



Nº de Reg. 72239
Folio

MINISTERIO DE TRANSPORTES Y COMUNICACIONES

"AÑO DEL ESTADO DE DERECHO Y DE LA GOBERNALIDAD DEMOCRÁTICA"

Lima, 15 ABR. 2004

OFICIO Nº 146 -2004-MTC/17

Señora
LILIANA RUIZ VILCHEZ
Gerenta General
Organismo Supervisor de Inversión
Privada en Telecomunicaciones
Av. De La Prosa 136
San Borja.-

OSIPTEL
2004 APR 15 AM 10:14
RECEPCION

Ref. : C.207-GG.GL/2004 e Informe de Evaluación

De mi consideración:

Me dirijo a usted, en atención a los documentos de la referencia, relacionados con la solicitud de renovación gradual del plazo de concesión presentada por Telefónica del Perú S.A.A, a fin de solicitarle se sirva ampliar su Informe de Evaluación, de acuerdo con los requerimientos establecidos en el Anexo 01, el mismo que forma parte integrante del presente.

Asimismo, debo manifestarle que de acuerdo a los Contratos de Concesión, Cláusula 4, Sección 4.03, literal (b), su Informe de Evaluación deberá señalar sí, y en que medida, la empresa concesionaria, durante el periodo de los 5 años anteriores o durante el plazo de la concesión, ha cumplido con cada una de las obligaciones señaladas en los puntos: i), ii), iii), iv) y v). En tal sentido, es necesario que el Informe de Evaluación indique si la empresa concesionaria ha cumplido o no con sus obligaciones, precisando expresamente el criterio y grado de cumplimiento de cada una de ellas (conforme lo señala vuestro Informe de Evaluación remitido con carta C.207-GG.GL/2004, en su numeral 5, de la parte I. Antecedentes, respecto al: cumplimiento, incumplimiento en menor grado o cumplimiento en mayor grado).



Por otro lado, a fin de contar con mayores elementos para realizar la evaluación correspondiente, mucho agradeceré se sirva pronunciarse respecto a si los incumplimientos controvertidos en el Poder Judicial o en vía arbitral, surten efectos para lo dispuesto en la sección 4.04 de los contratos de concesión aprobados por Decreto Supremo Nº 011-94-TCC.

Finalmente, solicito a usted se sirva evaluar los comentarios u objeciones remitidos con los documentos que a continuación se detallan, cuyas copias se adjuntan, por contener temas de su competencia:

- Carta P/D Nº 015719 de la empresa Rural Telecom S.A.C.;
- Oficio P/D Nº 016286 de la Defensoría del Pueblo;
- Carta P/D Nº 015934 de la Asociación de Consumidores y Usuarios;



MINISTERIO DE TRANSPORTES Y COMUNICACIONES

"AÑO DEL ESTADO DE DERECHO Y DE LA GOBERNALIDAD DEMOCRÁTICA"

- Carta P/D N° 014004 del Sindicato de Trabajadores de Telefónica del Perú S.A.A.;
- Copia del correo electrónico remitido por el Congresista de la República Yonhy Lescano.

Mucho agradeceré se sirva alcanzar a este Despacho la información antes solicitada, en un plazo no mayor de diez (10) días hábiles.

Sin otro particular, hago propicia la ocasión para expresarle los sentimientos de mi mayor consideración.

Atentamente,




Ing. JORGE ENRIQUE DE LA ROCA CHALCO
Director General de Gestión
de Telecomunicaciones



OFICIO N° 146-2004-MTC/17

MINISTERIO DE TRANSPORTES Y COMUNICACIONES

ANEXO 1

OBSERVACIONES AL INFORME DE EVALUACIÓN

CLÁUSULA 6

Sección 6.01 y 6.04, Pago de tasa por explotación comercial del servicio y canon por uso de espectro radioeléctrico.

OBSERVACIÓN: Se recomienda pronunciarse en forma expresa sobre el cumplimiento de esta sección. Para tal efecto, se remite copia del Memorándum N° 266-2004-MTC/03.03 de la Oficina de Recaudación y Soporte Operativo sobre el estado de los pagos de la tasa y canon.

Secciones 6.02 y 6.03, respecto al Fondo de Inversión de Telecomunicaciones (FITEL) y Tasa por Servicio de Supervisión.

OBSERVACIÓN: Se recomienda precisar si TELEFÓNICA ha cumplido con el pago correspondiente al Fondo de Inversión de Telecomunicaciones y Tasa por Servicio de Supervisión del año 2003, al vencimiento del plazo para que la empresa presente su declaración jurada.

Sección 6.05, Base de cálculo para el pago de derechos y tasas.

