de voltaje	1
66	Virus, gusanos y caballos de Troya	3
67	Ingerir alimentos, bebidas o fumar	3
68	Incendio	1

3- ACTIVOS POSIBLES CONSECUENCIAS Y MEDIDAS EXISTENTES

Se describe en los siguientes cuadros los activos de la Institución, los factores de riesgo que los afectaría directamente y las consecuencias que puede acarrear la ocurrencia de esos factores.

Así también se agrega información referida a las medidas que se han tomado para mitigar estas consecuencias.

Las medidas tomadas han sido ponderadas en tres niveles indicando sin son efectivas (e), mejorables (m) o deficientes (d).

Cuadro 2.1: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
1	Servidor 1	2	Acceso a datos no autorizado	Pérdida de confidencialidad de la información, quebrantamiento de la seguridad	Acceso físico, acceso lógico	e
2	Servidor 2	3	Acceso físico no autorizado	Robo de información, modificación de información	Acceso físico, acceso lógico	m
		5	Almacenamiento de contraseñas negligente	Acceso total a los servidores	Seguridad lógica, políticas de contraseñas	e
		16	Corte de luz	Falta del sistema	U.P.S. , generador	e
		19	Destrucción o mal funcionamiento de un componente	Pérdida de tiempo por reemplazo	Posee 3 fuentes de poder redundantes	m
		25	Errores de configuración y operación	Inestabilidad en el sistema, aumento de vulnerabilidades	Contratación de especialistas, capacitación del personal a cargo	e
		34	Límite de vida útil - Máquinas obsoletas	Deterioro en el rendimiento del sistema	Mejoramiento de las características del hardware	e
		42	Mantenimiento mal realizado en el equipamiento informático	Interrupciones en el funcionamiento del sistema	Mantenimiento de personal propio	e
		44	Modificación de datos no autorizada	Inconsistencia de datos, mala configuración, fraude	Control de acceso físico, control de acceso lógico	e
		53	Robo	Pérdida de equipamiento, pérdida de información	Control de acceso físico	m
		63	UPS del centro de cómputo descargado	Apagado anómalo de los equipos en caso de corte de luz, discontinuidad en el funcionamiento del sistema, corte inesperado de los procesos en ejecución	Chequeo preventivo del UPS	e
		65	Variaciones de voltaje	Daño de los componentes en los equipos	UPS	e
		66	Virus, gusanos y caballos de Troya	Fallas generales en el sistema, fallas en la red	Software antivirus, firewall	e
		67	Ingerir alimentos, bebidas o fumar	Daño de teclado, mouse o dispositivos del servidor	Divulgación de políticas de seguridad física	m
		68	Incendio	Pérdida de equipamiento, perdida de información		d

Cuadro 2.2: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
3	Servidor 3	2	Acceso a datos no autorizado	Pérdida de confidencialidad de la información, quebrantamiento de la seguridad	Acceso físico, acceso lógico	e
		3	Acceso físico no autorizado	Robo de información, modificación de información	Acceso físico, acceso lógico	m
		5	Almacenamiento de contraseñas negligente	Acceso total a los servidores	Seguridad lógica, políticas de contraseñas	e
		16	Corte de luz	Falta del sistema	U.P.S. , generador	e
		19	Destrucción o mal funcionamiento de un componente	Pérdida de tiempo por reemplazo	Analizar la posible contratación externa para soporte en repuestos	d
		25	Errores de configuración y operación	Inestabilidad en el sistema, aumento de vulnerabilidades	Contratación de especialistas, capacitación del personal a cargo	e
		34	Límite de vida útil - Máquinas obsoletas	Deterioro en el rendimiento del sistema	Mejoramiento de las características del hardware	e
		42	Mantenimiento mal realizado en el equipamiento informático	Interrupciones en el funcionamiento del sistema	Mantenimiento de personal propio	e
		44	Modificación de datos no autorizada	Inconsistencia de datos, mala configuración, fraude	Control de acceso físico, control de acceso lógico	e
		53	Robo	Pérdida de equipamiento, pérdida de información	Control de acceso físico	m
		63	UPS del centro de cómputo descargado	Apagado anómalo de los equipos en caso de corte de luz, discontinuidad en el funcionamiento del sistema, corte inesperado de los procesos en ejecución	Chequeo preventivo del UPS	e
		65	Variaciones de voltaje	Daño de los componentes en los equipos	UPS	e
		66	Virus, gusanos y caballos de Troya	Fallas generales en el sistema, fallas en la red	Software antivirus, firewall	e
		67	Ingerir alimentos, bebidas o fumar	Daño de teclado, mouse o dispositivos del servidor	Divulgación de políticas de seguridad física	
		68	Incendio	Pérdida de equipamiento, perdida de información		d

Cuadro 2.3: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
4	Switch principal 4900SX	3	Acceso físico no autorizado	Cambio de configuración	Seguridad física	m
5	Switch 4228G	4	Administración impropia de los recursos dependiendo de los roles y las responsabilidades	Desconfiguración lógica y física, deterioro en el rendimiento del sistema	Definición adecuada de los roles (VERBAL)	m
6	Switch 4226T	5	Almacenamiento de contraseñas negligente	Acceso total a configuración de la red	Seguridad lógica, políticas de contraseñas	e
7	Switch 4250T	11	Conexión de cables inadmisible	Fallas en el sistema, pérdida de tiempo	Seguridad física	m
8	Hubs	13	Configuración inadecuada de componentes de red	Pérdida de comunicación con los servidores, fallas en el sistema	Seguridad lógica	m
		16	Corte de luz	Falta del sistema	U.P.S. , generador	e
		19	Destrucción o mal funcionamiento de un componente	Pérdida de tiempo por reemplazo	Analizar la posible contratación externa para soporte en repuestos	d
		25	Errores de configuración y operación	Inestabilidad en el sistema, aumento de vulnerabilidades	Contratación de especialistas, capacitación del personal a cargo	e
		34	Límite de vida útil - Máquinas obsoletas	Deterioro en el rendimiento del sistema	Equipamiento moderno, actualización del hardware	e
		44	Modificación de datos no autorizada	Fallas en el sistema, inconsistencia de datos, pérdida de tiempo	Controles de acceso lógico	e
		50	Registro de red desactualizado	Pérdida de tiempo, usuarios sin sistema	Actualización constante de acuerdo a los cambios	e
		63	UPS del centro de cómputo descargado	Discontinuidad en el funcionamiento del sistema, fallas en el sistema	Chequeo preventivo de UPS	e
		68	Incendio	Pérdida de equipamiento, interrupción general del sistema		d

Cuadro 2.4: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
9	UPS del centro de cómputo	3	Acceso físico no autorizado	Modificación de controles	Seguridad física del centro de cómputo	m
		16	Corte de luz	Falta del sistema	Generador	e
		19	Destrucción o mal funcionamiento de un componente	Indisponibilidad del equipo	Chequeo permanente calendarizado, empresa distribuidora garantiza stock de repuestos	m
		41	Mantenimiento ausente en el equipamiento informático	Falla del equipo, ausencia de respaldo en caso de corte	Chequeo permanente calendarizado	m
		68	Incendio	Pérdida de equipamiento		d

Cuadro 2.5: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
10	Sistema de aire acondicionado edificio Roca	3	Acceso físico no autorizado	Manipulación del equipamiento	Seguridad física	m
11	Sistema de aire acondicionado edificio Tocuyo	16	Corte de luz	Equipamiento del centro de cómputo desprotegido	Generador propio	e
		19	Destrucción o mal funcionamiento de un componente	Equipamiento del centro de cómputo desprotegido	Empresa distribuidora garantiza stock de repuestos	e
		25	Errores de configuración y operación	Posibles daños en el equipamiento del centro de cómputo	Seguridad física, capacitación de la forma de uso al personal encargado	e
		27	Factores ambientales	Posible daño del condesador ubicado en el exterior	Seguridad propia	e
		41	Mantenimiento ausente en el equipamiento informático	Pérdida de equipamiento	Mantenimiento y cambio calendarizado de partes y filtros	e
		42	Mantenimiento mal realizado en el equipamiento informático	Fallas en el equipo, posibles daños en el equipamiento del centro de cómputo	Mantenimiento realizado por técnicos especializados	e
		68	Incendio	Pérdida de equipamiento		d

Cuadro 2.6: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
12	Equipo ADSL	3	Acceso físico no autorizado	Manipulación de equipamiento	Seguridad física	m
		5	Almacenamiento de contraseñas negligente	Acceso lógico al equipo	Seguridad lógica, políticas de contraseñas	e
		11	Conexión de cables inadmisible	Servicio de Internet interrumpido	Seguridad física	m
		16	Corte de luz	Servicio de Internet interrumpido	U.P.S. , generador	e
		18	Denial of service	Interrupción de los servicios de red	Seguridades físicas y lógicas	e
		25	Errores de configuración y operación	Inseguridad en la red	Contratación de especialistas, capacitación del personal a cargo	e
		53	Robo	Pérdida de equipamiento, servicio de Internet interrumpido	Seguridades físicas	m
		68	Incendio	Pérdida de equipamiento		d

Cuadro 2.7: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
13	Firewall	3	Acceso físico no autorizado	Cambio de configuración	Seguridad física	m
		5	Almacenamiento de contraseñas negligente	Acceso lógico al equipo	Seguridad lógica, políticas de contraseñas	e
		11	Conexión de cables inadmisible	Fallas en el sistema, pérdida de tiempo	Seguridad física	m
		13	Configuración inadecuada de componentes de red	Pérdida de comunicación con los servidores, fallas en el sistema	Cambios realizados por personal capacitado	e
		16	Corte de luz	Falta del sistema	U.P.S. , generador	e
		25	Errores de configuración y operación	Inestabilidad en el sistema, aumento de vulnerabilidades	Cambios realizados por personal capacitado	e
		44	Modificación de datos no autorizada	Fallas en el sistema, inconsistencia de datos, pérdida de tiempo	Controles de acceso lógico	e
		63	UPS del centro de cómputo descargado	Discontinuidad en el funcionamiento del sistema, fallas en el sistema	Chequeo preventivo de UPS	e
		68	Incendio	Pérdida de equipamiento, interrupción general del sistema		d

Cuadro 2.8: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
14	Central telefónica	2	Acceso a datos no autorizado	Pérdida de confidencialidad de la información, robo de información	Seguridad lógica	e
		3	Acceso físico no autorizado	Daño físico	Seguridad física del centro de cómputo	m
		4	Administración impropia de los recursos dependiendo de los roles y las responsabilidades	Uso y abuso de los recursos adquiridos o asignados	Software, para control del uso de los teléfonos	e
		5	Almacenamiento de contraseñas negligente	Abuso de contraseñas para modificación de configuración	Seguridad lógica	e
		7	Backups desactualizados	Imposibilidad de restaurar el sistema telefónico con todas las configuraciones	Actualización de respaldos de acuerdo con las modificaciones	e
		8	Backups perdidos o inexistentes	Imposibilidad de restaurar el sistema telefónico en caso de emergencia	Resguardo de los backups	e
		16	Corte de luz	Pérdida de servicio telefónico	Respaldo de baterías propias, con un backup de aproximadamente 30 minutos. Generador	e
		17	Daño de cables inadvertido	Usuarios sin servicio telefónico	Partes estratégicas del cableado telefónico esta protegido físicamente, el resto del cableado es interno	e
		21	Documentación deficiente o faltante	Administración insegura de la central telefónica	Resguardo y almacenamiento adecuado de la información	e
		25	Errores de configuración y operación	Usuarios sin servicio telefónico	Modificaciones realizadas por técnicos contratados	e
		29	Falta de auditorías	Desconocimiento de acciones en el sistema telefónico	Realizar auditorías trimestrales	e
		68	Incendio	Pérdida de equipamiento		d

Cuadro 2.9: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
15	Gabinete 1	3	Acceso físico no autorizado	Destrucción física de gabinetes, robo de equipamiento, conexión de cables inadmisible	Gabinetes se encuentran cerrados con llave, la administración de las llaves está a cargo de funcionarios de la Dirección de Informática	e
16	Gabinete 2	11	Conexión de cables inadmisible	Pérdida de conexión de estaciones de trabajo con los servidores, indisponibilidad de recursos de la red, pérdida de estabilidad y fiabilidad del sistema	Protección física de los gabinetes	e
		12	Conexiones todavía activas	Ingreso fácil a la red por terceros, obtención automática de IP		d
		16	Corte de luz	Apagado de equipos activos, segmentos de la red sin servicios	Todo el equipamiento del backbone posee un UPS capaz de soportar toda la carga. Generador	e
		23	Equipos informáticos con escasos medios físicos de protección	Robo, daño físico, cambio de configuración	Protección física de los gabinetes y su equipo activo	e
		50	Registro de red desactualizado	Segmentos de la red o estaciones de trabajo sin servicios, pérdida de tiempo en búsqueda de fallas	Actualización del registro de red inmediatamente luego de realizar un cambio	e
		68	Incendio	Pérdida de equipamiento		d

Cuadro 2.10: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
17	Bases de datos	6	Backups (Mala configuración del schedule)	Datos sin respaldo	Organización de las tareas programadas	m
		8	Backups perdidos o inexistentes	Incapacidad de restauración de datos	Almacenamiento adecuado y en lugar seguro de los backups	m
		15	Copia no autorizada de un medio de datos	Divulgación de información	Controles lógicos	e
		26	Errores de software	Inconsistencia en los datos	Controles internos	e
		28	Falla de las bases de datos	Inconsistencia en los datos	Controles internos	
		32	Falta de espacio de almacenamiento	Falla en la aplicación	Recursos en disco	e
		39	Mala integridad de los datos	Inconsistencia y redundancia de datos	Controles en las aplicaciones desarrolladas	e
		45	Pérdida de confidencialidad en datos privados	Divulgación de información	Controles físicos y controles lógicos a información crítica	e
		47	Pérdida de datos en tránsito	Inconsistencia de datos	Configuración de la red	e
		53	Robo	Divulgación de información	Controles lógicos	e
		60	Transferencia de datos incorrectos o no deseados	Inconsistencia de datos	Controles lógicos	e
		66	Virus, gusanos y caballos de Troya	Pérdida o modificación de información. Pérdida de productividad	Antivirus	e

Cuadro 2.11: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
18	Software de aplicación, programas fuente, sistemas operativos	2	Acceso a datos no autorizado	Modificación del software en desarrollo	Controles físicos y controles de acceso lógicos	e
		14	Conocimiento insuficiente de los documentos de requerimientos en el desarrollo	Sistema inestable y excesivo mantenimiento de las aplicaciones	Buen análisis y diseño documentado	m
		30	Falta de compatibilidad	Datos erróneos e inestabilidad del sistema, conexiones manuales al servidor	Uso de una única plataforma con versiones diferentes del mismo sistema operativo y soporte para red	e
		31	Falta de confidencialidad	Divulgación de información	Manejo con discreción de información	e
		46	Pérdida de datos	Divulgación de información	Respaldos	m
		48	Poca adaptación a cambios del sistema	Sistema inestable y de difícil modificación	Metodología de análisis y desarrollo	e
		57	Software desactualizado	Probabilidad incremental de vulnerabilidades y virus	Mantenimiento y actualización constante	m
		58	Software sin licencia	Multas y problemas con legalización del software	Compra de software licenciado	e
		66	Virus, gusanos y caballos de Troya	Inestabilidad y mal funcionamiento del sistema	Antivirus	e

Cuadro 2.12: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
19	Backup	6	Backups (Mala configuración del schedule)	Falta de copias de respaldo	Mantener una agenda de backups	d
		8	Backups perdidos o inexistentes	Incapacidad de restaurar el sistema en caso emergente, discontinuidad del sistema, retraso del sistema	Backups incrementales	d
		15	Copia no autorizada de un medio de datos	Robo de información	Control de seguridad física, almacenamiento de los backups en un medio seguro	d
		32	Falta de espacio de almacenamiento	Falla en la generación de los backups	Existencia de medios redundantes	d
		39	Mala integridad de los datos	Errores durante la restauración de los datos	Backups incrementales	d
		43	Medios de datos no están disponibles cuando son necesarios	Pérdida de backups, retraso del sistema	Backups incrementales	d
		53	Robo	Incapacidad de restaurar el sistema, divulgación de información	Controles de acceso físico	d
		54	Rótulos inadecuados en medios magnéticos	Errores durante la restauración de los datos	Rótulos capaces de diferenciar cada medio de datos como único	d
		61	Transporte inseguro de archivos	Pérdida de información	Seguridad física	m
		66	Virus, gusanos y caballos de Troya	Pérdida de información	Antivirus	e
		68	Incendio	Perdida de información, imposibilidad de restaurar la información		d

Cuadro 2.13: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
20	Datos de configuración	2	Acceso a datos no autorizado	Divulgación de información de configuración del equipamiento, aumento de vulnerabilidades en el sistema	Controles de seguridad físicos, controles de acceso lógicos	e
		9	Borrado, modificación o revelación desautorizada o inadvertida de información	Pérdida de información, divulgación de información, aumento de vulnerabilidad en la seguridad	Controles de seguridad físicos, controles de acceso lógico, almacenamiento adecuado de la información	e
		15	Copia no autorizada de un medio de datos	Robo de información	Controles de seguridad física, controles de acceso lógico	e
		31	Falta de confidencialidad	Medidas de seguridad inservibles	Almacenamiento adecuado de la información y no divulgación de información de configuración	e
		44	Modificación de datos no autorizada	Pérdida de configuración de los equipos, incapacidad de administrar los recursos en ausencia de la persona que realizó el cambio	Cambios controlados, con conocimiento de las personas que requieran conocer los cambios	e
		66	Virus, gusanos y caballos de Troya	Pérdida o modificación de información, pérdida de productividad	Antivirus	e

Cuadro 2.14: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
21	Administración del centro de cómputo (Departamento de sistemas).	2	Acceso a datos no autorizado	Pérdida de información, manipulación de información, borrado de información	Seguridad lógica	e
		3	Acceso físico no autorizado	Manipulación de equipamiento	Seguridad física	m
		4	Administración impropia de los recursos dependiendo de los roles y las responsabilidades	Asignación impropia de los roles	Designación de tareas y segregación de funciones	m
		5	Almacenamiento de contraseñas negligente	Uso y abuso de los derechos que le otorga el contraseña	Seguridad lógica, políticas de contraseñas	e
		25	Errores de configuración y operación	Inestabilidad del sistema, perdida de rendimiento del sistema, aumento de las vulnerabilidades	Mantenimiento por personal con conocimiento	e
		29	Falta de auditorías	Imposibilidad de seguimiento de usuarios y generación de reportes	Existen logs generados automáticamente por el sistema operativo y aplicaciones principales	e
		36	Mal uso de derechos de administrador	Todos los administradores tienen acceso a toda la administración		d
		37	Configuración impropia del servicio de Mail	Tráfico de virus a través de archivos adjuntos	Capacitación sobre la herramienta	e
		38	Mala evaluación de datos de auditoría	Desconocimiento de eventos relevantes como: detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría	Lectura de ciertos logs	m