OBSERVACIÓN: Precisar si para efectos del cálculo del pago de tasas y derechos especiales creados por la Ley de Telecomunicaciones y la Ley 26285, TELEFÓNICA ha incluido los ingresos brutos facturados y percibidos anualmente, por concepto de la prestación de los servicios de telecomunicaciones y los ingresos provenientes por el tráfico internacional de entrada y salida, tal como lo prevé la mencionada sección.

Sección 6.06, Pago Total.

OBSERVACIÓN: Se recomienda pronunciarse en forma expresa sobre el cumplimiento de esta sección. Para tal efecto, se remite copia del Memorándum N° 266-2004-MTC/03.03 de la Oficina de Recaudación y Soporte Operativo sobre el estado de los pagos de la tasa y canon.

Sección 6.07, Normas Complementarias.

OBSERVACIÓN: Se recomienda pronunciarse en forma expresa sobre el cumplimiento de esta sección. Para tal efecto, se remite copia del Memorándum N° 266-2004-MTC/03.03 de la Oficina de Recaudación y Soporte Operativo sobre el estado de los pagos de la tasa y canon.



CLÁUSULA 8

Sección 8.01, Prestación de los Servicios Públicos de Telecomunicaciones, a) Obligación del Servicio y b) Continuidad del servicio,

OBSERVACIÓN: Precisar si la empresa presta los servicios en el área de concesión de acuerdo con los términos del contrato, la Ley de Telecomunicaciones, sus Reglamentos y demás normas pertinentes.

Si bien en el numeral III de su informe denominado "obligaciones establecidas en la cláusula 8: Obligación de la empresa concesionaria" (Pág.12), indica que la empresa ha cumplido lo señalado en el literal b) de la Sección 8.01 de los contratos de



OFICIO N° 146-2004-MTC/17

MINISTERIO DE TRANSPORTES Y COMUNICACIONES

concesión, también señala que se suspendió el servicio, por lo que se le inició un procedimiento sancionador y, posteriormente, se le condonó la deuda. En ese sentido, se le solicita informar el grado de cumplimiento o incumplimiento de esta sección.

Asimismo, deberá informar sobre la verificación de la continuidad de la prestación de los servicios en los centros poblados contenidos en los anexos 1A, 1B y 1C, del contrato de concesión de ex ENTEL, parte II, por ser un tema de competencia de OSIPTEL, independientemente de la obligación que tiene TELEFÓNICA de informar sobre las interrupciones del servicio al MTC. Para tal efecto se remite copia de la información presentada al MTC sobre el particular.

Sección 8.02 del Contrato de Concesión ex ENTEL PERÚ S.A. parte I y ex CPT S.A. Prestación del servicio de arrendamiento de líneas y circuitos locales.

OBSERVACIÓN: Precisar si la empresa ha cumplido con los plazos ofertados para proveer en arrendamiento las líneas o circuitos locales de acuerdo a lo establecido en los párrafos primero y segundo de esta sección.

Sección 8.02 del Contrato de Concesión ex ENTEL PERÚ S.A. parte II. Prestación del servicio de arrendamiento de líneas y circuitos.

OBSERVACIÓN: Precisar si la empresa ha cumplido con los plazos ofertados para proveer en arrendamiento las líneas o circuitos de larga distancia, de acuerdo a lo establecido en los párrafos primero, segundo y tercero de esta sección.

Sección 8.04, Obligaciones en caso de Emergencia o Crisis.

Emergencia con relación a Desastres Naturales
Emergencia relacionada con la Seguridad Nacional

OBSERVACIÓN: Es necesario que se pronuncie sobre el cumplimiento de esta sección.

Sección 8.05, Requisitos de expansión de la red. (Contratos de Ex ENTEL, parte I y Ex CPT. S.A.)

OBSERVACIÓN: Ampliar su informe de evaluación respecto a los párrafos 2, 3, 4 y 5 del literal a) de esta sección. Asimismo, precisar si TELEFÓNICA ha cumplido con los literales (b) Área de Expansión, (c) Presentación del Plan de Expansión de Líneas de Abonado, (d) Presentación del Plan de Expansión de Líneas de Abonado modificado y (e) Presentación del Plan de Expansión de Líneas de Abonado Reducido; de esta sección.

En cuanto al literal a), deberá cumplir con presentar la evaluación del indicador Tiempo Máximo de Espera para Conexión para el año 2003, teniendo en cuenta que el plazo para el cumplimiento de esta obligación venció el 31 de diciembre de 2003, de acuerdo con lo establecido en los contratos de concesión.

En lo relativo al literal c), OSIPTEL debe evaluar el cumplimiento de la presentación al MINISTERIO y a OSIPTEL, del programa quinquenal del plan de expansión de líneas de abonado para los cinco (5) años siguientes, respetando cuando menos el compromiso de expansión mínimo establecido en el anexo 2.





OFICIO N° 146-2004-MTC/17

MINISTERIO DE TRANSPORTES Y COMUNICACIONES

Sección 8.05: Requisitos de Expansión de la Red (Contrato de Ex ENTEL, parte II)
OBSERVACIÓN: OSIPTEL no se ha pronunciado sobre los incisos a), b), c), d) y f), referidos a Metas de Expansión, Obligación del Servicio, Derecho de Preferencia, Instalación de Teléfonos Públicos y Contratos Necesarios, respectivamente, toda vez que señaló de manera general que el cumplimiento de la sección 8.05 ya fue informado al Ministerio con carta N° C.114-PD.L/99 del 19.02.99, en el Informe de Evaluación emitido con ocasión de la primera solicitud de renovación solicitada por la empresa.

OSIPTEL debe informar detalladamente sobre el cumplimiento de dichas obligaciones durante la totalidad del periodo comprendido entre los años 1999 -2003.

En lo que se refiere al literal c), deberá precisar si TELEFÓNICA ha cumplido con mantener interconectados los centros poblados sobre los cuales ejerció su derecho de preferencia.

Sección 8.06, Teléfonos Públicos (Contratos de Ex ENTEL, parte I y Ex CPT. S.A.)

- a) Plan de Expansión
- b) Líneas de Interconexión

OBSERVACIÓN: Se señala que el cumplimiento del indicador instalación de teléfonos públicos fue informado al Ministerio con carta N° C.114-PD.L/99, del 19.02.99, en el Informe de Evaluación remitido con ocasión de la primera solicitud de renovación.

No obstante, OSIPTEL debe informar si TELEFÓNICA mantiene el número de líneas instaladas de conformidad con los Anexos 1 (Ex CPT) y 2 (Ex ENTEL); y asimismo, precisar si los teléfonos públicos instalados brindan acceso a todos los servicios de la categoría I.

Finalmente, es necesario que OSIPTEL se pronuncie respecto al cumplimiento del literal b) de esta sección, denominado "Líneas de Interconexión".

Sección 8.06, Calidad del Servicio (Contrato con Ex ENTEL, parte II)

OBSERVACIÓN: Se señala que se ha evaluado el cumplimiento de este indicador para el período 1999 a 2002, debido a que la supervisión del año 2003 recién se efectúa en el año 2004, indicando que la empresa concesionaria para este período ha cumplido con su obligación.

No obstante, OSIPTEL debe cumplir con presentar la evaluación de este indicador para el año 2003, teniendo en cuenta que el plazo para su cumplimiento venció el 31 de diciembre de 2003 y el plazo para la presentación de la información de los indicadores de calidad anual para el año 2003 venció el 30 de enero de 2004, de acuerdo a lo establecido en el contrato de concesión y el procedimiento de supervisión y control de calidad del servicio respectivamente.

Secciones 8.07 de los Contratos de Concesión ex CPT S.A. y ex ENTEL PERÚ S.A., parte I, Requisitos de calidad de servicio





OFICIO N° 146-2004-MTC/17

MINISTERIO DE TRANSPORTES Y COMUNICACIONES

OBSERVACIÓN: Es necesario que se incluya en el Informe de Evaluación al año 2003, conforme lo indica el Anexo 3, del Contrato de Concesión de ex ENTEL PERÚ S.A., parte I y Anexo 2 del Contrato de Concesión Ex CPT S.A.

Secciones 8.09 de los contratos de concesión de ex ENTEL PERÚ S.A. parte I y ex CPT S.A., **8.08** del contrato de concesión de ex ENTEL PERÚ S.A. parte II, Requisitos Mínimos

Los requisitos de expansión de la red, requisitos de teléfonos públicos y requisitos de calidad de servicio establecidos en las secciones 8.05, 8.06 y 8.07 y especificados en los Anexos 2 y 3, constituyen las obligaciones mínimas que la EMPRESA CONCESIONARIA debe cumplir de acuerdo con los cronogramas establecidos en las fechas de vencimiento allí previstas.

OBSERVACIÓN: Es necesario que OSIPTEL se pronuncie sobre el cumplimiento de esta sección.

Secciones 8.10 de los Contratos de Concesión de ex ENTEL PERÚ S.A. parte I y ex CPT S.A., y **8.09** del Contrato de Concesión de ex ENTEL PERÚ S.A. parte II. Secreto de las Telecomunicaciones y Protección de Datos.