Cuadro 2.15: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
22	Red, cableado red LAN.	13	Configuración inadecuada de componentes de red	Inestabilidad del sistema, reducción del rendimiento, aumento de las vulnerabilidades	Cambios realizados por personal capacitado en el manejo de los equipos	e
		17	Daño de cables inadvertido	Segmentos de la red sin servicio	Cableado estructurado	e
		18	Denial of service	Interrupción de todos o de algunos servicios de red.		
		19	Destrucción o mal funcionamiento de un componente	Segmentos de la red sin servicio	Equipamiento fuera del alcance de personas	e
		31	Falta de confidencialidad	Quebrantamiento de las normas de seguridad	Manejo de información confidencial con mucha discreción	e
		33	Incumplimiento con las medidas de seguridad del sistema	Desastre informático	Información sensible manejada con mucha responsabilidad y discreción	e
		35	Longitud de los cables de red excedida	Transmisión de datos con interferencias, pérdida de conexión	Cableado estructurado normalizado y probado	e
		50	Registro de red desactualizado	Pérdida de tiempo	Actualización del registro de acuerdo a cambios	e
		52	Riesgo por el personal de limpieza o personal externo	Daño o desconexión de equipos	Equipamiento protegido y fuera del alcance de terceros	e

Cuadro 2.16: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
23	Red eléctrica	3	Acceso físico no autorizado	Pérdida del servicio de energía eléctrica	Los tableros principales se encuentran en un área segura y fuera del alcance de terceros	e
		11	Conexión de cables inadmisible	Pérdida del servicio de energía eléctrica	Todas las conexiones nuevas son realizadas por técnicos contratados	e
		16	Corte de luz	Pérdida del servicio de energía eléctrica	Generador	e
		17	Daño de cables inadvertido	Perdida del servicio de energía eléctrica	Cableado interno y realizado por técnicos contratados	e
		40	Manipulación de los tableros de los circuitos eléctricos	Pérdida sectorizada del servicio de energía eléctrica		d
		50	Registro de red desactualizado	Imposibilidad de detectar un daño	Actualización continua del registro en base a los cambios realizados	e
		52	Riesgo por el personal de limpieza o personal externo	Pérdida sectorizada del servicio de energía eléctrica	Indicaciones sobre el uso de las tomas eléctricas para los equipos de limpieza	m

Cuadro 2.17: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
24	Usuarios.	2	Acceso a datos no autorizado	Divulgación o robo de información	Control de acceso lógico a unidades compartidas de los servidores	e
		3	Acceso físico no autorizado	Robo de equipamiento e insumos, divulgación de información	Controles de acceso físico	m
		5	Almacenamiento de contraseñas negligente	Control total de estaciones por parte de terceras personas	Capacitar y recalcar sobre el cuidado y discreción de información crítica	m
		9	Borrado, modificación o revelación desautorizada o inadvertida de información	Pérdida de seguridad de la información	Controles lógico de estaciones y aplicaciones	e
		10	Condiciones de trabajo adversas	Predisposición a distracción, bajo rendimiento de usuarios	Ambiente de trabajo cómodo	e
		19	Destrucción o mal funcionamiento de un componente	Pérdida de tiempo en reemplazo de componente	Redundancia de componentes (disco, teclado, mouse)	m
		20	Desvinculación del personal	Robo o modificación de información, sabotaje interno		d
		21	Documentación deficiente o faltante	Mayor probabilidad de errores por falta de instrucciones		d
		22	Entrenamiento de usuarios inadecuado	Predisposición a errores y bajo rendimiento	Capacitación continua a los usuarios	m
		29	Falta de auditorías	Falta de concienciación sobre responsabilidades y seguridad		d
		33	Incumplimiento con las medidas de seguridad del sistema	Medidas correctivas tomadas por las autoridades, según la gravedad del incidente	Permanente concienciación de los usuarios	d
		36	Mal uso de derechos de administrador	Robo o modificación de información, sabotaje interno	Protección de claves y acceso de administrador	e
		45	Pérdida de confidencialidad en datos privados	Pérdida de características básicas de la información, errores en la información, conocimiento de la información por terceros	Controles lógicos de acceso a datos	m

Cuadro 2.18: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
25	Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	2	Acceso a datos no autorizado	Pérdida de confidencialidad, integridad y disponibilidad de la información	Control de acceso físico a instalaciones y áreas de documentación en general	e
		9	Borrado, modificación o revelación desautorizada o inadvertida de información	Documentación incorrecta, divulgación de información	Control de acceso físico a instalaciones y áreas de documentación en general	e
		15	Copia no autorizada de un medio de datos	Divulgación de información	Controles de acceso físico	m
		21	Documentación deficiente o faltante	Entorpecimiento de la administración y uso del sistema	Creación de manuales y documentación en general	m
		27	Factores ambientales	Destrucción de información	Archivos de documentación seguros	m
		43	Medios de datos no están disponibles cuando son necesarios	Pérdida de tiempo, demoras en el uso del sistema	Almacenamiento de datos en dispositivos probados	m
		44	Modificación de datos no autorizada	Errores en la información	Controles de acceso físico y lógico a medios de datos	m
		45	Pérdida de confidencialidad en datos privados	Divulgación de información	Controles de acceso físico y lógico a medios de datos	m
		46	Pérdida de datos	Pérdida de tiempo, demoras en el uso del sistema, indisponibilidad de la información	Controles de acceso físico de medios	m
		53	Robo	Divulgación de información	Controles de acceso físico y lógico a medios de datos	m

	54	Rótulos inadecuados en medios magnéticos	Información accesada errónea, demoras en uso de la información requerida	Rotulación adecuada y oportuna	m
	66	Virus, gusanos y caballos de Troya	Pérdida, modificación de la información, pérdida de productividad	Antivirus actualizado y bien configurado	e

Cuadro 2.19: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
26	Hardware (estaciones de trabajo impresoras de red)	3	Acceso físico no autorizado	Avería de partes, piezas o periféricos de las estaciones de trabajo, cambio de configuración física o lógica, robo o cambio de partes	Únicamente pueden acceder a las estaciones de trabajo personal de la dirección de informática o los usuarios asignados a cada equipo	m
		16	Corte de luz	Interrupción del funcionamiento del equipo	Generado, UPS	e
		19	Destrucción o mal funcionamiento de un componente	Interrupción de las tareas de los usuarios	Proveedores de servicios de mantenimiento	m
		34	Límite de vida útil - Máquinas obsoletas	Averías en los equipos, equipos lentos poco ágiles	Mantenimiento y configuración de acuerdo a sus limitaciones	m
		41	Mantenimiento ausente en el equipamiento informático	Avería de partes o piezas de las estaciones de trabajo	Mantenimiento calendarizado	
		42	Mantenimiento mal realizado en el equipamiento informático	Equipos mal configurados, funcionamiento anómalo de las estaciones de trabajo	Los equipos deben ser recibidos en conformidad de los usuarios finales	e
		52	Riesgo por el personal de limpieza o personal externo	Avería de partes o periféricos de las estaciones de trabajo	Instrucciones adecuadas al personal de limpieza sobre el manejo de los equipos e instalaciones	m
		53	Robo	Pérdida del equipamiento	Controles de acceso físico	m
		62	UPS de cada equipo descargado	Discontinuidad en el trabajo, molestias, borrado de información, inoportunidad en la prestación de atención al usuario final	Revisión continua de UPS	m
		65	Variaciones de voltaje	Interrupción del funcionamiento del equipo	UPS	m
		67	Ingerir alimentos, bebidas o fumar	Avería de teclado, mouse o estación ene general	Recalcar en no ingerir alimentos o bebidas mientras se usa las estaciones de trabajo	m

Cuadro 2.20: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
27	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	3	Acceso físico no autorizado	Daño de los insumos	Protección física	e
		27	Factores ambientales	Destrucción o avería de insumos	Respaldo de insumos	e
		34	Límite de vida útil - Máquinas obsoletas	Destrucción o avería de insumos	Respaldo de insumos	e
		53	Robo	Pérdida de insumos	Seguridad física	e
		68	Incendio	Pérdida de insumos		d

Cuadro 2.21: (Activos y factores de riesgos)

Nº	Nombre del activo	Nº	Factor de Riesgo	Consecuencias	Tipo de Protección	Es efectiva?
28	Información procesada de usuarios.	32	Falta de espacio de almacenamiento	Retraso de las actividades	Capacidad de almacenamiento sobredimensionado	e
		43	Medios de datos no están disponibles cuando son necesarios	Retraso de las actividades	Verificación de los medios antes de sacar un respaldo	m
		45	Pérdida de confidencialidad en datos privados	Divulgación de información	Controles de acceso lógico y físico a las estaciones de trabajo	e
		53	Robo	Divulgación de información	Controles de acceso lógico y físico a las estaciones de trabajo	m
		59	Spoofing y sniffing	Divulgación, modificación o robo de información	Seguridad lógica	e
		66	Virus, gusanos y caballos de Troya	Pérdida y modificación de datos, pérdida de tiempo y productividad	Antivirus	e

4- ACTIVOS Y PROBABILIDAD DE OCURRENCIA

En los siguientes cuadros se representa, el activo, el factor de riesgo y la probabilidad de ocurrencia de estos riesgos.

Probabilidad de ocurrencia: representa la probabilidad de que ocurran los factores de riesgo mencionados, en una escala del 1 al 3.

Los factores de riesgo cuya probabilidad de ocurrencia es de valor 3, son los factores de mayor peligro por lo tanto sobre los cuales mayor atención debemos poner y trabajar para disminuir su incidencia sobre los activos.

Cuadro 2.22: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo	Nivel de importancia	Nº	Factor de Riesgo	Probabilidad de ocurrencia
2	Servidor 2	10	3	Acceso físico no autorizado	3
1	Servidor 1	10	66	Virus, gusanos y caballos de Troya	3
			2	Acceso a datos no autorizado	2
			19	Destrucción o mal funcionamiento de un componente	2
			63	UPS del centro de cómputo descargado	2
			16	Corte de luz	1
			25	Errores de configuración y operación	1
			34	Límite de vida útil – Máquinas obsoletas	1
			42	Mantenimiento mal realizado en el equipamiento informático	1
			44	Modificación de datos no autorizada	1
			53	Robo	1
			65	Variaciones de voltaje	1

Cuadro 2.23: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
3	Servidor 3	10	3	Acceso físico no autorizado	3
			66	Virus, gusanos y caballos de Troya	3
			2	Acceso a datos no autorizado	2
			19	Destrucción o mal funcionamiento de un componente	2
			63	UPS del centro de cómputo descargado	2
			16	Corte de luz	1
			25	Errores de configuración y operación	1
			34	Límite de vida útil - Máquinas obsoletas	1
			42	Mantenimiento mal realizado en el equipamiento informático	1
			44	Modificación de datos no autorizada	1
			53	Robo	1
			65	Variaciones de voltaje	1

Cuadro 2.24: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
4	Switch principal 4900SX	10	3	Acceso físico no autorizado	3
5	Switch 4228G	10	36	Mal uso de derechos de administrador	3
6	Switch 4226T	10	11	Conexión de cables inadmisible	2
7	Switch 4250T	10	13	Configuración inadecuada de componentes de red	2
8	Hubs	10	19	Destrucción o mal funcionamiento de un componente	2
			50	Registro de red desactualizado	2
			63	UPS del centro de cómputo descargado	2
			4	Administración impropia de los recursos dependiendo de los roles y las responsabilidades	1
			16	Corte de luz	1
			25	Errores de configuración y operación	1
			34	Límite de vida útil - Máquinas obsoletas	1
			44	Modificación de datos no autorizada	1

Cuadro 2.25: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
9	UPS del centro de cómputo	7	3	Acceso físico no autorizado	3
			19	Destrucción o mal funcionamiento de un componente	2
			41	Mantenimiento ausente en el equipamiento informático	2
			16	Corte de luz	1
			53	Robo	1

Cuadro 2.26: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
10	Sistema de aire acondicionado edificio Roca	4	3	Acceso físico no autorizado	3
11	Sistema de aire acondicionado edificio Tocuyo	4	19	Destrucción o mal funcionamiento de un componente	2
			41	Mantenimiento ausente en el equipamiento informático	2
			16	Corte de luz	1
			25	Errores de configuración y operación	1
			27	Factores ambientales	1
			42	Mantenimiento mal realizado en el equipamiento informático	1

Cuadro 2.27: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
12	Equipo ADSL	6	3	Acceso físico no autorizado	3
			68	Incendio	3
			11	Conexión de cables inadmisible	2
			5	Almacenamiento de contraseñas negligente	1
			16	Corte de luz	1
			18	Denial of service	1
			25	Errores de configuración y operación	1
			53	Robo	1

Cuadro 2.28: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
13	Firewall	9	3	Acceso físico no autorizado	3
			68	Incendio	3
			11	Conexión de cables inadmisible	2
			13	Configuración inadecuada de componentes de red	2
			63	UPS del centro de cómputo descargado	2
			5	Almacenamiento de contraseñas negligente	1
			16	Corte de luz	1
			25	Errores de configuración y operación	1
			44	Modificación de datos no autorizada	1

Cuadro 2.29: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
14	Central telefónica	8	3	Acceso físico no autorizado	3
			7	Backups desactualizados	3
			21	Documentación deficiente o faltante	3
			29	Falta de auditorías	3
			2	Acceso a datos no autorizado	2
			8	Backups perdidos o inexistentes	2
			4	Administración impropia de los recursos dependiendo de los roles y las responsabilidades	1
			5	Almacenamiento de contraseñas negligente	1
			16	Corte de luz	1
			17	Daño de cables inadvertido	1
			25	Errores de configuración y operación	1

Cuadro 2.30: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
15	Gabinete 1	10	3	Acceso físico no autorizado	3
16	Gabinete 2	10	12	Conexiones todavía activas	3
			11	Conexión de cables inadmisible	2
			23	Equipos informáticos con escasos medios físicos de protección	2
			50	Registro de red desactualizado	2
			16	Corte de luz	1

Cuadro 2.31: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
17	Bases de datos	9	66	Virus, gusanos y caballos de Troya	3
			8	Backups perdidos o inexistentes	2
			15	Copia no autorizada de un medio de datos	2
			6	Backups (Mala configuración del schedule)	1
			26	Errores de software	1
			28	Falla de las base de datos	1
			32	Falta de espacio de almacenamiento	1
			39	Mala integridad de los datos	1
			45	Pérdida de confidencialidad en datos privados	1
			47	Pérdida de datos en tránsito	1
			53	Robo	1
			60	Transferencia de datos incorrectos o no deseados	1

Cuadro 2.32: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
18	Software de aplicación, programas fuente, sistemas operativos	6	66	Virus, gusanos y caballos de Troya	3
			2	Acceso a datos no autorizado	2
			14	Conocimiento insuficiente de los documentos de requerimientos en el desarrollo	2
			58	Software sin licencia	2
			30	Falta de compatibilidad	1
			31	Falta de confidencialidad	1
			46	Pérdida de datos	1
			48	Poca adaptación a cambios del sistema	1
			57	Software desactualizado	1

Cuadro 2.33: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
19	Backup	9	66	Virus, gusanos y caballos de Troya	3
			8	Backups perdidos o inexistentes	2
			15	Copia no autorizada de un medio de datos	2
			6	Backups (Mala configuración del schedule)	1
			32	Falta de espacio de almacenamiento	1
			39	Mala integridad de los datos	1
			43	Medios de datos no están disponibles cuando son necesarios	1
			53	Robo	1
			54	Rótulos inadecuados en medios magnéticos	1

Cuadro 2.34: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
20	Datos de configuración	8	66	Virus, gusanos y caballos de Troya	3
			2	Acceso a datos no autorizado	2
			15	Copia no autorizada de un medio de datos	2
			9	Borrado, modificación o revelación desautorizada o inadvertida de información	1
			31	Falta de confidencialidad	1
			44	Modificación de datos no autorizada	1

Cuadro 2.35: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
21	Administración del centro de cómputo (Departamento de sistemas).	9	3	Acceso físico no autorizado	3
			29	Falta de auditorías	3
			36	Mal uso de derechos de administrador	3
			38	Mala evaluación de datos de auditoría	3
			2	Acceso a datos no autorizado	2
			37	Configuración impropia del servicio de Mail	2
			4	Administración impropia de los recursos dependiendo de los roles y las responsabilidades	1
			5	Almacenamiento de contraseñas negligente	1
			25	Errores de configuración y operación	1

Cuadro 2.36: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
22	Red, cableado red LAN.	8	13	Configuración inadecuada de componentes de red	2
			19	Destrucción o mal funcionamiento de un componente	2
			33	Incumplimiento con las medidas de seguridad del sistema	2
			50	Registro de red desactualizado	2
			17	Daño de cables inadvertido	1
			31	Falta de confidencialidad	1
			35	Longitud de los cables de red excedida	1
			52	Riesgo por el personal de limpieza o personal externo	1

Cuadro 2.37: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
23	Red eléctrica	8	3	Acceso físico no autorizado	3
			40	Manipulación de los tableros de los circuitos eléctricos	3
			11	Conexión de cables inadmisible	2
			50	Registro de red desactualizado	2
			16	Corte de luz	1
			17	Daño de cables inadvertido	1
			52	Riesgo por el personal de limpieza o personal externo	1

Cuadro 2.38: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
24	Usuarios.	5	3	Acceso físico no autorizado	3
			21	Documentación deficiente o faltante	3
			29	Falta de auditorías	3
			36	Mal uso de derechos de administrador	3
			2	Acceso a datos no autorizado	2
			19	Destrucción o mal funcionamiento de un componente	2
			22	Entrenamiento de usuarios inadecuado	2
			33	Incumplimiento con las medidas de seguridad del sistema	2
			5	Almacenamiento de contraseñas negligente	1
			9	Borrado, modificación o revelación desautorizada o inadvertida de información	1
			10	Condiciones de trabajo adversas	1
			20	Desvinculación del personal	1
			45	Pérdida de confidencialidad en datos privados	1

Cuadro 2.39: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
25	Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.	4	21	Documentación deficiente o faltante	3
			66	Virus, gusanos y caballos de Troya	3
			2	Acceso a datos no autorizado	2
			15	Copia no autorizada de un medio de datos	2
			9	Borrado, modificación o revelación desautorizada o inadvertida de información	1
			27	Factores ambientales	1
			43	Medios de datos no están disponibles cuando son necesarios	1
			44	Modificación de datos no autorizada	1
			45	Pérdida de confidencialidad en datos privados	1
			46	Pérdida de datos	1
			53	Robo	1
			54	Rótulos inadecuados en medios magnéticos	1

Cuadro 2.40: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
26	Hardware (estaciones de trabajo impresoras de red)	4	3	Acceso físico no autorizado	3
			67	Ingerir alimentos, bebidas o fumar	3
			19	Destrucción o mal funcionamiento de un componente	2
			41	Mantenimiento ausente en el equipamiento informático	2
			62	UPS de cada equipo descargado	2
			16	Corte de luz	1
			34	Límite de vida útil - Máquinas obsoletas	1
			42	Mantenimiento mal realizado en el equipamiento informático	1
			52	Riesgo por el personal de limpieza o personal externo	1
			53	Robo	1
			65	Variaciones de voltaje	1

Cuadro 2.41: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
27	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	3	3	Acceso físico no autorizado	3
			68	Incendio	3
			27	Factores ambientales	1
			34	Límite de vida útil - Máquinas obsoletas	1
			53	Robo	1

Cuadro 2.42: (Activos, factores de riesgo y probabilidad de ocurrencia)

Nº	Nombre del activo		Nº	Factor de Riesgo	Probabilidad de ocurrencia
28	Información procesada de usuarios.		66	Virus, gusanos y caballos de Troya	3
			32	Falta de espacio de almacenamiento	1
			43	Medios de datos no están disponibles cuando son necesarios	1
			45	Pérdida de confidencialidad en datos privados	1
			53	Robo	1
			59	Spoofing y sniffing	1

CAPITULO III

PLAN MAESTRO DE SEGURIDAD

GENERALIDADES

ALCANCE

Este documento se aplica para todos los funcionarios del Ministerio Público, así también a organizaciones y personas externas que colaboren prestando un servicio o producto.

VIGENCIA

El Plan de Seguridad Informática entrará en vigencia a partir de la fecha de su aprobación por parte de la máxima autoridad de la Institución.

INTERVALO DE LA VIGENCIA

Un intervalo tentativo de la vigencia del Plan será de dos años a partir de la aprobación del presente documento.

RESPONSABILIDADES

- Los usuarios son responsables de cumplir con todas las políticas de la Institución relativas a la seguridad informática y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar[8] información confidencial de la Institución a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Institución a personas no autorizadas.
- No utilizar los recursos[9] informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con las actividades en la Institución.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares o grupo de trabajo.
- Reportar inmediatamente a su jefe inmediato y a un funcionario de la Dirección Nacional de Informática cualquier evento que pueda comprometer la seguridad de la Institución y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

- Se debe designar un encargado de Seguridad quien es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

[8] "La divulgación o la utilización fraudulenta de la información protegida" esta tipificada y penada el el primer artículo innumerado, agregado después del Art. 202 del Código Penal, mediante reforma contenida en el Art. 58, Título V, de la Ley de Comercio Electónico, Firmas y Mensajes de Datos, publicada en el Registro Oficial No. 557, de 17 de abril del 2002. Ver texto de la ley en el anexo 3.

[9] El uso de los recursos y materiales de la Institución deben apegarse a las normas que se indican en el Reglamento General de la Administración de los Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, Literal a. Ver anexo 3.

- El encargado de la administración de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso, y llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto.
- La Dirección Nacional de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad informática a lo largo de toda la organización. También es responsable de evaluar, gestionar la adquisición e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y operativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

1 - SEGURIDAD FÍSICA

1.1 EQUIPAMIENTO

- Debe existir una adecuada protección física y mantenimiento permanente de los equipos e instalaciones que conforman los activos de la Institución.

- Los equipos de la Institución sólo deben usarse[10] para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos[11].

- Debe respetarse y no modificar la configuración de hardware y software establecida por la Dirección Nacional de Informática.

- No se permite fumar, comer o beber mientras se está usando una estación de trabajo.

- Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

[10] El uso de los recursos y materiales de la Institución deben apegarse a las normas que se indican en el Reglamento General de la Administración de los Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, Literal a. Ver anexo 3.

[11] Los juegos y pasatiempos no están permitidos en horas laborables, lo indica el Reglamento General de la Administración de Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, literal n. Ver anexo 3.

- Cualquier falla en los computadores o en la red debe reportarse inmediatamente al personal de la Dirección Nacional de Informática ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

- Ningún equipo que pertenece a la Institución puede moverse o ser reubicado sin permiso. Para llevar un equipo fuera de la Institución se requiere una autorización escrita emitida por parte del Director Nacional de Informática o un funcionario encargado.

- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso.

- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada a la Dirección Nacional de Informática inmediatamente.

- Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que se les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la Institución.

- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño.

1.2 CONTROL DE ACCESO FÍSICO AL CENTRO DE COMPUTO

- Únicamente los funcionarios de la Dirección Nacional de Informática tienen acceso al **área del centro de cómputo** donde se encuentran los servidores, los switches de comunicaciones y demás equipamiento crítico.

- Ninguna persona sin autorización previa podrá ingresar al área del **centro de cómputo,** para reducir el riesgo de accidentes y actividades fraudulentas.

- Toda persona que ingrese a las áreas restringidas, debe registrarse y requerirá autorización para ingresar.

- Cualquier **persona ajena a la Institución** que necesite ingresar al centro de cómputo deberá anunciarse en la entrada de la dirección, un personal de sistemas lo escoltará desde la puerta hacia el interior del centro de cómputo y lo acompañará durante el transcurso de su tarea, hasta que ésta concluya.

- La puerta de acceso al centro de cómputo permanecerá siempre cerrada y con llave.

- El personal podrá permanecer en las instalaciones de la Institución durante el **horario autorizado.** Se deberá establecer un procedimiento de autorización para el personal que deba permanecer fuera de su horario habitual de trabajo.

- Se realizará un adecuado mantenimiento y **prueba de los procedimientos** para la restricción de acceso físico.

1.3 CONTROL DE ACCESO A EQUIPOS

- Las **disqueteras** en aquellas máquinas en que no se puede instalar la herramienta antivirus, estarán deshabilitadas.

- Las estaciones de trabajo de la Institución deben tener una contraseña de administrador en el **BIOS**, que deberán gestionar los funcionarios del área de Sistemas.

- Cualquier **dispositivo externo como fax modems, equipos de comunicación y otros** que no se encuentren en uso, permanecerán guardados bajo llave dentro del centro de cómputo.

- El rack de los servidores siempre estará asegurado con llave.

- Los **gabinetes** donde se ubican los switches, permanecerán con llave, y fuera del alcance de personal no autorizado.

- Se debe instruir a los funcionarios de las oficinas, donde se encuentran los gabinetes, sobre la importancia de ellos.

- Un funcionario encargado, realizará chequeos periódicos para comprobar:
    - Que las estaciones de trabajo se encuentren conectadas al circuito eléctrico que corresponde al equipo computacional, las placas de color tomate identifican al circuito,
    - La correcta instalación de los dispositivos de los equipos y,
    - El buen funcionamiento de los dispositivos.

1.4 DISPOSITIVOS DE SOPORTE

Deben existir los siguientes **dispositivos de soporte** en la Institución.

- **Aire acondicionado y calefacción:** debe existir un equipo de precisión que sea capaz de mantener la temperatura y humedad adecuadas dentro del centro de cómputo. La temperatura debe mantenerse entre 19º C y 20º C.

- **Extintor de incendios**: deben ser dispositivos a gas y automáticos o químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos de computación, deberán estar instalados en lugares estratégicos de la Institución, el centro de cómputo deberá contar con uno propio.

- **Generador de energía:** debe existir un generador de energía que se pondrá en marcha cada vez que hay problemas con el suministro normal de energía eléctrica.

- **UPS**: (Ininterrumpible Power Supply) debe existir al menos un UPS que pueda mantener funcionando todos los equipos de comunicaciones y servidores que se encuentran en el centro de cómputo y gabinetes.

- **Descarga a tierra**: Deben instalarse métodos de descarga a tierra.

- Todos estos dispositivos deberán ser **evaluados periódicamente** por personal de mantenimiento.

- Deberán existir procedimientos detallados a seguir por el personal en **caso de emergencia**s, indicando responsables, quienes deben estar adecuadamente capacitados.

2 - ADMINISTRACIÓN DEL CENTRO DE COMPUTO

2.1 ADMINISTRACIÓN DEL CENTRO DE COMPUTO

- La Institución debe brindar el soporte necesario con el fin de asegurar la correcta **organización y administración** del área de sistemas a fin de que ésta brinde condiciones generales de operación que posibiliten un ambiente adecuado de control.

- Debe designarse un **encargado de la seguridad** del sistema, que coordine las tareas correspondientes, haciendo cumplir las políticas de seguridad en toda la Institución.

- Debe existir un encargado de llevar a cabo el **mantenimiento preventivo** del equipamiento informático de la Institución, monitoreando, chequeando y auditando las estaciones de trabajo y demás dispositivos que conforman la red.

- Debe generarse un **inventario** detallado donde se describan los sistemas de información y de los equipos de cómputo utilizados en la Institución. Debe asignarse un responsable de mantenerlo actualizado y de realizar controles periódicos.

- Debe existir una **planificación** formalizada y completa de las actividades que se desarrollan normalmente. Deberán designarse responsabilidades claras y documentadas para cada actividad.

- Debe desarrollarse un plan de sistemas a **corto plazo**, que contenga un cronograma de las actividades, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un periodo de un año.

- Debe desarrollarse un plan estratégico a **largo plazo**, que contenga los proyectos principales y los cronogramas de su implementación, para un periodo de por lo menos 3 años.

- Deben generarse **reportes** trimestrales y evaluar el progreso de los planes propuestos y el cumplimiento de las políticas impuestas.

- El equipo de sistemas debe hacer hincapié en la toma de conciencia de todos los usuarios, generando una **cultura de la seguridad**, haciéndolos partícipes de las medidas de seguridad, tanto a los usuarios actuales como a los que se incorporen en el futuro. Este proceso debe ser renovado y transmitido a los usuarios en forma anual.

- Debe implementarse un **buzón de sugerencias o implementar encuestas** donde los usuarios recomienden mejoras o realicen comentarios, expresando sus inquietudes.

- Debe existir un procedimiento para realizar la **publicidad** de políticas, planes o normas de la Institución y sus modificaciones.

- Los administradores deben informar el tiempo de **suspensiones** en el servicio necesarias por mantenimiento, especificando fecha, hora y duración de la suspensión.

- Deberán existir procesos para **rotula**r, manipular y dar de baja el equipamiento informático.

- Los **medios de instalación originales** del software deberán respaldarse[12] y resguardarse adecuadamente, en caso de que no sean de solo lectura, siempre se mantendrán con las protecciones contra escritura que estén disponibles para el medio. En la medida de lo posible se evitará instalar el software directamente de los medios originales.

- Debe existir un procedimiento para controlar que en la Institución solamente se utilicen productos de **software**[13] adquiridos por vías legales.

[12] La persona que adquiere software lícitamente, está autorizado para obtener una copia para seguridad o resguardo únicamente, de conformidad a lo dispuesto en el Art. 30, literal a), de la ley de Propiedad Intelectual. Ver anexo 3.

[13] La legalidad del software se desprende de la observancia de las normas especiales relativas a programas de ordenador contempladas en los Arts. 11, 18, 19 y sgts., 28, 29, 30 y 31; así como también en las normas de la Competencia Desleal, contempladas en el Libro IV de la Ley de Propiedad Intelectual, con relación a la responsabilidad civil y penal por violación a los derechos de autor y a la titularidad de los derechos de autor, especialmente los Arts. 284 al 318 y 234 al 331; y Tutela Administrativa. Libro V Ley de Propiedad Intelectual Arts 332 al 345. . Ver texto legal en el anexo 3.

2.2 CAPACITACIÓN

- El personal de la **Dirección Nacional de Informática** debe mantenerse capacitado respecto de las tecnologías utilizadas en la Institución.

- Debe **impartirse capacitación** a los usuarios finales a efectos de que puedan operar adecuadamente los recursos informáticos.

- El personal debe ser entrenado respecto al cumplimiento de lo especificado en las **políticas de seguridad** informática. Se debe entregar una copia de la misma a cada funcionario.

- Asegurar que los funcionarios reciban **capacitación continua** para desarrollar y mantener sus conocimientos, habilidades y toma de conciencia en materia de seguridad informática dentro del nivel requerido a fin de lograr un desempeño eficaz.

2.3 RESPALDO

- El procedimiento de generación del respaldo debe estar **automatizado** con alguna herramienta de generación de copias de resguardo de datos.

- Debe existir un **procedimiento** aprobado para la generación periódica de respaldos sobre toda la información necesaria para las operaciones de la Institución, donde se

especifique la unidad de la cual se obtiene el respaldo, la periodicidad y el lugar físico donde se deben mantener las copias generadas.

- La **periodicidad** de la generación de los respaldos depende de la frecuencia de los cambios.

- La **ubicación** de los respaldos debe contar con adecuadas medidas de seguridad. Los respaldos de configuración de los servidores, programas y datos vitales para la operación de la Institución deben guardarse en otra sede, lejos del edificio, de ser transportados será necesario un medio resistente que los proteja.

- Deben generarse copias de respaldo de las **configuraciones de los servidore**s, documentando las modificaciones realizadas para identificar las distintas versiones. Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las **versiones autorizadas anteriores.**

- Debe designarse un **responsable** y un suplente encargados de la obtención, restauración y custodia de los respaldos, y se generará un registro de los **movimientos** de estos medios.

- Los archivos de respaldo deben tener un **control de acceso** lógico de acuerdo a la sensibilidad de sus datos, además de contar con protección física.

- Debe realizarse chequeos para comprobar el funcionamiento correcto de los **medios externos** donde se realizan las copias de respaldo. Además se debe llevar

un control para reemplazo de los medios externos de almacenamiento, de manera de sustituirlos antes de su degradación física

- Debe rotularse todo medio externo de almacenamiento de datos.

- Debe existir un **procedimiento de recuperación** de copias de respaldo, donde se incluya la metodología a seguir y el responsable de su realización. Deberán realizarse **chequeos** para comprobar que los procedimientos de restauración son eficientes.

- Se debe llevar un **inventario** actualizado de las copias de respaldo.

- Se deberá generar una copia de respaldo de toda la **documentación** del centro de cómputo, incluyendo el hardware, el software, y el plan de contingencias, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.

2.4 DOCUMENTACIÓN

- Debe generarse un **soporte** de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Debe asignarse un **responsable** a cargo de la gestión de la documentación en el centro de cómputo.

- Debe desarrollarse documentación detallada referente al equipamiento informático, que consista en diagramas y distribución física de las instalaciones y equipos, **inventarios** de hardware y software y diagramas topológicos de las redes.

- Debe existir un registro de los eventos, **errores** y problemas del hardware y del software a los que se enfrentan diariamente los técnicos.

- Esta documentación debe mantenerse actualizada.

3 - SEGURIDAD DE LAS APLICACIONES

3.1 SOFTWARE DE SERVIDORES

- El sistema operativo de los servidores presenta las siguientes características:
    - Alta confiabilidad,
    - Compatibilidad e interoperatividad con los sistemas operativos de las estaciones de trabajo y demás sistemas usados en la Institución,
    - Escalabilidad,
    - Disponibilidad de software de aplicación y actualizaciones,
    - Buena administración y generación de logs,
    - Buen rendimiento (performance),
    - Cumplir con los requerimientos funcionales impuestos por la Institución,
    - Amigable con el usuario,
    - Disponibilidad de documentación.

- Además debe presentar las siguientes características en lo relativo a la seguridad:
    - Identificación y autenticación,
    - Control de acceso,
    - Ingreso a la red,
    - Fiabilidad,
    - Seguridad en la transmisión,
    - Respaldo de datos,
    - Encriptación,

- Funciones para preservar la integridad de datos,
- Requerimientos sobre privacidad de datos.

3.2 SEGURIDAD DE BASES DE DATOS

- Los archivos de la Institución, las carpetas donde se encuentran almacenados y las aplicaciones que los administran deben tener controles de acceso.

- Se debe verificar en cada estación de trabajo que únicamente tengan acceso a los sistemas y servicios autorizados.

- Debe hacerse chequeos regulares de la seguridad de la base de datos, en los que se debe verificar que:
    - se hacen y son efectivos los respaldos y los mecanismos de seguridad,
    - no haya usuarios de la base de datos que no tengan asignada una contraseña,
    - La base de datos y las aplicaciones que la administran tienen suficientes recursos libres para trabajar eficientemente.

- Los registros de la base de datos no se borrarán físicamente, sino que deben marcarse como eliminados.

- Deberá existir una clasificación de los datos en base a su sensibilidad para definirlos como críticos y así determinar controles específicos. Se deberán definir tres niveles de información:
    - Información Crítica:

- La no-disponibilidad de esta información ocasiona un daño en los activos de la Institución;
- Se considera recurso crítico a aquel recurso interno que debe estar disponible solamente para un conjunto determinado de personas, debe ponerse un cuidado especial en información que por ley o que por políticas de la Institución debe permanecer confidencial[14]; la clasificación de un recurso como crítico deberá incluir los criterios para determinar quienes tienen acceso a él. De ser necesaria su transmisión por redes externas o su almacenamiento en sistemas de la red perímetro, deberán tomarse medidas de seguridad extremas, la información deberá encriptarse;

- Información Confidencial:
  - En poder de personas no autorizadas compromete los intereses de la Institución;
  - Se considera recurso confidencial a todo aquel que solo debe utilizarse y ser del conocimiento de miembros de la Institución y por defecto todo aquel recurso que no haya sido explícitamente clasificado como disponible al público;

- Pública:
  - Información de libre circulación;

[14] Quién vulnera la confidencialidad de la información protegida, subsume su conducta a la conducta tipificada en el primer inciso del primer artículo innumerado agregado después del Art. 202 del Código Penal, mediante reforma contenida en el Art. 58, Título V, de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 557, de 17 de abril del 2002. Ver texto legal en el anexo 3.

- Se considera recurso disponible al público aquel que no requiere permanecer como de uso interno y que explícitamente se ha clasificado como un recurso público.

Esta clasificación deberá ser documentada e informada a todo el personal de la Institución, y deberá evaluarse y actualizarse periódicamente.

- Debe existir un responsable en cada área de la Institución, que responda por la información que se maneja en dicho sector. Debe definir la clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador del sistema.

3.3 CONTROL DE APLICACIONES EN ESTACIONES DE TRABAJO

- Debe existir estándares de configuración de las estaciones de trabajo, servidores y demás equipos de la red informática.

- En base al estándar se deberá generar un **procedimiento** donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario.

- Los usuarios deben asumir que todo el software la Institución está protegido por derechos de autor[15] y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Debe instalarse una herramienta antivirus, la cual debe mantenerse actualizada.

- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por la Dirección de Informática.

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de

[15] Los programas de ordenador (software), se protege por el régimen de derechos de autor, toda vez que, se consideran obras literarias, siendo procedente para tal protección de aplicación de las normas pertinentes del Libro I de la Ley de Propiedad Intelectual y especialmente las contenidas en los Arts. 28, 29, 30 y 31 de dicho cuerpo legal. Ver texto de estas normas jurídicas en el anexo 3.

distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Director de Informática.

- Debe utilizarse un programa antivirus para examinar todo software que venga de afuera de la Institución.

- No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la Institución a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

- Las **aplicaciones solo se actualizarán** cuando exista el reporte de algún mal funcionamiento o por un nuevo requerimiento por parte de los usuarios o del personal del centro de cómputo.

- Se deberán **documentar** no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se les realicen.

- En el momento en que un nuevo usuario ingrese a la Institución, se lo debe **notificar y deberá aceptar** que tiene prohibida la instalación de cualquier producto de software en los equipos.

- Se deberán realizar **chequeos periódicos** en las estaciones de trabajo, los servidores y demás equipos, en búsqueda de aplicaciones instaladas no autorizadas o innecesarias.

- Antes de hacer un cambio en la configuración de los servidores se deberá hacer un **respaldo de la configuración existente**. Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.

- Se deberá establecer un **procedimiento de emergencia de los servidores** para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores en el caso de generarse problemas.

3.4 CONTROL DE DATOS EN LAS APLICACIONES

- Los datos de entrada y salida a los diferentes sistemas son validados en cada sistema e ingresados solo desde las estaciones de trabajo con los permisos de acceso necesarios.

- Los datos de salida de los diferentes sistemas utilizados en la Institución son restringidos con controles lógicos, de acuerdo a los permisos de acceso.

- Todas las aplicaciones y sus archivos deben poseer controles de acceso y solo el administrador debe tener acceso a ellas.

- Se debe sincronizar fecha y hora en todas las estaciones de trabajo y servidores conectadas a la red, asegurando de esta manera consistencia de los datos de las aplicaciones.

3.5 CICLO DE VIDA DE LAS APLICACIONES

- Debe utilizarse un plan detallado de sistemas, donde se definan las asignaciones de recursos, el establecimiento de prioridades y responsabilidades, la administración de tiempos. Esta norma debe aplicar tanto para el desarrollo de las aplicaciones como para las modificaciones que se realicen.