- a) Obligación de Salvaguardar el Secreto de Telecomunicaciones y Protección de Datos
- b) Ámbito de la Obligación de Secreto y Protección de Datos
- c) Seguridad Nacional
- d) Medidas de Cumplimiento

OBSERVACIÓN: Deberá precisar el cumplimiento de los literales (a), (b), (c) y (d) de esta sección. Para tal efecto, se adjunta el Memorandum N° 571-2004-MTC/18 de la Dirección General de Control y Supervisión de Telecomunicaciones y el Informe N° 217-2003-MTC/18.01.1 de la Dirección de Monitoreo e Inspección de Telecomunicaciones.

Secciones 8.11 de los contratos de concesión ex CPT S.A. y ex ENTEL PERÚ S.A. parte I, y **8.10** del contrato de concesión de ex ENTEL PERÚ S.A., parte II. Requisitos de Asistencia a Abonados y Usuarios

OBSERVACIÓN: Con relación al literal a), si bien OSIPTEL indica que en los procedimientos que se han tramitado ante el Tribunal Administrativo de Solución de Reclamos de Usuarios (TRASU), no se han encontrado casos por incumplimiento de esta obligación en última instancia administrativa, por lo que se podría considerar que la empresa concesionaria ha cumplido con las obligaciones contenidas en este punto; por otro lado, las evaluaciones efectuadas para los incisos b) y c) sólo se refieren al servicio de telefonía fija. En tal sentido, deberá precisar si la evaluación efectuada corresponde también a la parte II del contrato de ex -ENTEL, es decir, al servicio portador de larga distancia nacional e internacional.

Respecto al literal (b), si bien se señala que la empresa ha venido incumpliendo con sus obligaciones relativas a la Solución de Reclamos y Conflictos, al incurrir permanentemente en errores reiterados; explicando además que el criterio para definir el incumplimiento de esta obligación se ha determinado a partir de la revisión de quejas declaradas fundadas y de las sanciones impuestas por el Tribunal Administrativo de Solución de Reclamos de Usuarios (TRASU) por incumplimiento de la normativa existente, la información adicional que sustenta esta afirmación está





OFICIO N° 146-2004-MTC/17

MINISTERIO DE TRANSPORTES Y COMUNICACIONES

relacionada aparentemente sólo con el servicio de telefonía fija, por lo que se deberá complementar la evaluación de este punto.

Finalmente, es necesario que OSIPTEL se pronuncie respecto al cumplimiento de cada una de las obligaciones contenidas en el literal c) de esta sección, comprendiendo a todos los teléfonos, tal como lo establecen los contratos de concesión, toda vez que el informe de evaluación sólo menciona a los teléfonos públicos.

Secciones 8.12 de los contratos de concesión ex CPT S.A. y ex ENTEL PERÚ S.A., parte I, y **8.11** del contrato de concesión de ex ENTEL PERÚ S.A. parte II. Cooperación con otros prestadores de servicios públicos de telecomunicaciones.

OBSERVACIÓN: Su informe de evaluación deberá precisar expresamente si TELEFÓNICA cumplió con esta obligación.

Secciones 8.14 de los contratos de concesión ex CPT S.A. y ex ENTEL PERÚ S.A. parte I, y **8.13** del contrato de concesión de ex ENTEL PERU S.A. parte II. Archivo y Requisitos de Información.

OBSERVACIÓN: Su informe de evaluación deberá incluir si la empresa cumplió con la información solicitada por el Ministerio.

Sección 4.03, literal b). (v) CUMPLIMIENTO CON LAS LEYES DEL PERÚ

OBSERVACIÓN: OSIPTEL adjunta documentación remitida por entidades públicas, pero es necesario que precise si TELEFÓNICA cumplió o no cumplió las obligaciones de prestar sus servicios públicos de telecomunicaciones y llevar sus negocios conforme a las leyes del Perú.

Asimismo, sírvase informar sobre el estado de la denuncia en contra de Telefónica del Perú S.A.A. y diversas personas por violación al Secreto de las Telecomunicaciones, indicando en qué medida afecta la obligación contenida en esta sección.





MINISTERIO DE TRANSPORTES Y COMUNICACIONES

MEMORANDUM N° 266 - 2004-MTC/03.03

A : DIRECTOR GENERAL DE GESTION DE TELECOMUNICACIONES

Asunto: Situación de Pagos de la empresa Telefónica del Perú S.A.A.

Ref. : Memorandum N° 611-2004-MTC/17

Fecha: Lima, 26 MAR. 2004

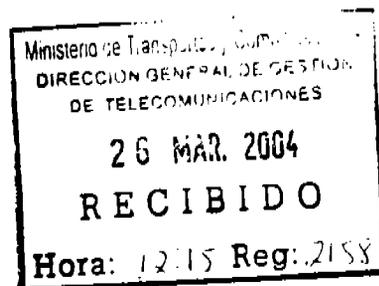
Me dirijo a usted, con relación al documento de la referencia, a fin de remitirle un informe de los pagos efectuados por la empresa TELEFÓNICA DEL PERU S.A.A., por concepto **tasa** anual de los años 2000, 2001, 2002 y 2003, y por concepto **canon** de los años 2001, 2002, 2003 y 2004; con lo cual se da cumplimiento al requerimiento de su Despacho.

Atentamente,



C. Salardi B

.....
Dco. CARMEN SALARDI BRAMONT
DIRECTORA
Oficina de Recaudación y Soporte Operativo
Viceministerio de Comunicaciones



EMPRESA : TELEFONICA DEL PERU S.A.A.
 SERVICIO : SERVICIOS PUBLICOS
 CONCEPTO: PAGOS REALIZADOS POR CONCEPTO DE TASA ANUAL
 PERIODO : 2000 - 2001- 2002 - 2003

AÑO 2000

MES	Nº FACT/RECIBO	FECHA	MONTO PAGADO
ENERO	11584	10-02-00	1.526.458,00
FEBRERO	12754	10-03-00	1.521.601,00
MARZO	13773	10-04-00	1.665.951,00
ABRIL	14652	10-05-00	1.346.539,00
MAYO	15631	12-06-00	1.604.628,00
JUNIO	16463	10-07-00	1.399.406,00
JULIO	17334	10-08-00	1.484.118,00
AGOSTO	18161	11-08-00	1.672.994,00
SEPTIEMBRE	19139	10-10-00	1.547.064,00
OCTUBRE	20303	10-11-00	1.533.551,00
NOVIEMBRE	21214	11-12-00	1.498.343,00
DICIEMBRE	22034	10-01-01	1.577.665,00
TOTAL DEL PAGO A CUENTA			18.378.318,00
INGRESOS BRUTOS DELAÑO 3,060'340,017,00			15.301.700,08
SALDO A FAVOR			3.076.617,92

AÑO 2001

MES	Nº FACT/RECIBO	FECHA	MONTO PAGADO
ENERO	022981	12-02-01	1.527.353,00
FEBRERO	024387	12-03-01	1.366.693,00
MARZO	025501	10-04-01	1.604.044,00
ABRIL	(*) DEC S/PAGO	10-05-01	1.259.243,00
MAYO	(*) DEC S/PAGO	11-06-01	1.401.125,00
JUNIO	(*) DEC S/PAGO	10-07-01	416.250,00
JUNIO	028870	10-07-01	793.075,00
JULIO	029955	10-08-01	1.352.268,00
AGOSTO	031021	10-09-01	1.226.020,00
SEPTIEMBRE	032145	10-10-01	1.223.641,00
OCTUBRE	033358	12-11-01	1.408.086,00
NOVIEMBRE	034574	10-12-01	1.258.778,00
DICIEMBRE	035603	10-01-02	1.271.661,00
TOTAL DEL PAGO A CUENTA			16.108.237,00
INGRESOS BRUTOS DELAÑO 3,198'319,336,00			15.991.596,68
SALDO A FAVOR			116.640,32

(*) APLICACIÓN DEL SALDO A FAVOR AÑO 2000



EMPRESA : TELEFONICA DEL PERU S.A.A.
 SERVICIO : SERVICIOS PUBLICOS
 CONCEPTO: PAGOS REALIZADOS POR CONCEPTO DE TASA ANUAL
 PERIODO : 2000 - 2001- 2002 - 2003

AÑO 2002

MES	Nº FACT/RECIBO	FECHA	MONTO PAGADO
ENERO	036774		
FEBRERO	038126	11-02-02	1.376.229,00
MARZO	039379	11-03-02	1.186.133,00
ABRIL	(*) DEC S/PAGO	10-04-02	1.260.295,00
ABRIL	040586	10-05-02	116.640,00
MAYO	041691	10-05-02	1.234.112,00
JUNIO	042893	10-06-02	1.231.110,00
JULIO	00631	10-07-02	1.136.619,00
AGOSTO	01953	12-08-02	1.245.913,00
SEPTIEMBRE	03405	10-09-02	1.118.366,00
OCTUBRE	04801	10-10-02	1.106.983,00
NOVIEMBRE	06240	11-11-02	1.154.722,00
DICIEMBRE	00300	10-12-02	1.032.827,00
		10-01-03	1.153.786,00
TOTAL DEL PAGO A CUENTA			14.353.735,00
INGRESOS BRUTOS DELAÑO 3.026'563,183,00			15.132.815,91
SALDO POR REGULARIZAR			-779.080,91