- Debe existir un documento formal de solicitud de cambios, donde quede reflejado el motivo y la solicitud del cambio, allí se agregarán los requerimientos de seguridad necesarios, definidos por el responsable de la información y el administrador de sistemas. La documentación de los cambios debe incluir:
    - Sistema que afecta,
    - Fecha de la modificación,
    - Desarrollador que realizó el cambio,
    - Funcionario que solicitó el cambio,
    - Descripción global de la modificación.

- El formulario anterior se utilizará para actualizar la documentación del desarrollo y de los distintos manuales generados.

- Todo nuevo desarrollo o modificación deber estar probado y aprobado por los usuarios del mismo antes de su instalación en el ambiente de trabajo.

- Se deberá informar por escrito la importancia de la seguridad de la información a todo el personal contratado y terceros. El Director Nacional de Informática, junto con los directivos, serán quienes:
    - Especifiquen los requerimientos de seguridad,
    - Determinen los pasos a seguir en caso que no se respete lo establecido en el contrato,
    - Establezcan cláusulas sobre confidencialidad de la información.

- Los contratos con terceros deberán contener una cláusula que indique “Derecho de auditar su desempeño”.

- Con respecto a la contratación de terceros para el desarrollo de aplicaciones, éste deberá entregar a la Institución:
    - Aplicación ejecutable,
    - Código fuente de la aplicación,
    - Documentación del desarrollo,
    - Manuales de uso.

- Antes de realizar la compra de una aplicación de software, deberá:
    - Realizarse un análisis de costo – beneficio,
    - Comprobar la adaptabilidad a los sistemas existentes en la Institución,
    - Verificar la compatibilidad con los sistemas operativos de la Institución,
    - Evaluar las medidas de seguridad que posee,
    - Solicitar la misma documentación que se exige a los terceros.

- Las modificaciones en los sistemas adquiridos, solo se realizarán por personal técnico de la Empresa a la que le pertenece el producto.

4 - SEGURIDAD LÓGICA

4.1 ASPECTOS GENERALES

- Cuando un usuario recibe una cuenta, se debe obtener un **compromiso firmado** por parte de los funcionarios respecto al cumplimiento de las medidas de seguridad definidas en las políticas de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad[16] de las claves de acceso, la no-divulgación[17] de información de la Institución, el cuidado de los recursos, la utilización de software[18] sin licencia, el reporte de situaciones anormales y la **aceptación de sus responsabilidades con relación al uso de esa cuenta**. Debe confirmarse este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas al personal.

- Las estaciones de trabajo deben tener instalado un **protector de pantalla con contraseña.**

[16] Este aspecto tiene relación con lo tipificado en el primer artículo innumerado, agregad después del Art. 202 del Código Penal, relativo a delitos contra la información protegida. Ver texto legal en el anexo 3.

[17] La divulgación o la utilización fraudulenta de la información protegida, es infracción informática y como tal se halla tipificada en el primer artículo innumerado agregado después del Art. 202 del Código Penal, relativo a delitos contra la información protegida. Ver texto legal en el anexo 3.

[18] La legalidad del software se desprende de la observancia de las normas especiales relativas a programas de ordenador contempladas en los Arts. 11, 18, 19 y sgts., 28, 29, 30 y 31; así como también en las normas de la Competencia Desleal, contempladas en el Libro V de la Ley de Propiedad Intelectual, con relación a la responsabilidad civil y penal por violación a los derechos y a la titularidad de los derechos de autor. Ver texto legal en el anexo 3.

- Cuando un funcionario es despedido o renuncia a la Institución, debe desactivarse su cuenta antes de que deje el cargo.

- Los privilegios otorgados a los usuarios deben ser ratificados cada año. El encargado de la Dirección de Sistemas debe bloquear la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un funcionario cesa en sus funciones.

4.2 IDENTIFICACION DE USUARIOS

- Debe existir una herramienta para la administración y el control de acceso a los datos.

- Debe existir una **política formal de control de acceso** a datos donde se detalle como mínimo:
    - El nivel de confidencialidad de los datos y su sensibilidad,
    - Los procedimientos de otorgamiento de claves de usuarios para el ingreso a los sistemas,
    - Los estándares fijados para la identificación y la autenticación de usuarios.

- Para **ingresar a un usuario** al sistema (**dar de alta**)debe existir un procedimiento formal, por escrito, que regule y exija el ingreso de los siguientes datos:
    - Nombres y apellidos completo,
    - Identificación del usuario, deberá ser única e irrepetible,
    - Unidad administrativa a la que pertenece,
    - Permisos de acceso.

- Cada cuenta de usuario debe contar con los permisos mínimos y necesarios que le permitan desempeñar su tarea.

- Debe restringirse el acceso al sistema o la utilización de recursos en un **rango de horario definido**, teniendo en cuenta que:

- Las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan,
- Durante las vacaciones o licencias las cuentas de usuarios deben desactivarse,
- En días feriados las cuentas de usuarios administrativos, deben permanecer desactivadas.

- El administrador del sistema debe realizar un chequeo mensual de los usuarios del sistema, comprobando que existen solo los usuarios que son necesarios y que sus permisos sean los correctos.

- Se debe bloquear el perfil de todo usuario que **no haya accedido al sistema** después de cierto período de inactividad. Se recomienda un período de 30 días.

- Se debe minimizar la generación y el uso de perfiles de **usuario con máximos privilegios**. Todos los usos de estas clases de perfiles deben ser registrados y revisados por el administrador de seguridad.

- Deberá existir un **administrador total del sistema**. Un **segundo** administrador (súper-usuario) debe ser creado con privilegios similares al anterior. Se creará un **tercer** perfil de administrador del sistema, con los permisos mínimos necesarios para la realización de tareas cotidianas del administrador. Ninguno de estos usuarios tendrá permitida la eliminación del usuario administrador total del sistema.

- Los administradores que realizan tareas de mantenimiento, deberán tener otro perfil, con un nivel de acceso menor, denominado **mantenimiento**, para ser utilizado en tareas cotidianas que no requieran privilegios de súper usuario.

- Si se realiza **mantenimiento externo**, deberá crearse una cuenta de usuario especial para esta tarea, con los permisos mínimos necesarios para desempeñar las funciones; una vez finalizado el mantenimiento el administrador del sistema deberá modificar la contraseña de esta cuenta. Cada vez que sea necesario realizar mantenimiento, el administrador deberá proporcionar esta clave al personal externo.

- Periódicamente el administrador del sistema deberá **chequear** las acciones desempeñadas con las cuentas de administradores y de mantenimiento.

- No debe concederse una cuenta a personas que no sean funcionarios de la Institución a menos que estén debidamente autorizados, en cuyo caso la cuenta deberá ser monitorizada y expirar automáticamente al cabo 5 días.

- Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.

- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Director de Informática o Jefe de Desarrollo de Sistemas determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo.

4.3 AUTENTICACIÓN

- La **pantalla de ingreso a la red (logeo)** debe mostrar los siguientes datos:
    - Nombre de usuario,
    - Contraseña,
    - Dominio.

- Mientras el usuario está **ingresando su contraseñ**a, esta no debe ser mostrada por pantalla.

- La **aplicación para administrar los datos de usuarios** solo debe ejecutarse en máquinas designadas del Centro de Cómputo.

4.4 CONTRASEÑAS (PASSWORDS)

- Las contraseñas deben incluir mayúsculas, minúsculas, números y caracteres especiales.

- La longitud mínima de una contraseña no debe ser menor de 8 caracteres.

- La **fecha de expiración** de las contraseñas deberá ser de 30 días. El sistema exigirá automáticamente el cambio, una vez cumplido el plazo.

- La contraseña **no deberá contener** el nombre de la empresa, el nombre del usuario, o palabras que sean asociadas con el usuario.

- Se debe bloquear el perfil de todo usuario que haya intentado **acceder al sistema en forma fallida** por más de **cinco** veces consecutivas.

- Se debe controlar que la contraseña ingresada sea **diferente a las últimas diez utilizadas**.

- La contraseña deberá tener un **período de duración mínimo** de 2 días. El sistema no permitirá el cambio de contraseña si este período no se ha cumplido.

- Si un usuario **olvida su contraseña**, el administrador eliminará la contraseña, y permitirá que el usuario ingrese una nueva desde su terminal, la próxima vez que ingrese a la red.

- No se debe compartir la contraseña a ningún usuario o administrador de la red, el compartir expone al usuario a las consecuencias por las acciones que otros hagan con esa contraseña.

- El usuario no debe guardar su contraseña en una forma legible y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.

- La contraseña inicial emitida a un nuevo usuario o a un usuario cuyo equipo ha sido reparado, sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como switches, firewalls, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

- Los usuarios no deben intentar violar[19] los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias[20] de las políticas de la Institución.

4.5 POLITICAS DE DOMINIO Y UNIDADES ORGANIZACIONALES

- Se deberá crear unidades organizacionales de acuerdo a las unidades administrativas para permitir ejercer un mejor control sobre las estaciones de trabajo que se encuentran dentro del dominio.

- Se debe quitar el menú archivo del Explorador de Windows, para evitar que el usuario acceda al menú Archivo.

[19] "El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida," será sancionado de acuerdo a lo que indican las reformas al Código Penal, de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, en su articulo innumerado después del artículo 202. Ver anexo 3.

[20] De las prohibiciones estipuladas en el Reglamento General de la Administración de Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, literal dice: i) "Incurrir en actos que impliquen abusos de confianza, fraude, estafa, robos y otros que signifiquen perjuicio para la Institución".

- Quitar el acceso a los menúes contextuales en la barra de tareas, con el fin de ocultar los mensajes que aparecen cuando se hace clic derecho en el menú Inicio y la barra de tareas.

- Ocultar el elemento Administrar del menú contextual del explorador de Windows, para evitar que los usuarios al presionar el botón derecho del ratón sobre Mi PC accedan a la opción de administrar.

- Quitar "Conectar a una Unidad de Red" y "Desconectar de Unidad de Red", impidiendo que los usuarios usen el Explorador de Windows o Mis sitios de red para asignar unidades de red o desconectarlas.

- Quitar el menú opciones de carpeta del menú herramientas, para evitar que los usuarios puedan usar las opciones de carpeta.

- Eliminar el Administrador de Tareas, para prevenir que los usuarios accedan a esta utilidad.

- Quitar vínculos y accesos a Windows Update, impidiendo que los usuarios accedan al sitio de Web Windows Update.

- Quitar Conexiones de red del menú inicio, para prevenir que los usuarios accedan a conexiones de red.

- Bloquear Barra de Tareas, para impedir al usuario mover o cambiar de tamaño a la barra de tareas.

- Impedir cambios en la Barra de Tareas y Menú Inicio, con esto se previene que los usuarios puedan sobrescribir cualquier cambio que realicen sobre el Menú Inicio.

- Prohibir el acceso al Panel de Control, para prevenir que los usuarios ejecuten o accedan al panel de control.

- Quitar el elemento Propiedades del Menú Contextual de Mi PC, de esta maneta la opción propiedades no estará presente cuando el usuario haga clic derecho en Mi PC.

- Prohibir al usuario cambiar la ruta de Mis Documentos, evitando que los usuarios puedan escribir una nueva ubicación de la carpeta Mis Documento.

- Ocultar el icono Mis sitios de red del escritorio, evitando la visualización completa de todos los usuarios de red en el explorador de Windows.

- Impedir la eliminación de impresoras, para prevenir que los usuarios eliminen impresoras instaladas.

4.6 SEGREGACIÓN DE FUNCIONES

- Debe existir una adecuada y documentada **separación de funciones** dentro de la Dirección Nacional de Informática.

- Deberá realizarse **rotación en las tareas del personal** del Centro de Cómputo para controlar el desempeño que los funcionarios han tenido durante un período de tiempo.

5 - SEGURIDAD DE COMUNICACIONES

5.1 ASPECTOS GENERALES

- Por Políticas Generales se prohíbe la divulgación[21], duplicación, modificación, destrucción[22], pérdida, mal uso, robo y acceso no autorizado[23] de información propietaria.

- Todos los cambios en la central telefónica, en los servidores y equipos de red de la Institución, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switches, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

[21] "La divulgación o la utilización fraudulenta de la información protegida" esta penada según contemplan las reformas al Código Penal, de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, en su articulo innumerado después del artículo 202. Ver anexo 3.

[22] Este aspecto tiene relación directa con lo determinado en el Art. 262 reformado del Código Penal; primer y segundo artículos innumerados agregados después del Art. 415 del Código Penal; y. Primer artículo innumerado agregado después del Art. 202 del Código Penal, mediante reforma contenida en los Arts. 59, 61 y 58, Título V, de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, publicada en el Registro Oficial No. 557, de 17 de abril del 2002, que tipifica la destrucción maliciosa y fraudulenta de mensajes de datos e información; los daños informáticos: y delitos contra la información protegida, respectivamente. Ver en el anexo 3.

[23] "El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida," será sancionado de acuerdo a lo que indican las reformas al Código Penal, de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, en su articulo innumerado después del artículo 202. Ver anexo 3.

- Es política de la Institución no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones será supervisado ocasionalmente en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema

- Los empleados y funcionarios de la Institución no deben interceptar las comunicaciones o divulgar su contenido, tampoco deben ayudar a otros para que lo hagan así también se hacen responsables del buen uso de sus redes de comunicación. La Institución se compromete a respetar los derechos de sus empleados, incluyendo su privacidad.

- De manera consistente con prácticas generalmente aceptadas, la Institución procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica, que contienen detalles sobre el número llamado su duración, la hora en que se efectuó, etc.

5.2 CABLEADO ESTRUCTURADO

- El cableado debe seguir las normas del **cableado estructurado**, que garantizan el funcionamiento eficiente de la red.

- Si el tendido del cableado se **terceriza**, la Institución encargada debe prestar garantías escritas sobre su trabajo.

- Mantener un **registro de red actualizado** con la ubicación de los puntos de voz y datos existentes en la red.

- Deberá medirse periódicamente el **nivel del ancho de banda** de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.

- Ante un **corte del suministro de energía eléctrica** debe apagarse los equipos del centro de cómputo de forma segura, como medida de prevención.

5.3 USO DE LOS SISTEMAS DE COMUNICACIÓN

- Se debe promover el uso responsable[24] de las comunicaciones, en particular el teléfono, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Institución y no propiedad de los usuarios de los servicios de comunicación.

- Los sistemas de comunicación[25] de la Institución generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con las productividad del funcionario ni con las actividades de la Institución.

- Se debe prohibir el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento[26] y diversión.

[24] El uso de los recursos y materiales de la Institución deben apegarse a las normas que se indican en el Reglamento General de la Administración de los Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, Literal a. Ver anexo 3.

[25] Los sistema de comunicación son otros de los recursos que deben usarse de acuerdo a las normas que se indican en el Reglamento General de la Administración de los Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, Literal a. Ver anexo 3.

[26] Los juegos y pasatiempos no están permitidos en horas laborables, lo indica el Reglamento General de la Administración de Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, literal n. Ver anexo 3.

- La navegación en Internet[27] para fines personales no debe hacerse a expensas del tiempo y los recursos de la Institución y en tal sentido deben usarse las horas no laborables.

5.4 TOPOLOGÍA DE RED

- Se debe asegurar integridad, exactitud, disponibilidad y confidencialidad de los datos transmitidos, ya sea a través de medios de comunicación de datos o dispositivos de hardware.

- Debe existir documentación detallada (registro de red) sobre los diagramas topológicos de las redes.

- Debe existir un medio alternativo de comunicación en caso de que alguna contingencia afecte al medio primario de comunicación.

5.5 CONEXIONES EXTERNAS

- Asegurar la definición e implementación de procedimientos pertinentes para el control de las actividades de usuarios externos del organismo a fin de garantizar la adecuada protección de los bienes de información de la Institución.

[27] El uso del Internet siendo un servicio que presta la institución debe usarse de acuerdo a las normas que se indican en el Reglamento General de la Administración de los Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, Literal a. Ver anexo 3.

- La conectividad a Internet se debe otorgar para propósitos relacionados con las actividades de la Institución. Los usuarios no autorizados deben ser imposibilitados de conectarse al exterior.

- Los usuarios de la Institución que utilicen Internet deben ser capacitados, respecto a su funcionalidad, a los riesgos y medidas de seguridad pertinentes y sus responsabilidades.

- Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, es filtrado y controlado por un **firewall**, prohibiendo el paso de todo el tráfico que no se encuentre expresamente autorizado.

- Para prevenir vacíos de seguridad, no está permitido el uso de módems en estaciones de trabajo que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Institución.

- Cada vez que se establezca una vía de comunicación con terceros (personal de mantenimiento externo, proveedor de servicios de Internet, etc.), los mecanismos de transmisión y las responsabilidades de las partes deberán fijarse por escrito.

- El uso de Internet debe ser monitoreado periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada o existe algún abuso[28] en particular, personal designado puede revisar el contenido de las comunicaciones de Internet.

- El acceso casual a los mensajes de correo electrónico por los administradores y similares, se considera una violación a la política de seguridad de la información. Sin embargo, la Dirección de Informática tiene el derecho de examinar cualquier información, sin previo consentimiento o notificación del funcionario, en caso que se considere que se está utilizando inadecuadamente el equipamiento del Ministerio Público.

- De ser necesario realizar **mantenimiento remoto** a los servidores, se utilizarán protocolos y servicios de comunicación que garanticen la seguridad de los datos que se transmiten a través de la red, utilizando encriptación. Deberán documentarse cada una de las actividades que el personal externo realice sobre los equipos utilizando acceso remoto.

5.6 CONFIGURACIÓN LÓGICA DE RED

- El riesgo aumenta con el número de conexiones a redes externas por lo tanto, la conectividad debe ser la mínima necesaria para cumplir con los objetivos de la Institución.

[28] Como se a indicado anteriormente los bienes y servicios de la institución deben usarse de acuerdo a las normas que se indican en el Reglamento General de la Administración de los Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, Literal a. Ver anexo 3.

- El esquema de direcciones de la red interna no debe ser visible ante las conexiones externas.

- Los recursos de los servidores serán visibles solo en los casos necesarios y con las medidas de seguridad correspondientes.

- Se tomarán las medidas necesarias para restringir todo tipo de aplicaciones que no ayudan al cumplimiento de los objetivos de la Institución.

5.7 MAIL

- Se definirá un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático.

- La Institución debe contar con un aplicativo de correo electrónico, el cual brinde las condiciones de seguridad necesarias para evitar los virus informáticos o la ejecución de código malicioso.

- Todas las cuentas de correo que pertenecen a la Institución deben estar gestionadas por una misma aplicación.

- Los mensajes[29] de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.

- Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

- El correo electrónico no debe ser utilizado para enviar cadenas de mensajes, no debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la Institución[30].

- Los datos que por su contenido se consideraron "confidenciales" o "críticos" deben encriptarse.

- Debe existir un procedimiento de priorización de mensajes, de manera que los correos electrónicos de prioridad alta sean resguardados.

- Se debe asignar una capacidad máxima de almacenamiento de 10Mb fija para cada una de las cuentas de correo electrónico de los funcionarios.

[29] Revisar los términos constantes en el GLOSARIO que tomado de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, se transcribe en el Anexo 3.
[30] Los sistema de comunicación son otros de los recursos que deben usarse de acuerdo a las normas que se indican en el Reglamento General de la Administración de los Recursos Humanos del Ministerio Público del Ecuador, Artículo 79, Literal a. Ver anexo 3.