AÑO 2003

MES	Nº FACT/RECIBO	FECHA	MONTO PAGADO
ENERO	01804	10-02-03	1.060.993,00
FEBRERO	03712	10-03-03	957.347,00
MARZO	05469	10-04-03	1.251.327,00
ABRIL	05470		781.781,00
ABRIL	06816	REGULARIZACION AÑO 2002	28.889,00
ABRIL	06822	REINT. ABRIL 2003	1.152.453,00
MAYO	08222	12-05-03	1.516.481,00
JUNIO	09739	10-06-03	992.185,00
JULIO	11170	10-07-03	1.276.216,00
AGOSTO	12612	11-08-03	1.110.715,00
SEPTIEMBRE	13995	10-09-03	1.167.063,00
OCTUBRE	15500	10-10-03	1.352.213,00
OCTUBRE	15501	10-11-03	4.512,00
NOVIEMBRE	16822	10-11-03	1.169.993,00
DICIEMBRE	00459	10-12-03	1.301.220,00
		12-01-04	15.123.388,00
TOTAL DEL PAGO A CUENTA			15.123.388,00



EMPRESA : TELEFONICA DEL PERU S.A.A.
SERVICIO : SERVICIOS PUBLICOS
CONCEPTO: PAGOS REALIZADOS POR CONCEPTO DE CANON ANUAL
PERIODO : 2001 - 2002- 2003 - 2004

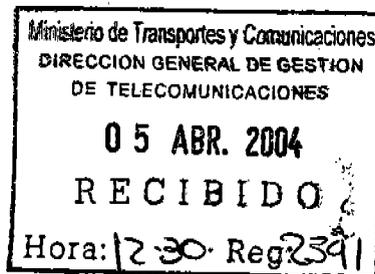
AÑO	Nº FACT/RECIBO	FECHA	MONTO PAGADO
2001	23704	28-02-01	1.425.420,00
2002	37684	28-02-02	1.505.526,00
2003	03228	28-02-03	1.317.564,00
2004	02982	27-02-04	1.508.736,00
TOTAL DEL CANON PAGADO			5.757.246,00



L.



MINISTERIO DE TRANSPORTES Y COMUNICACIONES
Dirección General de Control y Supervisión de Telecomunicaciones



MEMORANDO N° 571 -04-MTC/18

Al : Ing. Jorge De la Roca Chalco
Director General de Gestión de Telecomunicaciones

Asunto : Información de Telefónica del Perú S.A.A., referente al Secreto de las Telecomunicaciones y Protección de Datos.

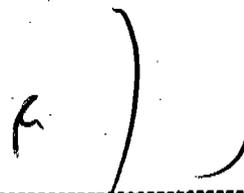
Ref. : GGR-107-A-126/OT-04

Fecha : Lima, 05 ABR 2004

Tengo el agrado de dirigirme a usted, a fin de remitirle copia de la información anual que obra en nuestro poder como DGCST para los años 2003 y 2004, enviada por la empresa TELEFONICA DEL PERU S.A.A., con la que dá cumplimiento a lo establecido en la Resolución Ministerial N° 622-96-MTC/15.17, que aprueba los "Procedimientos de Inspección y Requerimiento de Información relacionados al Secreto de las Telecomunicaciones y Protección de Datos".

Asimismo se adjunta copia del Informe N° 217-2003-MTC/18.01.1 del 22.09.2003, con los resultados de la verificación técnica que se hiciera a la mencionada operadora, a fin de comprobar las medidas de seguridad y protección a las comunicaciones de los abonados y usuarios del servicio telefónico. Dicho informe no registra ningún reparo importante sobre estas medidas.

Atentamente,


Ing. GUILLERMO VILLANUEVA PINTO
Director General de Control y
Supervisión de Telecomunicaciones

Adj.: Lo indicado (72 fs.):
- Carta GGR-107-A-081/OT-03 (14.Feb.2003) (P/D 008690)
- Carta GGR-107-A-126/OT-04 (13.Feb.2004) (P/D 009191)
2004-04-05



MINISTERIO DE TRANSPORTES Y COMUNICACIONES
DIRECCIÓN GENERAL DE CONTROL Y SUPERVISIÓN DE TELECOMUNICACIONES

Lima,

22 SET. 2003

INFORME N° 217 -2003-MTC/18.01.1

Señor : Director de Monitoreo e Inspección de Telecomunicaciones.
Asunto : Verificación Técnica a empresa de Servicio Público de Telefonía Fija Local sobre medidas de protección al secreto de las comunicaciones.
Ref. : R.M. N° 622-96-MTC-15.17 de fecha 21 de noviembre de 1996.

Tenemos el agrado de dirigimos a usted, con relación al asunto en mención, a fin de hacer de su conocimiento lo siguiente:

I. ANTECEDENTE

En cumplimiento a lo dispuesto en la Directiva N° 002-96-MTC/15.17 aprobado mediante Resolución Ministerial N° 622-96-MTC/15.17, por el que se establece los procedimientos de inspección y requerimiento de información, relacionados al secreto de las telecomunicaciones y la protección de datos, se programó una verificación técnica a las instalaciones de la empresa **TELFÓNICA DEL PERÚ S.A.A.**, operadora que cuenta con concesión de este Ministerio, a fin de comprobar las medidas de seguridad y protección a las comunicaciones de los abonados y usuarios del servicio telefónico.

II. MEDIDAS DE PROTECCIÓN ADOPTADAS POR LA EMPRESA

- II.1. Durante la inspección se trataron tres aspectos fundamentales en relación al secreto de telecomunicaciones: a) Seguridad de las comunicaciones en el lado del cliente, b) Acceso del personal autorizado a los nodos y c) Acceso a la información de abonados del sistema
- II.2. Con respecto a la seguridad del terminal de abonado para su operación, los representantes de la empresa manifestaron que La responsabilidad de la empresa en el lado del cliente, termina en el block de conexión. A este se conecta el aparato o el sistema telefónico (teléfono, Central Telefónica, etc.), de propiedad y responsabilidad del abonado. La Planta Externa, conformada por las instalaciones de comunicaciones que van desde el domicilio del abonado hasta la Central Telefónica pública, puede ser accesada a través de las cajas terminales telefónicas, armarios telefónicos o en los buzones telefónicos. Las cajas terminales que concentran los cables que van hacia las ubicaciones de los abonados, han sido instalados en lugares de difícil acceso. Los armarios que concentran los cables que van hacia las cajas terminales, tienen candado en unos casos o sistema de seguridad en otros, requiriendo de un código o del uso de una tarjeta mas una clave de seguridad, para su apertura. Los buzones tienen tapas que han sido selladas con soldadura.

Los servicios de instalación y mantenimiento preventivo de las líneas de abonado, están tercerizados. Las empresas subcontratadas están sujetas a un contrato mediante el cual, tienen la obligación de comunicar la relación del personal técnico involucrado en los servicios solicitados así como portar la debida identificación ante los abonados de la empresa. La empresa verifica al culminar una instalación, el correcto cumplimiento del requerimiento efectuando una llamada de comprobación al abonado.



MINISTERIO DE TRANSPORTES Y COMUNICACIONES
DIRECCIÓN GENERAL DE CONTROL Y SUPERVISIÓN DE TELECOMUNICACIONES

- II.3. En relación al acceso del personal autorizado a los nodos, De acuerdo a la normativa vigente de la empresa, para que el personal autorizado y funcionarios de OSIPTEL o del MTC en visitas de inspección, pueda ingresar a uno de los nodos de la red de la empresa, se requiere de una autorización escrita o vía e-mail, emitida por cualquiera de las gerencias de red a la gerencia de seguridad.

De acuerdo a los procedimientos de seguridad establecidos, las personas deben identificarse y registrarse al momento de ingresar, siendo responsabilidad del personal de seguridad, verificar el permiso otorgado al personal visitante. Al momento de salir, el personal de seguridad debe registrar la salida del personal visitante. En casos extremos, el jefe de seguridad tiene la potestad para permitir el ingreso al personal visitante

De manera complementaria, la empresa cuenta con un Sistema Inteligente de Seguridad (Tele Vigilancia electrónica a distancia), instalado en diferentes locales de la empresa a nivel nacional, que permite controlar el flujo de movimiento de personal en ambientes restringidos, así como el control de daños a la planta y bienes ubicados dentro de estos.

- II.4. Con respecto al acceso a la información de abonados del sistema, la empresa tiene clasificada de dos maneras la información de sus clientes: pública (No. de abonado, nombre, dirección, etc., siempre que el abonado no haya solicitado la exclusión de la publicación de sus datos en la Guía Telefónica) y no pública. La información declarada como no pública (facturación, estadísticas de llamadas, etc.), es de acceso de los funcionarios de la empresa, la cual únicamente se entrega al abonado titular del servicio o a los usuarios que cuenten con autorización expresa del titular. En caso de detalle de llamadas se requiere además de firma legalizada notarialmente.

III. CONCLUSIONES

- III.1. La interceptación telefónica en la última milla de la red de Planta Externa de abonados es factible y no se requiere de equipamiento sofisticado para ello. En el tramo que va desde los armarios hasta el domicilio de los usuarios, es el mas vulnerable debido a que es accesible. La empresa ha manifestado las limitaciones en este sentido y las previsiones que ha tomado a nivel de armarios y buzones.
- III.2. La empresa entregó una copia del informe anual sobre medidas y procedimientos para salvaguardar el secreto de las telecomunicaciones y confidencialidad de la información de la información de los usuarios de los servicios públicos de Telecomunicaciones, en cumplimiento a la Directiva N° 002-96-MTC/15.17 que establece las medidas de protección al secreto de las comunicaciones.