- El tamaño máximo de un archivo adjunto en un mensaje de correo es de 4MB, no debe ser de tipo EXE, BAT, COM., esta definición se utiliza tanto para enviar como para recibir.

5.8 ANTIVIRUS

- En todos los equipos de la Institución debe existir instalada una herramienta antivirus ejecutándose permanentemente y en continua y automática actualización.
- Deberán existir discos de rescate de los antivirus, tanto para los servidores como para los puestos de trabajo, que sean capaces de restaurar los sistemas.
- La actualización del servidor antivirus se realiza de forma automática, luego a través de la red interna el servidor antivirus se encarga de actualizar todas las estaciones de trabajo de la Institución.
- Deben programarse búsquedas periódicas de virus en todos las estaciones de la Institución.
- Si en una estación de trabajo se detectare la presencia de un virus u otro agente potencialmente peligroso, se debe poner la estación de trabajo en cuarentena hasta que el problema sea resuelto.

5.9 FIREWALL

- El firewall de la Institución presenta una postura de negación preestablecida, configurado de manera que se prohíban todos los protocolos y servicios, y habilitando únicamente los que son necesarios.

- Los servicios o protocolos que sean considerados riesgosos deben habilitarse bajo estrictas limitaciones de uso.

- El encargado de mantenimiento debe controlar periódicamente la configuración del firewall y los servicios de red, documentando los resultados de dichas pruebas.

5.10 ATAQUES DE RED

- Toda la información que se considere confidencial debe encriptarse durante la transmisión, o viajar en formato no legible.

- Se deberá usar algún sistema de detección de intrusos (IDS), tolerantes al fallo, utilizando los mínimos recursos posibles.

- Se debe implementar un sistema de prevención de intrusos (IPS).

- Deberá utilizarse una herramienta que monitoree la red, con el fin de evitar el ataque de denegación de servicio (DoS).

- Para garantizar la seguridad de los puertos libres del cableado estructurado de voz, deben cambiarse los switches existentes por otros con las siguientes características:
    - Bloqueo de puertos a través de software.
    - Características de administración superiores a los del los switches actuales.
    - Control de acceso a través de la dirección de hardware (IEEE 802.2).
    - Capacidad de respaldar la configuración establecida.

5.11 SISTEMAS ANTIINTRUSOS

Sistemas de Detección de Intrusos (IDS), debe existir una herramienta para detección de intrusos que sea capaz de:

- Ejecutarse continuamente sin intervención o supervisión de un operador humano.
- Ejecutarse en background, pero debe ser flexible para que su funcionamiento interno sea examinado.
- Tolerar fallas, o superarse a una caída del sistema, sin tener que reconstruir su base de datos de conocimientos al reiniciarse.
- Automonitorearse para asegurar su correcto funcionamiento.
- Ejecutarse sin cargar al sistema de una manera tal que le impida realizar otras tareas con relativa normatividad.
- Observar desviaciones del comportamiento estándar.

Sistema de prevención de Intrusos (IPS), debe existir una herramienta para prevención de intrusos que sea capaz de:

- Reaccionar automáticamente ante incidentes.
- Requerir mínima vigilancia
- No requerir demasiada dedicación; en consecuencia requeriría menos inversión en recursos para administrar y operar estos sistemas.
- Reducir falsas alarmas.
- Integrarse con otros controles de seguridad de diferentes tipos como firewalls, antivirus, aplicaciones criptográficas, sistemas de cómputo, etc.

6 - AUDITORÍAS Y REVISIONES

6.1 CHEQUEOS DEL SISTEMA

- Se deben registrar, mediante logs de auditoría, aquellos eventos relacionados con la seguridad de la información. Dichos registros deberán contener como mínimo:
    - Fecha y hora del evento,
    - Fuente (el componente que disparó el evento),
    - ID del evento (número único que identifica el evento),
    - Equipo (máquina donde se generó el evento),
    - Usuario involucrado,
    - Descripción (acción efectuada y datos asociados con el evento).

- Se deben registrar como mínimo los siguientes eventos respecto a los servidores:
    - Los servicios de mail,
    - Servicios de red,
    - Configuración de los servidores,
    - Reinicio de servidores.

- Deben actualizarse continuamente las herramientas de análisis de logs, asignándole la responsabilidad de esta tarea a una persona en particular.

- Deberá existir un proceso encargado de la rotación y eliminación de logs. Se deberá conservar esta información al menos durante tres meses.

- Deben programarse auditorías periódicas y chequeos aleatorios, para controlar las áreas o funciones críticas con respecto a la seguridad de los datos de la Institución, documentando la ejecución y los resultados de dichas pruebas.

- Se deberán analizar periódicamente los siguientes eventos específicos como mínimo:
    - Controles de acceso y permisos de los usuarios,
    - Uso de recursos informáticos,
    - Operaciones de borrado o modificación de objetos críticos,
    - Intentos de ingreso al sistema fallidos.

- Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

6.2 RESPONSABILIDADES DE LOS ENCARGADOS DE SEGURIDAD

- El encargado de auditorías, debe:
    - Determinar qué logs se generarán,
    - Determinar qué eventos de seguridad se auditarán,
    - Determinar qué datos se recogerán de estas auditorías,

- Administrar, desarrollar e implementar los procedimientos de auditoría y revisión,
- Monitorizar y reaccionar a los avisos (warnings) y reportes,
- Chequear aleatoriamente para verificar el cumplimiento de los requerimientos y procedimientos de seguridad,
- Revisar los reportes de auditorías cuando es advertido de anomalías.

6.3 AUDITORÍAS DE REDES

- Debe generarse un archivo de log cuando se produzca el bloqueo de un usuario.

- Debe generarse un plan de monitorización de red utilizando alguna herramienta destinada para ello.

- Con respecto a las conexiones a Internet deben almacenarse datos sobre:
  - Número IP de la máquina conectada,
  - Dirección de las páginas visitadas,
  - Cookies guardadas,
  - Archivos descargados,
  - Servicios utilizados,
  - Aplicaciones utilizadas.

- Con respecto a la utilización del correo electrónico deben almacenarse datos sobre:
  - Correo entrante y saliente,
  - Hora de envío,

- Contenido del mail,
- Asunto del mail,
- Archivos adjuntos,
- Reporte de virus del mail,
- Direcciones de máquina destino y fuente,
- Tamaño del mensaje.

- Con respecto a la utilización de la red informática deben almacenarse datos sobre:
  - Ancho de banda utilizado y cuellos de botella en el tráfico de red,
  - Tráfico generado por las aplicaciones,
  - Recursos de los servidores que utilizan las aplicaciones,
  - Intentos de intrusión,
  - Uso de los protocolos.

- Considerar para el futuro la contratación de servicios de análisis forense por empresas externas que brinden este tipo de soporte y tengan la capacidad de:
  - Determinar el grado de afectación del sistema.
  - Localizar cuando sea posible desde donde se realizó el ataque.
  - Determinar los procedimientos empleados en el ataque.

- Si la contratación de empresas que brindan servicios de análisis forense no es posible debe designarse y capacitarse a un funcionario para que se especialice en temas de seguridad pudiendo manejar las herramientas que se utilizan en técnicas de análisis forense tales como:
  - Respaldo de información y recuperación de evidencias de discos duros.
  - Detección de virus Troyanos y Spyware.
  - Análisis de servicios en la red y saber como se registran sus actividades.
  - Configuraciones de seguridad propias del sistema operativo.

7- PLAN DE CONTINGENCIAS

7.1 PLAN DE ADMINISTRACIÓN DE INCIDENTES

- Se deberá asegurar la continuidad de la recolección de datos y su procesamiento ante cualquier contingencia que afecte a los centros de procesamiento. Para ello se deberá:
    - Generar procedimientos manuales de respaldo para cada una de las actividades desarrolladas en la Institución,
    - Preparar, probar y mantener actualizado un plan de contingencias, coordinando el mismo con los procedimientos de copias de respaldo y almacenamiento externo. Dicho plan deberá ser desarrollado de forma tal que cubra las distintas áreas de riesgo, o definir y asignar claramente las responsabilidades de las tareas detalladas en el plan,
    - Prever un programa de entrenamiento para el personal involucrado en el plan de contingencias.

- Deberá almacenarse una copia del **plan de contingencias** en el exterior de la Institución o en un medio seguro como en una caja fuerte, protegiéndola contra su divulgación y actualizándola permanentemente.

7.2 RESPALDO DE EQUIPAMIENTO

- El equipamiento informático de la Institución debe contar con dispositivos de respaldo, ante cualquier tipo de incidente.

- Los mecanismos de recuperación de los dispositivos de respaldo deben ser probados periódicamente comprobando su buen funcionamiento.

- El sistema informático no deberá verse afectado ante una contingencia en el centro de cómputo, por lo que el equipamiento informático debe distribuirse en lugares físicos diferentes, contando ambos con las medidas y condiciones de calidad y seguridad especificadas en esta política.

7.3 ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES

- Debe conformarse un grupo de recuperación encargado de concebir, probar e implementar el plan de contingencias. Este tentativamente debe estar a cargo el Jefe de Desarrollo de Sistemas , e integrado por los líderes de cada área de la Institución.

- Debe asignarse un orden de importancia a los sistemas de información y a los equipos de la red informática, de acuerdo al análisis de riesgo y al impacto que representaría para la Institución su ausencia.

- Los equipos deberán estar señalizados o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

- Deberán definirse las funciones o servicios críticos de la Institución, junto con los recursos mínimos necesarios para su funcionamiento, asignándoles una prioridad en el plan de contingencia.

- Deberá conformarse un plan de emergencias, determinando los procedimientos a llevar a cabo para cada contingencia identificada, considerando los distintos escenarios posibles. Cada procedimiento deberá estar claramente definido, y tener asignado un responsable para su ejecución.

- Para el desarrollo del plan de contingencias deben contemplarse las siguientes pautas:
    - Deberá estar documentado y probado antes de su puesta en práctica.
    - Deberá basarse en un análisis de riesgo, determinando que acciones merecen estar incluidas.
    - Deberá mantenerse actualizado de acuerdo a nuevos puestos de trabajos y funciones.
    - Deberá ser probado frecuentemente.

- Debe definirse hasta cuánto tiempo se aceptará estar en condición de emergencia.

- Debe documentarse la realización de las siguientes actividades después de un incidente:
    - Determinar la causa del daño,
    - Evaluar la magnitud del daño que se ha producido,

- Que sistemas se han afectado,
- Qué modificaciones de emergencia se han realizado,
- Que equipos han quedado no operativos,
- Cuales se pueden recuperar y en cuanto tiempo.

- Cada una estas actividades deberán ser reportadas al Coordinador General.

- Deberá retroalimentarse el plan luego de una contingencia, ajustando las directivas en consecuencia.

- Deben establecerse planes de prueba periódicos que incluyan simulacros de siniestros para evaluar la eficacia y eficiencia del plan.

CAPITULO IV

PLAN DE CONTINGENCIAS

INTRODUCCIÓN

El Plan de Contingencia de Informática es parte del Plan general de Contingencias del Ministerio Público.

Es función primordial del Plan de Contingencias informático garantizar la continuidad de las funciones primordiales de la Institución durante el período de recuperación de desastres.

La organización y establecimiento de grupos de trabajo y funciones que deben ser desarrolladas ante la presencia de una emergencia, son parte importante y deben ser descritas en el desarrollo del Plan de Contingencias.

OBTETIVOS

El objetivo principal del plan es establecer lineamiento generales para determinar las acciones de combate de emergencias con el objeto de minimizar sus efectos y consecuencias y salvaguardar:

- La integridad física o la vida de los funcionarios o de terceros presentes en las instalaciones del Ministerio Público.
- La integridad física de los bienes de la Institución.

1- PLAN DE EMERGENCIAS

1.1 ORGANIZACIÓN GENERAL ANTE EMERGENCIAS

Todo el personal de la Dirección Nacional de Informática forma parte de la organización ante contingencias. Esta organización debe mantener coordinación con las entidades o instituciones de apoyo externo como son la Policía Nacional, cuerpo de Bomberos y otras Instituciones

Pueden presentarse situaciones de emergencia en dos escenarios:

- **Durante el horario normal de trabajo**, en el cual se dispone de todo el personal para construir y activar la organización del plan de contingencias.

- **Fuera del horario normal de trabajo**, durante el cual la detección y comunicación de la contingencia y eventualmente la toma de acciones iniciales estará a cargo de los Policías Nacionales de turno, hasta que el responsable y coordinadores puedan llegar al sitio de la emergencia.

1.2 ORGANIZACIÓN DEL SISTEMA DE CONTROL DE EMERGENCIAS

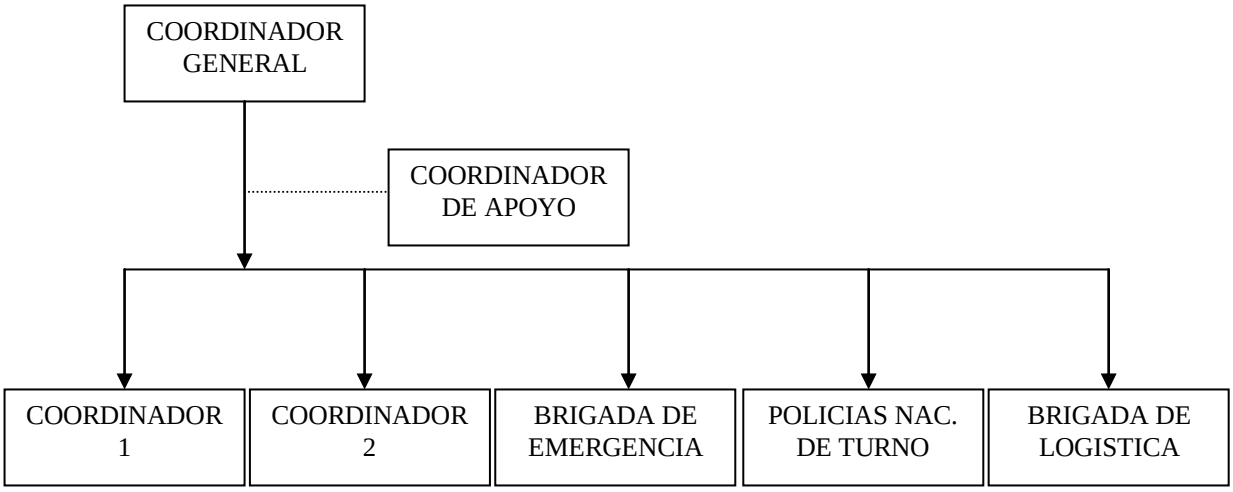


Figura 4.1: (Organización del sistema control de emergencias)

2- PLAN DE RECUPERACIÓN

El plan de recuperación es la capacidad de responder y recuperar la información de los sistemas críticos que posee la Institución. El equipo y las funciones del equipo de recuperación se detallan a continuación.

2.1 CENTROS DE CÓMPUTO ALTERNATIVOS

Si una emergencia se presenta en el edifico Tocuyo, el centro de cómputo alternativo será el del edifico Roca y viceversa.

El centro de cómputo alternativo iniciará sus nuevas funciones, sólo si la emergencia lo amerita, como por ejemplo la pérdida de equipamiento de comunicaciones, pérdida de servidores, o cualquier falla que imposibilite un funcionamiento confiable para los sistemas y un ambiente seguro de trabajo para los funcionarios.

2.2 FUNCIONES DE LOS MIEMBROS DE LA ORGANIZACIÓN PARA LAS CONTINGENCIAS

Las responsabilidades de cada miembro del grupo de contingencias se detalla a continuación.

2.2.1 Coordinador General (Encargado del plan de contingencias)

Es el encargado de:

- Llevar a cabo la declaratoria de emergencia.
- Comunicarse con las máximas autoridades de la Institución para poner en conocimiento la emergencia.
- Coordinar con las Instituciones externas de apoyo (Policía, Bomberos).
- Dirigir a los coordinadores especializados en cada área.
- Poner en funcionamiento los sistemas críticos, junto con todos los coordinadores.

2.2.2 Coordinador 1 (Custodio de los respaldos)

Su responsabilidad es transportar al centro de cómputo alternativo, los respaldos en forma segura y oportuna, inmediatamente después de haberse declarado la emergencia. Una vez trasladados los respaldos debe poner en acción el **plan de respaldos.**

2.2.3 Coordinador 2 (Responsable de la administración de los sistemas)

Su responsabilidad es transportar al centro de cómputo alternativo, toda la documentación pertinente a la administración de los sistemas críticos, si fuera necesario deberá comunicarse con los proveedores de los sistemas adquiridos para recibir el soporte necesario.

2.2.4 Coordinador de apoyo (Usuario final de cada sistema crítico)

Son cada uno de los usuarios finales que conoce a cabalidad el funcionamiento de los sistemas críticos. Sus funciones son probar cada uno de los sistemas críticos una vez que han sido instalados en el centro de cómputo alternativo.

2.2.5 Responsabilidades de los Policías Nacionales de turno

- Control de puertas de acceso al ingreso del edificio.

- Se encargará de comunicar de inmediato con el mayor detalle la emergencia al Coordinador General de contingencias.

2.3 ACCIONES A TOMAR EN EL CENTRO DE CÓMPUTO ALTERNATIVO

Una vez determinada una emergencia, los siguientes coordinadores deben trasladarse al centro de cómputo alternativo.

- El Coordinador General.
- El responsable de la administración de los sistemas (Coordinador 1).
- El custodio de los respaldos (Coordinador 2).

Una vez que los sistemas estén en funcionamiento, los coordinadores de apoyo deben trasladarse al centro de cómputo alternativo para verificar el correcto funcionamiento de los sistemas críticos.

2.4 PLAN DE RESPALDOS

El plan de respaldos comprende:

- Instalación de los sistemas críticos de la Institución en el servidor del centro de cómputo alternativo.
- Restauración de las bases de datos de los sistemas críticos de la Institución.
- Otorgar permisos a las cuentas de usuario dependiendo de sus requerimientos.
- Prueba y puesta en funcionamiento de los sistemas críticos.

2.5 ACCIONES A TOMAR EN EL CENTRO DE CÓMPUTO DE LA EMERGENCIA

2.5.1 Brigada de emergencia

Durante la emergencia sus función son:

- Seguir las órdenes del coordinador General.
- Revisar y asegurar la zona afectada para impedir mayores daños.
- Interrumpir el fluido eléctrico.
- Control de incendio.
- El salvamento de los bienes informáticos para reducir pérdidas.

2.5.2 Brigada de logística

Durante la emergencia sus funciones son:

- Ponerse a disposición del Coordinador General.
- Provee los recursos necesarios de transportación, materiales, equipos, etc. necesarios para el control y mitigación de la emergencia.
- Es la encargada de contabilidad de los recursos, manejo de seguros y contratos.

2.5.3 Responsabilidades de los Policías Nacionales de turno

- Control de puertas de acceso al ingreso del edificio.
- Custodia de las oficinas afectadas.

2.6 SISTEMAS CRITICOS

Los sistemas considerados críticos para su puesta en funcionamiento en una emergencia son:

- El sistema que lleva el control de denuncias del Ministerio Público
- El sistema de contabilidad y presupuesto.

Dependiendo del tipo de emergencia los siguientes sistemas deben ser considerados

- El sistema de remuneraciones.
- El sistema de control de asistencia.
- El sistema de control de bienes.
- El sistema de recaudaciones.
- El sistema legal.

2.7 FUNCIONARIOS RESPONSABLES DEL PLAN DE CONTINGENCIAS

Cuadro 4.1: (Funcionarios responsables del Plan de Contingencias)

CARGO DE RESPONSABILIDAD	NOMBRE DEL FUNCIONARIO	TELEFONO	DIRECCIÓN
Coordinador General			
Coordinador 1			
Coordinador 2			
Coordinador de apoyo			
Brigada de emergencia			
Brigada de logística			

2.8 DIRECTORIO PARA LLAMADAS DE EMERGENCIA (Autoridades del Ministerio Público)

Cuadro 4.2: (Directorio interno, para llamadas de emergencia)

NOMBRE	CARGO	TELEFONO	DIRECCIÓN
Ing. Sergio Ruiz	Director Nac. de Informática		

2.9 DIRECTORIO PARA LLAMADAS DE EMERGENCIA (Notificación Externa)

Cuadro 4.3: (Directorio externo, para llamadas de emergencia)

ENTIDAD	TELEFONO
Compañía de bomberos	

3- SIMULACIÓN DEL PLAN DE CONTINGENCIAS

La finalidad del Plan de Contingencias es detectar posibles estrategias de recuperación ante un estado de emergencia informático. Es por ello que debe ponerse a prueba y realizar simulacros periódicamente.

4- MANTENIMIENTO DEL PLAN DE CONTINGENCIAS

Con el propósito de mantener vigente el Plan de Contingencias se deben tomar la siguientes decisiones y realizar las siguientes actividades.

- Designar un responsable de actualizar el Plan de Contingencias.

  Nombre:

  Cargo:

- Lugar donde se encuentran distribuidas las copias de respaldo del Plan de Contingencias.

  Entidad:

  Edificio:

  Lugar Físico:

  Dirección:

- Fecha de última modificación del Plan de Contingencias.
- Fecha de última simulación del Plan de Contingencias.
- Resultados de la última simulación realizada al Plan de Contingencias.
- Cual es la última emergencia que se presentó.
- Acciones tomadas para la retroalimentación del Plan de Contingencias después de la última emergencia.

CONCLUSIONES

- A lo largo del proyecto se pudo comprender que la seguridad es un conjunto de recursos destinados a lograr un ambiente de seguridad y responsabilidad, capaz de mantener disponibles recursos, servicios e información con toda la integridad que es necesaria y requerida por todos los usuarios de la Institución. Por lo tanto es sumamente importante disponer de políticas de seguridad que sean masivamente divulgadas para que sean conocidas por funcionarios e instituciones que colaboran con el Ministerio, y adquieran el compromiso de aplicarlas y llevarlas a cabo durante sus actividades cotidianas, generando una **"cultura de seguridad institucional",** definida en los objetivos propuestos.

- No existe un esquema de seguridad informática que cubra en su totalidad todos los posibles riesgos.

- Todo el personal del Ministerio Público, debe ser instruido en el conocimiento de las normas jurídicas relativas a Propiedad Intelectual, seguridad de la información, documento electrónico, mensajes de datos e infracciones electrónicas para impulsar el correcto uso de la tecnología informática y los datos.

- Existe mucha dificultad en la asignación de recursos económicos .

- Se debe elaborar una normativa reglamentaria para regular el uso de la tecnología informática en lo relativo a hardware y software y especialmente a la información institucional.

RECOMENDACIONES

Con el panorama de la situación actual del sistema y el análisis de riesgos de los activos de la Institución desarrollado en el Capítulo II, se desprenden las siguientes observaciones para mejorar el control de la seguridad en los activos de la Institución.

- El plan de seguridad informática debe ser renovado o reajustado con cada cambio importante ya sea de personal, de funciones que se han modificado al personal, cambios en la estructura física, cambio de hardware, etcétera.

- El plan de seguridad debe tener fecha de validez y un período específico de aplicación, por ende deber ser renovado cuando ese plazo se cumpla.

- Se debe estar preparado y dispuesto a reaccionar con rapidez ante cualquier contingente ya que las amenazas y los riesgos cambian con el paso del tiempo.

- La Dirección Nacional de Informática, y el centro de cómputo comparten la misma área, es imprescindible, mejorar las protecciones de acceso físico para salvaguardar el equipamiento y documentación en ella depositados.

- Es sumamente importante suscribir un contrato de soporte y mantenimiento para los servidores y equipos de comunicación con la finalidad de asegurar el perfecto funcionamiento y garantizar la prestación de servicios en la red.

- Adquirir un sistema contra incendios para el centro de cómputo y la implementación de equipos contra incendios que se instalen estratégicamente en distintos sectores de los edificios.

- Definir adecuadamente los roles y funciones de quienes conforman la Dirección Nacional de Informática.

- Estructurar un calendario de mantenimiento de los dispositivos de soporte, tanto del centro de cómputo como de las estaciones de trabajo y de todo el equipamiento informático.

- Mejorar el control de acceso a los puntos de la red de datos que se encuentran sin uso y sin ninguna protección, a través de herramientas de software propietario de los fabricantes de los switches o control físico de los puertos.

- Estructurar un procedimiento para mantener actualizado el software de las estaciones de trabajo, para facilitar el control y la administración a quienes realicen estas tareas.

- Diseñar procedimientos para de auditoría de los logs generados por el sistema operativo y dispositivos de seguridad, puede ser a través de herramientas de software.

- Se recomienda y sería conveniente que la Dirección de Recursos Humanos ponga en conocimiento de la Dirección de Informática, las personas que van a cesar en

sus funciones, de esta manera se puede llevar a cabo una política de desvinculación de personal.

- Poner protecciones de seguridad en los tableros de control del flujo eléctrico para impedir el acceso a personas no autorizadas .

- Instruir al personal de limpieza sobre el uso adecuado de las instalaciones eléctricas, así también se recomienda poner tomas diferenciadas para identificar plenamente los circuitos eléctricos.

- Es necesaria la adquisición de dispositivos físicos y herramientas de software que permitan la obtención de respaldos de la configuración de los servidores, sistemas instalados, bases de datos e información de los usuarios, para evitar su pérdida o destrucción.

- Difundir todas las políticas de seguridad establecidas, buscando que los funcionarios asuman su responsabilidad y tomen como suyos los objetivos de seguridad de la Institución.

- Proceder a un plan de capacitación en el cual se debe impartir conocimientos sobre las normas jurídicas asociadas con Propiedad Intelectual, seguridad de la información, documento electrónico, mensajes de datos e infracciones electrónicas. Así también se deberá mejorar la divulgación de las políticas de seguridad elaboradas.

- Desarrollar simulacros para poner en práctica el plan de contingencias, los mismos que ayudarán a identificar las debilidades y servirán para mejorarlo y retroalimentarlo obteniendo así cada vez un plan más completo y adaptado a las necesidades institucionales.

- Elaborar un reglamento de responsabilidades en el uso de equipamiento informático en el que intervengan la Dirección Nacional de Asesoría Jurídica y la Dirección Nacional de Informática.

- Realizar seguimiento comprometido a todos los trámites burocráticos para conseguir el equipamiento previsto, con la finalidad de mitigar o eliminar las amenazas encontradas en el sistema.

Como trabajos futuros se recomienda:

- La elaboración del Reglamento Interno de la Dirección Nacional de Informática del Ministerio Público del Ecuador, en el cual se debe definir las funciones de los cargos y las personas responsables de:
    - Mantenimiento de los equipos,
    - Administración de los sistemas,
    - Inventario de hardware y software,
    - La obtención, restauración y custodia de los respaldos,
    - La gestión de la documentación del centro de cómputo.
    - Plan de emergencias, etc.

- La elaboración de manuales de procedimientos de las actividades que se realizan en la Dirección Nacional de Informática.

- La implementación del plan de seguridad y el plan de contingencias para el Ministerio Público del Ecuador, es el paso final a dar, para ello es imprescindible, que el director Nacional de Informática estudie y apruebe los planes y los ponga en conocimiento de la máxima autoridad de la Institución, y ella con la autoridad que la enviste será la única quien disponga se apliquen las políticas y normas establecidas.

En la parte académica se recomienda:

- Implementar en la Facultad de Ingeniería de Sistemas e Informática de la Escuela Politécnica del Ejército, una asignatura que abarque los temas de seguridad en redes informáticas.

POLITICAS IMPLEMENTADAS

A pesar de que el proyecto no contempla la implementación de las políticas en la Institución, varias de la políticas recomendadas ya están puestas en práctica y en funcionamiento:

- Está ya en el proceso de adquisición el Sistema de Control de Accesos par el Centro de Cómputo del Edificio Tocuyo.
- Ya se adquirió y se encuentra instalado y en funcionamiento en el Centro de Cómputo del Edificio Tocuyo un sistema contra incendios a base de gas.
- Se implementaron políticas a nivel de dominio a través de Windows Server 2003 .
- Se implementaron políticas a nivel de unidades organizacionales a través de la Windows Server 2003.

BIBLIOGRAFIA

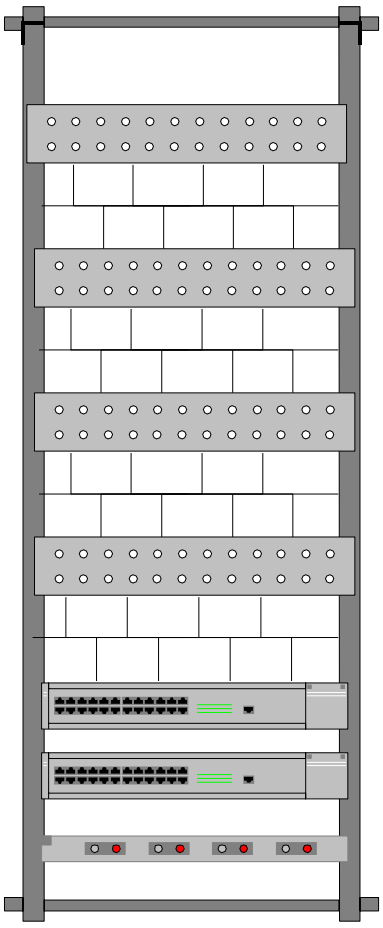
1. ISO (International Standard Organization). "**Estándar de Seguridad ISO 17799**".
2. NIST (National Institute of Standards and Technology - U.S. Department of Commerce). "An Introduction to Computer Security: The NIST Handbook" Special Publication 800-12.
3. COBIT Planificación y Gestión de Sistemas de Información
4. Elaboración de Políticas de Seguridad. http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_1128.html.
5. Elaboración de Políticas de Seguridad. www.information-security-policies-and-standards.com/infopolicies.htm
6. PLAN DE CONTINGENCIAS http://sistemas.dgsca.unam.mx/publica/pdf/Contingencias1.PDF
7. PLANIFICACIÓN DE DESASTRES http://www.infogroup.es/soluciones/docview.aspx?id=24
8. PLAN DE CONTINGENCIAS http://www.segu-info.com.ar/politicas/Cobit.pdf
9. AUDITORÍA INFORMÁTICA www.lafacu.com/apuntes/informatica/Auditoria_de_Base_de_datos/default.htm
10. Código penal. Capítulo Ley De Comercio Electrónico, Firmas Y Mensajes De Datos.
11. Ley de Propiedad Intelectual.
12. Reglamento General de la Administración de Recursos Humanos del Ministerio Público.

ANEXO 1

Diagrama del gabinete 1, de voz y datos, ubicado en el octavo piso del edificio Tocuyo

GABINETE 1

(OCTAVO PISO)

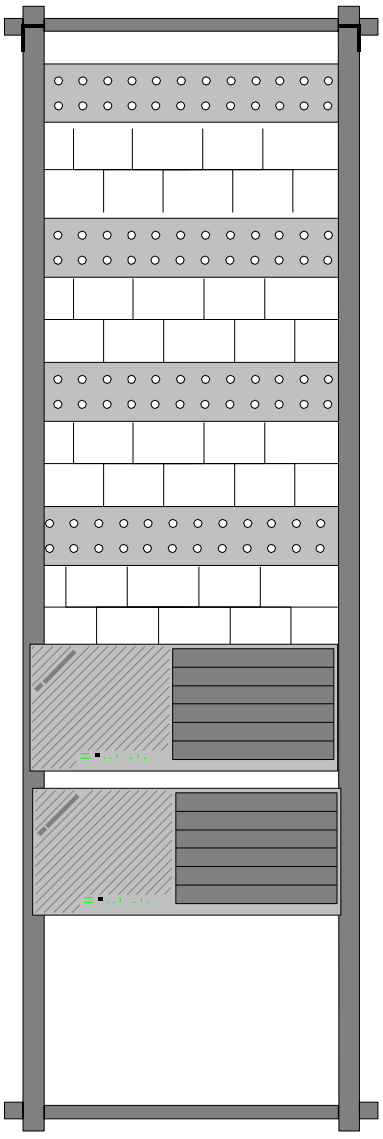


Rack 1 (abierto) de voz, ubicado en el quinto piso del edificio tocuyo.

RACK 1

(SEXTO PISO)

VOZ



A **PANEL 48 PUERTOS (HORIZONTAL DE VOZ)**

ORGANIZADOR HORIZONTAL

B **PANEL48 PUERTOS (HORIZONTAL DE VOZ)**

ORGANIZADOR HORIZONTAL

C **PANEL 48 PUERTOS (BACKBONE DE VOZ)**

ORGANIZADOR HORIZONTAL

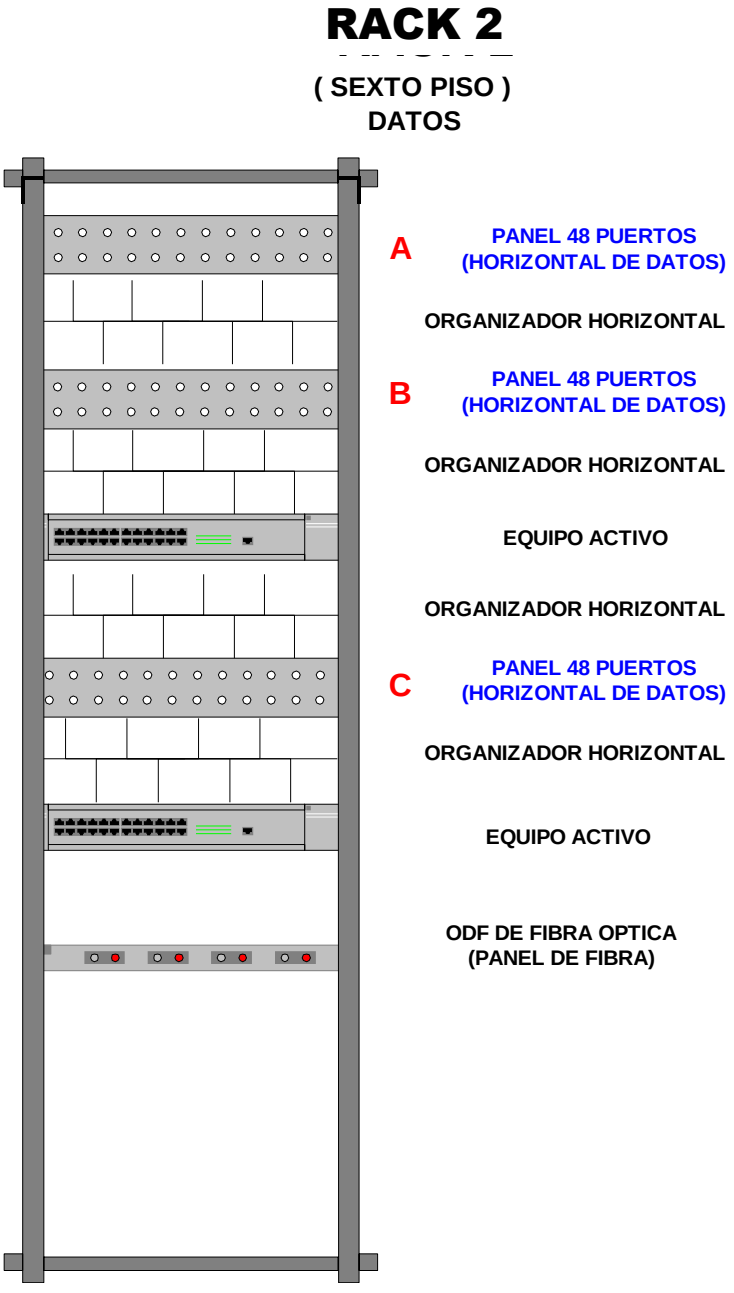
D **PANEL 48 PUERTOS (BACKBONE DE VOZ)**

ORGANIZADOR HORIZONTAL

REGLETAS 110 REFLEJO DE TODOS LOS RACK

REGLETAS 110 REFLEJO DE CENTRAL TELEFONICA

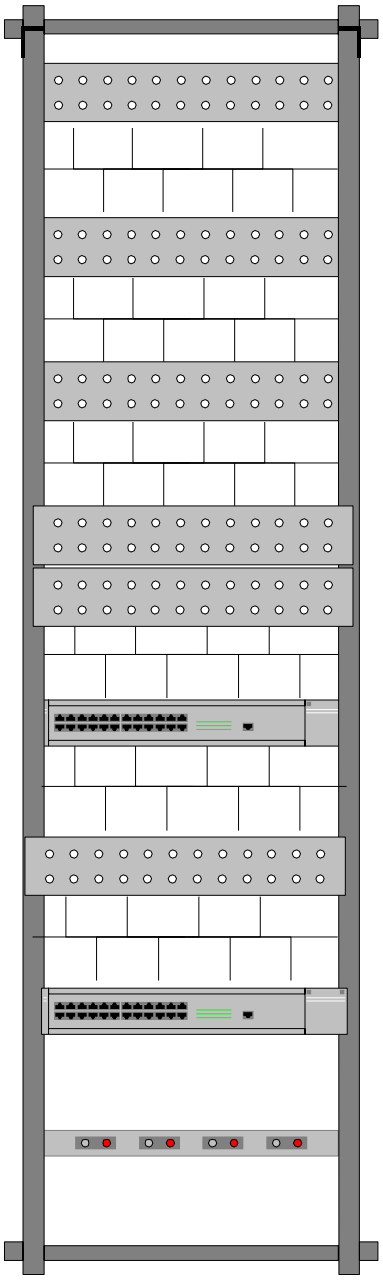
Rack 2 (abierto) de datos, ubicado en el quinto piso del edificio tocuyo.



Gabinete 2 de voz y datos, ubicado en el segundo piso del edificio tocuyo.

GABINETE 2

(SEGUNDO PISO)



A PANEL 48 PUERTOS (BACKBONE DE VOZ)

ORGANIZADOR HORIZONTAL

B PANEL 48 PUERTOS (BACKBONE DE VOZ)

ORGANIZADOR HORIZONTAL

C PANEL 48 PUERTOS HORIZONTAL VOZ)

ORGANIZADOR HORIZONTAL

D PANEL 24 PUERTOS HORIZONTAL VOZ)

E PANEL 24 PUERTOS HORIZONTAL DATOS

ORGANIZADOR HORIZONTAL

EQUIPO ACTIVO

ORGANIZADOR HORIZONTAL

F PANEL 48 PUERTOS HORIZONTAL DATOS

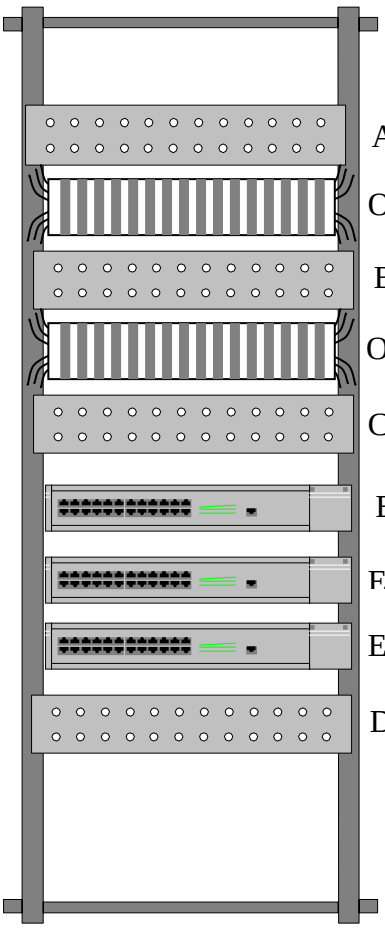
ORGANIZADOR HORIZONTAL

EQUIPO ACTIVO

ODF DE FIBRA OPTICA (PANEL DE FIBRA)

ANEXO 2

Diagrama de rack abierto de voz y datos del edificio Tocuyo.



A - PANEL DE 48 PUERTOS (BACKBONE DE VOZ)

ORGANIZADOR HORIZONTAL

B - PANEL DE 48 PUERTOS (BACKBONE DE VOZ)

ORGANIZADOR HORIZONTAL

C - PANEL 48 PUERTOS (HORIZONTAL DE VOZ)

EQUIPO ACTIVO HUB 24 PUERTOS

EQUIPO ACTIVO HUB 24 PUERTOS

EQUIPO ACTIVO HUB 16 PUERTOS

D - PANEL 12 PUERTOS (HORIZONTAL DE VOZ)

ANEXO 3

CÓDIGO PENAL

* (1) Ley 67, Registro Oficial Suplemento 557, 17/ABR/2002

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS

Reformas al Código Penal

Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:

"Art. ..- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor

ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. ..- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

* (1) Codificación s/n, Registro Oficial Suplemento 147, 22/ENE/1971

CODIGO PENAL

Art. ...- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Nota: Artículo agregado por Ley No. 67, publicada en Registro Oficial Suplemento 557 de 17 de Abril del 2002.

* (1) Ley 67, Registro Oficial Suplemento 557, 17/ABR/2002

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS

Art. 59.- Sustitúyase el artículo 262 por el siguiente:

"Art. ...- 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo".

* (1) Ley 67, Registro Oficial Suplemento 557, 17/ABR/2002

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS

Art. 62.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados:

"Art. ...- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. ...- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptadas;

3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,

5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

* (1) Ley 67, Registro Oficial Suplemento 557, 17/ABR/2002

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS

Art. 60.- A continuación del artículo 353, agréguese el siguiente artículo innumerado:

"Art. ...- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.".

* (1) Ley 67, Registro Oficial Suplemento 557, 17/ABR/2002

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS

Novena.- Glosario de términos.- Para efectos de esta ley, los siguientes términos serán entendidos conforme se definen en este artículo:

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

Red electrónica de información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Servicio electrónico: Es toda actividad realizada a través de redes electrónicas de información.

Comercio electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley.

Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Certificado electrónico de información: Es el mensaje de datos que contiene información de cualquier tipo.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Dispositivo de emisión: Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.

Emisor: Persona que origina un mensaje de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Quiebra técnica: Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta ley y su reglamento.

Factura electrónica: Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

SECCION V

DISPOSICIONES ESPECIALES SOBRE CIERTAS OBRAS

PARAGRAFO PRIMERO

DE LOS PROGRAMAS DE ORDENADOR

Art. 28.- Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

Art. 29.- Es titular de un programa de ordenador, el productor, esto es la persona natural o jurídica que toma la iniciativa y responsabilidad de la realización de la obra. Se considerará titular, salvo prueba en contrario, a la persona cuyo nombre conste en la obra o sus copias de la forma usual.

Dicho titular está además legitimado para ejercer en nombre propio los derechos morales sobre la obra, incluyendo la facultad para decidir sobre su divulgación.

El productor tendrá el derecho exclusivo de realizar, autorizar o prohibir la realización de modificaciones o versiones sucesivas del programa, y de programas derivados del mismo.

Las disposiciones del presente artículo podrán ser modificadas mediante acuerdo entre los autores y el productor.

Art. 30.- La adquisición de un ejemplar de un programa de ordenador que haya circulado lícitamente, autoriza a su propietario a realizar exclusivamente:

a) Una copia de la versión del programa legible por máquina (código objeto) con fines de seguridad o resguardo;

b) Fijar el programa en la memoria interna del aparato, ya sea que dicha fijación desaparezca o no al apagarlo, con el único fin y en la medida necesaria para utilizar el programa; y,

c) Salvo prohibición expresa, adaptar el programa para su exclusivo uso personal, siempre que se limite al uso normal previsto en la licencia. El adquirente no podrá transferir a ningún título el soporte que contenga el programa así adaptado, ni podrá utilizarlo de ninguna otra forma sin autorización expresa, según las reglas generales.

Se requerirá de autorización del titular de los derechos para cualquier otra utilización, inclusive la reproducción para fines de uso personal o el aprovechamiento del programa por varias personas, a través de redes u otros sistemas análogos, conocidos o por conocerse.

LIBRO IV

DE LA COMPETENCIA DESLEAL

Art. 284.- Se considera competencia desleal a todo hecho, acto o práctica contrario a los usos o costumbres honestos en el desarrollo de actividades económicas.

La expresión actividades económicas, se entenderá en sentido amplio, que abarque incluso actividades de profesionales tales como abogados, médicos, ingenieros y otros campos en el ejercicio de cualquier profesión, arte u oficio.

Para la definición de usos honestos se estará a los criterios del comercio nacional; no obstante cuando se trate de actos o prácticas realizados en el contexto de operaciones internacionales, o que tengan puntos de conexión con más de un país, se atenderá a los criterios que sobre usos honestos prevalezcan en el comercio internacional.

Art. 285.- Se consideran actos de competencia desleal, entre otros, aquellos capaces de crear confusión, independiente del medio utilizado, respecto del establecimiento, de los productos, los servicios o la actividad comercial o industrial de un competidor; las aseveraciones falsas en el ejercicio del comercio capaces de desacreditar el establecimiento, los productos o los servicios, o la actividad comercial o industrial de un competidor, así como cualquier otro acto susceptible de dañar o diluir el activo intangible o la reputación de la empresa; las indicaciones o aseveraciones cuyo empleo en el ejercicio del comercio pudieren inducir al público a error sobre la naturaleza, el modo de

fabricación, las características, la aptitud en el empleo o la calidad de los productos o la prestación de los servicios; o la divulgación, adquisición o uso de información secreta sin el consentimiento de quien las controle.

Estos actos pueden referirse, entre otros, a marcas, sean o no registradas; nombres comerciales, identificadores comerciales; apariencias de productos o establecimientos; presentaciones de productos o servicios; celebridades o personajes ficticios notoriamente conocidos; procesos de fabricación de productos; conveniencias de productos o servicios para fines específicos; calidades, cantidades u otras características de productos o servicios; origen geográfico de productos o servicios; condiciones en que se ofrezcan o se suministren productos o servicios; publicidad que imite, irrespete o denigre al competidor o sus productos o servicios y la publicidad comparativa no comprobable; y, boicot.

Se entenderá por dilución del activo intangible el desvanecimiento del carácter distintivo o del valor publicitario de una marca, de un nombre u otro identificador comercial, de la apariencia de un producto o de la presentación de productos o servicios, o de una celebridad o un personaje ficticio notoriamente conocido.

Art. 286.- Se considera también acto de competencia desleal, independientemente de las acciones que procedan por violación de información no divulgada, todo acto o práctica que tenga lugar en el ejercicio de actividades económicas que consista o tenga por resultado:

a) El uso comercial desleal de datos de pruebas no divulgadas u otros datos secretos cuya elaboración suponga un esfuerzo considerable y que hayan sido presentados a la autoridad competente a los efectos de obtener la aprobación de la comercialización de productos farmacéuticos o de productos químicos, agrícolas o industriales;

b) La divulgación de dichos datos, excepto cuando sea necesario para proteger al público y se adopten medidas para garantizar la protección de los datos contra todo uso comercial desleal; y,

c) La extracción no autorizada de datos cuya elaboración suponga un esfuerzo considerable para su uso comercial en forma desleal.

Art. 287.- Sin perjuicio de otras acciones legales que sean aplicables, toda persona natural o jurídica perjudicada podrá ejercer las acciones previstas en esta Ley, inclusive las medidas preventivas o cautelares.

Las medidas a que se refiere el inciso anterior podrán ser solicitadas también por asociaciones gremiales o de profesionales que tengan legítimo interés en proteger a sus miembros contra los actos de competencia desleal.

TITULO I

DE LA PROTECCION Y OBSERVANCIA DE LOS DERECHOS

DE PROPIEDAD INTELECTUAL

CAPITULO I

PRINCIPIOS GENERALES

Art. 288.- La violación de cualquiera de los derechos sobre la propiedad intelectual establecidos en esta Ley, dará lugar al ejercicio de acciones civiles y administrativas; sin perjuicio de las acciones penales a que hubiere lugar, si el hecho estuviese tipificado como delito.

La tutela administrativa de los derechos de propiedad intelectual se regirá por lo previsto en el Libro V de la presente Ley.

Art. 289.- En caso de infracción de los derechos reconocidos en esta Ley, se podrá demandar:

a) La cesación de los actos violatorios;

b) El comiso definitivo de los productos u otros objetos resultantes de la infracción, el retiro definitivo de los canales comerciales de las mercancías que constituyan infracción, así como su destrucción;

c) El comiso definitivo de los aparatos y medios empleados para el cometimiento de la infracción;

d) El comiso definitivo de los aparatos y medios para almacenar las copias;

e) La indemnización de daños y perjuicios;

f) La reparación en cualquier otra forma, de los efectos generados por la violación del derecho; y,

g) El valor total de las costas procesales.

Podrán exigirse también los derechos establecidos en los convenios internacionales vigentes en el Ecuador, especialmente los determinados en el Acuerdo sobre los Aspectos de Propiedad Intelectual relacionados con el Comercio (ADPIC) de la Organización Mundial del Comercio.

Art. 290.- Para que el titular de los derechos de autor y derechos conexos reconocidos en esta Ley, sea admitido como tal ante cualquier autoridad judicial o administrativa, bastará que el nombre o seudónimo, o cualquiera otra denominación que no deje dudas sobre la identidad de la persona natural o jurídica de que se trate, conste en

la obra, interpretación o ejecución, producción o emisión de radiodifusión, en la forma usual.

Art. 291.- Ninguna autoridad, ni persona natural o jurídica podrá autorizar la utilización de una obra, interpretación, producción fonográfica o emisión de radiodifusión o de cualquier otra prestación protegida por esta Ley, o prestar apoyo para su utilización, si el usuario no cuenta con la autorización expresa y previa del titular del derecho o de su representante. En caso de incumplimiento será solidariamente responsable.

Art. 292.- Si la violación de los derechos se realiza a través de redes de comunicación digital, tendrá responsabilidad solidaria el operador o cualquier otra persona natural o jurídica que tenga el control de un sistema informático interconectado a dicha red, a través del cual se permita, induzca o facilite la comunicación, reproducción, transmisión o cualquier otro acto violatorio de los derechos previstos en ésta Ley, siempre que tenga conocimiento o haya sido advertido de la posible infracción, o no haya podido ignorarla sin negligencia grave de su parte.

Se entenderá que ha sido advertido de la posibilidad de la infracción cuando se le ha dado noticia debidamente fundamentada sobre ella.

Los operadores u otras personas naturales o jurídicas referidas en esta norma, estarán exentos de responsabilidad por los actos y medidas técnicas que adopten a fin de evitar que la infracción se produzca o continúe.

Art. 293.- El titular de un derecho sobre marcas, nombres comerciales u obtenciones vegetales que constatare que la Superintendencia de Compañías o de

Bancos, hubiere aprobado la adopción por parte de las sociedades bajo su control de una denominación que incluya signos idénticos a dichas marcas, nombres comerciales u obtenciones vegetales, podrá solicitar al IEPI a través de los recursos correspondientes la suspensión del uso de la referida denominación o razón social para eliminar todo riesgo de confusión o utilización indebida del signo protegido.

El IEPI notificará a las partes y a la Superintendencia de Compañías o de Bancos con la resolución correspondiente; la sociedad tendrá el plazo de noventa días contados a partir de la notificación de la resolución del IEPI, para adoptar otra denominación o razón social; plazo que podrá prorrogarse por una sola vez y por igual tiempo siempre que existieren causas justificadas.

En el evento de que no adoptaren una nueva denominación o razón social dentro del plazo establecido en el inciso anterior, la Superintendencia procederá a disolver o a liquidar la compañía.

CAPITULO II

DE LOS PROCESOS DE PROPIEDAD INTELECTUAL

SECCION I

DE LOS PROCESOS DE CONOCIMIENTO

Art. 294.- Serán competentes para el conocimiento de las controversias sobre esta materia, en primera instancia, los Jueces Distritales de Propiedad Intelectual y, en segunda instancia los Tribunales Distritales de Propiedad Intelectual.

Los recursos de casación que se dedujeren en ésta materia serán conocidos por la Sala Especializada en Propiedad Intelectual de la Corte Suprema de Justicia.

Art. 295.- El Juzgado Distrital de Propiedad Intelectual No. 1, así como el Tribunal Distrital de Propiedad Intelectual No. 1, tendrán como su sede a la ciudad de Quito; y, jurisdicción en las provincias de Pichincha, Imbabura, Carchi, Cotopaxi, Tungurahua, Chimborazo, Bolívar, Pastaza, Napo y Sucumbíos.

El Juzgado Distrital de Propiedad Intelectual No. 2 y el Tribunal Distrital de Propiedad Intelectual No. 2, tendrán como su sede a la ciudad de Guayaquil; y, jurisdicción en las provincias de Guayas, Los Ríos, El Oro y Galápagos.

El Juzgado Distrital de Propiedad Intelectual No. 3 y el Tribunal Distrital de Propiedad Intelectual No. 3, tendrán como su sede a la ciudad de Cuenca y, jurisdicción en las provincias del Azuay, Loja, Cañar, Morona Santiago y Zamora Chinchipe.

El Juzgado Distrital de Propiedad Intelectual No. 4 y el Tribunal Distrital de Propiedad Intelectual No. 4, tendrán como su sede a la ciudad de Portoviejo; y, jurisdicción en las provincias de Manabí y Esmeraldas.

Art. 296.- La competencia en materia de propiedad intelectual se fija de conformidad con las reglas establecidas en los artículos 27, 28, 29 y 30 del Código de Procedimiento Civil y en el presente artículo.

Serán también competentes para conocer éstas causas los jueces del lugar en el que se hubiere cometido la infracción.

Tratándose de transmisiones a través de un satélite, la infracción se entenderá cometida bien en el lugar en que se iniciare dicha transmisión, bien en el lugar en que la señal se hiciere accesible al público de forma predominante.

En caso de infracciones cometidas a través de redes de comunicación digital, se entenderán cometidas las mismas, bien en el lugar en que se encuentren los sistemas informáticos referidos en el artículo 292, bien en el lugar en que la transmisión se hiciere accesible al público de forma predominante.

Art. 297.- Las demandas relacionadas con la propiedad intelectual se tramitarán en juicio verbal sumario, con las modificaciones constantes en el presente Capítulo.

Art. 298.- En los juicios sobre esta materia es admisible la reconvención conexa, la que será resuelta en sentencia, sin que por ello se altere el trámite de la causa. La reconvención será planteada en la audiencia de conciliación, luego de contestada la demanda. En la propia audiencia el actor deberá contestarla. De no hacerlo se tendrá como negativa pura y simple de los fundamentos de hecho y de derecho.

Art. 299.- Si durante el término de prueba se solicitare la actuación de prueba testimonial, el juez señalará día y hora para su recepción en audiencia oral, en la cual la parte que solicitó la prueba formulará sus preguntas pudiendo la otra parte repreguntar.

Art. 300.- Si hubiere necesidad de peritos, se designará uno por cada parte procesal, salvo que las partes estuvieren de acuerdo en la designación de un único perito.

Sin perjuicio de que el o los peritos presenten su informe por escrito, cualquiera de las partes podrán solicitar al juez que éstos concurran a una audiencia para que informen oralmente sobre las cuestiones que les formularen las partes.

Es causal de destitución de los Jueces Distritales de Propiedad Intelectual, además de otras previstas en la Ley, la violación del mandato contenido en esta norma.

Art. 301.- Todas las pruebas solicitadas dentro del término respectivo deberán practicarse dentro de los treinta días siguientes a su conclusión, salvo que las partes de común acuerdo solicitaren una prórroga.

Art. 302.- El juez tendrá la facultad para ordenar que sea presentada la prueba que se encontrare bajo el control de la parte contraria o en su posesión, a cuyo efecto señalará día, lugar y hora para su exhibición. Si la parte requerida no exhibiere la prueba, el juez, para resolver, podrá basarse en la información que le haya suministrado la parte que requirió la prueba.

Si cualquiera de las partes no facilitare las informaciones, códigos de acceso o de cualquier modo impidiere la verificación de instrumentos, equipos u otros medios en los que pueda almacenarse reproducciones no autorizadas, éstos se presumirán violatorios de los derechos de propiedad intelectual.

Si el juicio versare sobre violación de una patente de invención relacionada con procedimientos, la carga de la prueba sobre la licitud del procedimiento utilizado para la fabricación del producto, le corresponderá al demandado.

Art. 303.- La indemnización de daños y perjuicios comprenderá las pérdidas sufridas y el lucro cesante, causadas por la infracción. La cuantía de los ingresos no obtenidos, se fijará teniendo en cuenta entre otros, los siguientes criterios:

a) Los beneficios que el titular hubiese obtenido de no haberse producido la violación;

b) Los beneficios obtenidos por el infractor como consecuencia de la violación;

c) El precio, remuneración o regalía que el infractor hubiese tenido que pagar al titular, para la explotación lícita de los derechos violados; y,

d) Los gastos razonables, inclusive honorarios profesionales, incurridos por el titular con relación a la controversia.

Art. 304.- Las sentencias condenatorias de las acciones civiles por violación de los derechos de propiedad intelectual impondrán al infractor adicionalmente una multa de tres a cinco veces el valor total de los ejemplares de obras, interpretaciones, producciones o emisiones de radiodifusión, o de las regalías que de otro modo hubiere percibido el titular de los derechos por explotación legítima de éstas u otras prestaciones de propiedad intelectual.

Las multas que conforme a esta disposición se recauden se destinarán en un tercio al IEPI; en un tercio al titular del derecho infringido y el tercio restante se distribuirá de la siguiente manera:

a) Presupuesto de la Función Judicial;

b) Fondo de Solidaridad; y,

c) Fomento de Ciencia y Tecnología a través del IEPI.

SECCION II

DE LAS PROVIDENCIAS PREVENTIVAS Y CAUTELARES

Art. 305.- Las providencias preventivas y cautelares relacionadas con la propiedad intelectual, se tramitarán en conformidad con la Sección Vigésima Séptima, Título Segundo, Libro Segundo del Código de Procedimiento Civil, con las modificaciones constantes en esta Sección.

Art. 306.- El juez ordenará la medida al avocar conocimiento de la demanda, siempre que se acompañen pruebas sobre indicios precisos y concordantes que permitan razonablemente presumir la violación actual o inminente de los derechos sobre la propiedad intelectual reconocidos en ésta Ley, o sobre información que conduzca al temor razonable y fundado sobre su violación actual o inminente, atenta la naturaleza preventiva o cautelar de la medida y la infracción de que pueda tratarse.

El juez comprobará si el peticionario es titular de los derechos, a cuyo efecto se estará a las presunciones establecidas en esta Ley. En defecto de información proporcionada con la demanda que permita presumir la titularidad, bastará la declaración juramentada que al efecto se incluya en la demanda.

Art. 307.- El juez exigirá al actor, atentas las circunstancias, que presente fianza o garantía suficiente para proteger al demandado y evitar abusos.

Art. 308.- A fin de evitar que se produzca o continúe la infracción a cualquiera de los derechos reconocidos en la presente Ley, evitar que las mercancías ingresen en los circuitos comerciales, inclusive las mercancías importadas, o bien para preservar las pruebas pertinentes relacionadas con la presunta infracción, los jueces están facultados a ordenar, a petición de parte, las medidas cautelares o preliminares que, según las circunstancias, fueren necesarias para la protección urgente de tales derechos y, en especial:

a) El cese inmediato de la actividad ilícita;

b) La suspensión de la actividad de utilización, explotación, venta, oferta en venta, importación o exportación, reproducción, comunicación, distribución, según proceda; y,

c) Cualquier otra que evite la continuación de la violación de los derechos.

El secuestro podrá ordenarse sobre los ingresos obtenidos por la actividad infractora, sobre bienes que aseguren el pago de la indemnización, sobre los productos o mercancías que violen un derecho de propiedad intelectual, así como sobre los equipos, aparatos y medios utilizados para cometer la infracción y sobre los ejemplares originales que hayan servido para la reproducción o comunicación.

La retención se ordenará sobre los valores debidos por concepto de explotación o remuneración.

La prohibición de ausentarse del país se ordenará si el demandando no tuviere domicilio o establecimiento permanente en el Ecuador.

Art. 309.- El cese inmediato de la actividad ilícita podrá comprender:

a) La suspensión de la actividad infractora o la prohibición al infractor de reanudarla, o ambas;

b) La clausura provisional del local o establecimiento, la que se expedirá necesariamente cuando las mercancías infractoras o ejemplares ilícitos constituyan parte sustancial del comercio habitual del infractor;

c) El retiro del comercio de las mercancías, ejemplares ilícitos u objetos infractores y, su depósito judicial;

d) La inutilización de los bienes u objetos materia de la infracción y, en caso necesario, la destrucción de moldes, planchas, matrices, instrumentos, negativos, plantas o partes de aquellas y demás elementos destinados al empleo de invenciones patentadas, a la impresión de marcas, a la reproducción o comunicación no autorizada, o de aquellos cuyo uso predominante sea facilitar la supresión o neutralización de cualquier medio de protección técnica o de información electrónica y que sirvan predominantemente para actos violatorios de cualquier derecho de propiedad intelectual; y,

Nota: Literal declarado inconstitucional por Resolución Tribunal Constitucional No. 161, publicada en Registro Oficial 173 de 28 de Septiembre del 2000.

e) Cualquier otra medida que resulte necesaria para la protección urgente de los derechos sobre la propiedad intelectual, atenta la naturaleza y circunstancias de la infracción.

Art. 310.- Las medidas serán ejecutadas en presencia del juez, si el actor así lo requiere, quien podrá asesorarse de los peritos necesarios o de funcionarios del IEPI, cuyo dictamen en la propia diligencia constará del acta correspondiente y servirá para la ejecución. La orden que expida el juez conforme con el artículo precedente implicará, sin necesidad de formalidad ulterior o providencia adicional, la posibilidad de adopción de cualquier medida práctica necesaria para la plena ejecución de la medida cautelar, incluyendo el desquebrajamiento de seguridades, sin perjuicio de la facultad del juez de que al momento de la diligencia ordene cualquier otra medida cautelar que resulte necesaria para la protección urgente de los derechos, sea de oficio o a petición verbal de parte.

Art. 311.- Las demandas que se presenten a fin de obtener una medida cautelar, así como las providencias correspondientes, tendrán la categoría de reservadas y no se notificarán a la parte demandada si no hasta después de su ejecución.

Art. 312.- Si el actor indicare que para la prueba de la violación de los derechos se requiere de inspección judicial previa, el juez la dispondrá sin notificar a la parte contraria y podrá ordenar durante la diligencia las medidas cautelares pertinentes. Para este fin concurrirá con los funcionarios que deban cumplir tales medidas.

Art. 313.- En caso de obras fijadas electrónicamente en dispositivos de información digital o por procedimientos análogos, o cuya aprehensión sea difícil o pueda causar graves daños al demandado, el juez, previo consentimiento del actor y si lo considera conveniente, podrá ordenar que los bienes secuestrados permanezcan bajo la custodia del demandado, luego de identificados, individualizados e inventariados, sin perjuicio del secuestro de las fijaciones sobre soportes removibles.

El juez deberá poner sellos sobre los bienes identificados, individualizados e inventariados.

Art. 314.- Cumplida la medida cautelar se citará la demanda al demandado y el juez dispondrá que comience a correr el término de prueba previsto en el artículo 917 del Código de Procedimiento Civil.

Las medidas cautelares caducarán si dentro del término de quince días de ejecutadas no se propone la demanda en lo principal.

En los casos en que las medidas provisionales sean revocadas o caduquen por acción u omisión del demandante, o en aquellos casos en que posteriormente se determine que no hubo infracción o amenaza de infracción de un derecho de propiedad intelectual, el juez competente ordenará al actor, previa petición del demandado, la indemnización de daños y perjuicios.

Art. 315.- Los jueces que no cumplan con lo previsto en el artículo 73 del Código de Procedimiento Civil dentro de las cuarenta y ocho horas siguientes a la recepción de la

demanda o nieguen injustificadamente la adopción de una medida cautelar, serán responsables ante el titular del derecho por los perjuicios causados, sin perjuicio de la acción penal que corresponda.

Art. 316.- A fin de proteger secretos comerciales o información confidencial, en el curso de la ejecución de las medidas cautelares establecidas en esta Ley, únicamente el juez o el perito o peritos que el designe tendrán acceso a la información, códigos u otros elementos, en cuanto sea indispensable para la práctica de la medida. Por parte del demandado podrán estar presentes las personas que éste delegue y por parte del actor su procurador judicial. Todos quienes de este modo tengan acceso a tales informaciones, quedarán obligados a guardar absoluta reserva y quedarán sujetos a las acciones que ésta y otras leyes prescriben para la protección de los secretos comerciales y la información confidencial.

Art. 317.- Ya sea en la práctica de medidas cautelares o en la actuación de pruebas, podrán intervenir como peritos los funcionarios designados por el IEPI. El juez estará obligado a requerir la intervención pericial de tales funcionarios, a solicitud de parte.

Art. 318.- Los jueces observarán adicionalmente los procedimientos y medidas establecidos en convenios o tratados internacionales sobre propiedad intelectual vigentes en el Ecuador, en cuanto sean aplicables. Los jueces estarán exentos de responsabilidad en los términos del artículo 48 numeral 2 del Acuerdo sobre los aspectos de los derechos de Propiedad Intelectual relacionados con el comercio ADPIC.

Art. 324.- Serán reprimidos con prisión de tres meses a tres años y multa de quinientas a cinco mil unidades de valor constante (UVC), tomando en consideración el valor de los perjuicios ocasionados, quienes en violación de los derechos de autor o derechos conexos:

a) Alteren o mutilen una obra, inclusive a través de la remoción o alteración de información electrónica sobre el régimen de derechos aplicables;

b) Inscriban, publiquen, distribuyan, comuniquen o reproduzcan, total o parcialmente, una obra ajena como si fuera propia;

c) Reproduzcan una obra;

d) Comuniquen públicamente obras, videogramas o fonogramas, total o parcialmente;

e) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros reproducciones ilícitas de obras;

f) Reproduzcan un fonograma o videograma y en general cualquier obra protegida, así como las actuaciones de intérpretes o ejecutantes, total o parcialmente, imitando o no las características externas del original, así como quienes introduzcan al país, almacenen, distribuyan, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros tales reproducciones ilícitas; y,

g) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros reproducciones de obras, fonogramas o videogramas en las cuales se ha alterado o removido información sobre el régimen de derechos aplicables.

Art. 325.- Serán reprimidos con prisión de un mes a dos años y multa de doscientos cincuenta a dos mil quinientas unidades de valor contante (UVC), tomando en consideración el valor de los perjuicios ocasionados, quienes en violación de los derechos de autor o derechos conexos:

a) Reproduzcan un número mayor de ejemplares de una obra que el autorizado por el titular;

b) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros reproducciones de obras en número que exceda del autorizado por el titular;

c) Retransmitan por cualquier medio las emisiones de los organismos de radiodifusión; y,

d) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros aparatos u otros medios destinados a descifrar o decodificar las señales codificadas o de cualquier otra manera burlar o quebrantar los medios técnicos de protección aplicados por el titular del derecho.

Art. 326.- Serán reprimidos con prisión de un mes a dos años y multa de doscientos cincuenta a dos mil quinientas unidades de valor constante (UVC), quienes ilícitamente obstaculicen, incumplan o impidan la ejecución de una providencia preventiva o cautelar.

Art. 327.- Son circunstancias agravantes, además de las previstas en el Código Penal, las siguientes:

a) El haber recibido el infractor apercibimiento sobre la violación del derecho;

b) El que los productos materia de la infracción puedan provocar daños a la salud; y,

c) El que las infracciones se cometan respecto de obras inéditas.

Art. 328.- Las infracciones determinadas en este Capítulo son punibles y pesquisables de oficio.

Art. 329.- Las acciones civiles y penales prescriben de conformidad con las normas del Código Civil y del Código Penal, respectivamente, salvo las acciones por violación a los derechos morales, que son imprescriptibles.

Salvo prueba en contrario y, para los efectos de la prescripción de la acción, se tendrá como fecha de cometimiento de la infracción, el primer día del año siguiente a la última edición, reedición, reproducción, comunicación, u otra utilización de una obra, interpretación, producción o emisión de radiodifusión.

Art. 330.- En todos los casos comprendidos en este capítulo, se dispondrá el comiso de todos los objetos que hubieren servido directa o indirectamente para la comisión del delito, cuyo secuestro podrá ser ordenado por el juez penal en cualquier momento durante el sumario y obligatoriamente en el auto de apertura del plenario.

Art. 331.- El producto de las multas determinadas en éste Capítulo será destinado en partes iguales a la Función Judicial y al IEPI, el que lo empleará al menos en un cincuenta por ciento, en programas de formación y educación sobre propiedad intelectual.

LIBRO V

DE LA TUTELA ADMINISTRATIVA DE LOS

DERECHOS DE PROPIEDAD INTELECTUAL

Art. 332.- La observancia y el cumplimiento de los derechos de Propiedad Intelectual son de Interés Público. El Estado, a través del Instituto Ecuatoriano de la Propiedad Intelectual, IEPI, ejercerá la tutela administrativa de los derechos sobre la propiedad intelectual y velará por su cumplimiento y observancia.

Art. 333.- El IEPI a través de las Direcciones nacionales ejercerá, de oficio o a petición de parte, funciones de inspección, vigilancia y sanción para evitar y reprimir violaciones a los derechos sobre la propiedad intelectual.

Art. 334.- Cualquier persona afectada por la violación o posible violación de los derechos de propiedad intelectual podrá requerir al IEPI la adopción de las siguientes medidas:

a) Inspección;

b) Requerimiento de información; y,

c) Sanción de la violación de los derechos de propiedad intelectual.

Art. 335.- Las inspecciones se realizarán por parte de los Directores Nacionales o sus delegados, en la forma que determine el reglamento. Al momento de la inspección y, como requisito para practicarla válidamente, se entregará copia del acto administrativo en el que se la hubiere ordenado y, si fuese aplicable, la solicitud de la parte afectada.

Las peticiones que se presenten para obtener medidas cautelares permanecerán en reserva hasta luego de ejecutadas y, aún con posterioridad deberán adaptarse por las autoridades las medidas necesarias para preservar la confidencialidad de la información no divulgada que haya debido suministrarse en el curso del procedimiento.

Art. 336.- Si durante la diligencia se comprobare, aún presuntivamente, (prima facie) la violación de un derecho de propiedad intelectual o hechos que reflejen inequívocamente la posibilidad inminente de tal violación, se procederá a la formación de un inventario detallado de los bienes, de cualquier clase que estos sean, que se relacionen con tal violación. Se dejará constancia de lo examinado por los medios que de mejor manera permitan apreciar el estado de las cosas inspeccionadas.

Esta medida podrá incluir la remoción inmediata de rótulos que claramente violen derechos de propiedad intelectual, sin perjuicio de la aprehensión y depósito de las mercancías u otros objetos que violen derechos sobre patentes, marcas u otras formas de propiedad intelectual.

El IEPI, a través de las direcciones regionales competentes en razón de la materia, podrá adoptar cualquier medida cautelar de protección urgente de los derechos a que se refiere ésta Ley, si se acompañan a la pretensión cautelar las pruebas a que se refiere el artículo 306. Estas medidas tendrán carácter provisional, y estarán sujetas a revocación o confirmación conforme se dispone en el artículo 339.

Art. 337.- Cuando se presuma la violación de derechos de propiedad intelectual, el IEPI podrá requerir que se le proporcione cualquier información que permita establecer la existencia o no de tal violación. Dicha información deberá ser entregada en un término no mayor de quince días, desde la fecha de la notificación.

Art. 338.- Salvo el caso de medidas cautelares provisionales que se adopten de conformidad con el artículo 336, previo a la adopción de cualquier resolución, se escuchará a la parte contra la cual se inició el procedimiento. Si se estimare conveniente, podrá convocarse a una audiencia en la que los interesados podrán expresar sus posiciones.

Art. 339.- Concluido el proceso investigativo, el IEPI dictará resolución motivada. Si se determinare que existió violación de los derechos de propiedad intelectual, se

sancionará al infractor con una multa de entre veinte y setecientas unidades de valor constante, (UVC) y, podrá disponerse la adopción de cualquiera de las medidas cautelares previstas en esta Ley o confirmarse las que se hubieren expedido con carácter provisional.

Si existiere la presunción de haberse cometido un delito, se enviará copia del proceso administrativo al Juez Penal competente y al Ministerio Público.

Art. 340.- El IEPI impondrá igual sanción a la establecida en el artículo anterior a quienes obstaculizaren o dificultaren el cumplimiento de los actos, medidas o inspecciones dispuestos por el IEPI, o no enviaren la información solicitada dentro del término concedido.

Art. 341.- Anunciada o de cualquier modo conocida la comunicación publicada de una obra legalmente protegida sin que se hubiere obtenido la autorización correspondiente, el titular de los derechos podrá solicitar a la Dirección Nacional de Derechos de Autor y Derechos Conexos que se la prohiba, lo cual será ordenado inmediatamente. Al efecto se presume que el organizador, empresario o usuario no cuenta con la debida autorización por la sola protesta de parte del titular de los derechos.

Art. 342.- Los Administradores de Aduana y todos quienes tengan el control del ingreso o salida de mercaderías al o desde el Ecuador, tienen la obligación de impedir que ingresen o se exporten productos que de cualquier modo violen los derechos de propiedad intelectual.

Si a petición de parte interesada no impidieren el ingreso o exportación de tales bienes, serán considerados cómplices del delito que se cometa, sin perjuicio de la sanción administrativa que corresponda.

Cuando impidieren, de oficio o a petición de parte, el ingreso o exportación de cualquier producto que viole los derechos de propiedad intelectual, lo pondrán en conocimiento mediante informe pormenorizado al Presidente del IEPI, quien en el término de cinco días confirmará o revocará la medida tomada. Confirmada la medida, los bienes serán puestos a disposición de un juez de lo penal.

Si el Administrador de Aduanas o cualquier otro funcionario competente se hubiere negado a tomar la medida requerida o no se hubiere pronunciado en el término de tres días, el interesado podrá recurrir directamente, dentro de los tres días, posteriores, al Presidente del IEPI para que la ordene.

Quien ordene la medida podrá exigir caución de conformidad con el artículo siguiente.

Art. 343.- Sin perjuicio de lo establecido en el artículo anterior, cualquiera de los Directores Nacionales, según el área de su competencia, podrán ordenar a petición de parte, la suspensión del ingreso o exportación de cualquier producto que en cualquier modo viole los derechos de propiedad intelectual.

La resolución se dictará en el término de tres días desde la petición. Si se estima necesario o conveniente, se podrá disponer que el peticionario rinda caución suficiente. Si ésta no se otorgare en el término de cinco días de solicitada, la medida quedará sin efecto.

A petición de la parte afectada con la suspensión, el director Nacional del IEPI, según el caso, dispondrá la realización de una audiencia para examinar la mercadería y, si fuere procedente, revocar la medida. Si no la revocare, dispondrá que todo lo actuado se remita a un juez de lo penal.

Art. 344.- Sin perjuicio de lo establecido en esta Ley, en materia de procedimientos administrativos se aplicará el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva.

Art. 345.- La fuerza pública y en especial la Policía Judicial están obligadas a prestar a los funcionarios del IEPI el auxilio que éstos soliciten para el cumplimiento de sus funciones.

REGLAMENTO GENERAL DE LA ADMINISTRACIÓN DE LOS RECURSOS HUMANOS DEL MINISTERIO PUBLICO DEL ECUADOR

Art. 79.- DE LAS PROHIBICIONES

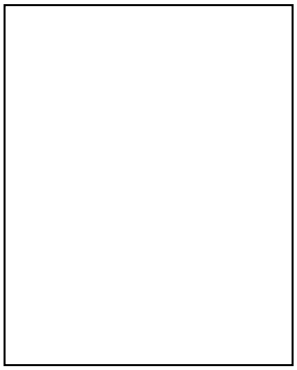
a) Utilizar sin autorización correspondiente los equipos, máquinas, vehículos, suministros y materiales de la Institución o emplearlas en uso distinto de aquel al que por su naturaleza están destinados y a disponer arbitrariamente de estos bienes;

i) Incurrir en actos que impliquen abusos de confianza, fraude, estafa, robos y otros que signifiquen perjuicio para la Institución;

n) Dedicar las horas laborables a juegos o distracciones de cualquier naturaleza que obstaculicen el cumplimiento de su trabajo;

13. q) Alterar informes , reportes, nóminas y cualquier otro documento que sea de uso oficial de la Institución sin el conocimiento y la autorización debidas.

BIOGRAFIA DEL AUTOR



Apellidos: Cortez Cartagena

Nombres: Luis Estalin

Fecha de nacimiento: 14 de abril de 1967

Lugar de nacimiento: Quito – Ecuador

corteze@minpec.gov.ec

Educación formal realizada:

- **Primaria**:

  1973 – 1978 Escuela "Nicolás Coopérnico"

- **Secundaria**:

  1979 – 1986 "Instituto Superior Central Técnico"

  Título obtenido: Bachiller Técnico Industrial

  Especialización: Mecánica Industrial

- **Superior**:

  1992 – 2003 "Escuela Politécnica del Ejército"

  Título obtenido: Egresado de la Facultad de Sistemas e Informática

  Proyecto de tesis: "Plan Maestro de Seguridad Informática para el Ministerio Público del Ecuador"

HOJA DE LEGALIZACION DE FIRMAS

ELABORADO POR

_____

Cortez Cartagena Luis Estalin

DECANO DE LA FACULTAD DE INGENIERIA

_____

ING. MARCO V. QUINTANA C.

MAYO DE E.M.

Sangolquí: 31 de octubre del 2005