IV. RECOMENDACIONES

- IV.1. Continuar las Inspecciones iniciadas a las instalaciones de la empresa, preferentemente de manera inopinada, a fin de volver a corroborar el cumplimiento de los procedimientos de seguridad.
- IV.2. Modificar la Directiva N° 002-96-MTC/15.17, que limita al MTC a inspecciones con aviso previo de 48 horas, a fin de hacer más efectivas las labores de inspección y verificación.



MINISTERIO DE TRANSPORTES Y COMUNICACIONES
DIRECCIÓN GENERAL DE CONTROL Y SUPERVISIÓN DE TELECOMUNICACIONES

Es cuanto cumplimos con informar a usted, de acuerdo a lo solicitado

ING. JULIO CONTRERAS ORTIZ
Especialista en Telecomunicaciones

ING. ADOLFO VALENZUELA ATANACIO
Especialista en Telecomunicaciones

ING. JAVIER MANSILLA YANQUI
Especialista en Telecomunicaciones

El suscrito eleva a su despacho el presente informe para los fines pertinentes.

.....
ADOLFO VALENZUELA ATANACIO
Sub-Director de Control Lima
Dirección de Monitoreo e Inspección de Telecomunicaciones



MINISTERIO DE TRANSPORTES Y COMUNICACIONES
DIRECCIÓN GENERAL DE CONTROL Y SUPERVISIÓN DE TELECOMUNICACIONES

ACTA DE VERIFICACIÓN

SERVICIO PÚBLICO DE TELEFONÍA FIJA LOCAL

En el distrito de Lince, Provincia de Lima, departamento de Lima, siendo las 10:00 horas del día 04 de setiembre de 2003, de conformidad con lo dispuesto en el T.U.O. de la Ley de Telecomunicaciones, D.S. N° 013-93-TCC y su Reglamento General, aprobado mediante D.S. N° 006-94-TCC, y modificatorias; en presencia de los representantes de la Dirección General de Control y Supervisión de Telecomunicaciones (DGCST) por parte del Ministerio de Transportes y Comunicaciones (MTC): Sres. Julio Contreras Ortiz, Adolfo Valenzuela Atanacio y Javier Mansilla Yanqui; y de otra parte los Sres. Carlos Barreda Tamayo, Jorge Reyes Vargas Machuca, Giuliana Herrera Rambla, Edy Céspedes Livia, María Luisa Arrese Rodríguez, José Luis Bravo Caro y José Valdivia Santibáñez, en calidad de representantes de la empresa TELEFÓNICA DEL PERÚ S.A.A., (que para efectos de la presente Acta se denominará "La empresa"), se procedió de oficio al desarrollo de la Verificación Técnica de las medidas de protección en relación al Secreto de la Telecomunicaciones, habiéndose constatado lo siguiente:

I. DATOS GENERALES:

Razón Social	:	TELEFÓNICA DEL PERÚ S.A.A.
Domicilio Legal	:	Av. Arequipa 1155, Sta. Beatriz, Cercado de Lima
Representante Legal	:	Jorge Melo Vega
Resolución Ministerial	:	D.S. 11-94-TC
Contrato de Concesión firmado el	:	16.05.1994

I.1. Seguridad de las comunicaciones en el lado del cliente.

La responsabilidad de la empresa en el lado del cliente, termina en el block de conexión. A este se conecta el aparato o el sistema telefónico (teléfono, Central Telefónica, etc.), de propiedad y responsabilidad del abonado. La Planta Externa, conformada por las instalaciones de comunicaciones que van desde el domicilio del abonado hasta la Central Telefónica pública, puede ser accesada a través de las cajas terminales telefónicas, armarios telefónicos o en los buzones telefónicos. Las cajas terminales que concentran los cables que van hacia las ubicaciones de los abonados, han sido instalados en lugares de difícil acceso. Los armarios que concentran los cables que van hacia las cajas terminales, tienen candado en unos casos o sistema de seguridad en otros, requiriendo de un código o del uso de una tarjeta mas una clave de seguridad, para su apertura. Los buzones tienen tapas que han sido selladas con soldadura.

Los servicios de instalación y mantenimiento preventivo de las líneas de abonado, están tercerizados. Las empresas subcontratadas están sujetas a un contrato mediante el cual, tienen la obligación de comunicar la relación del personal técnico involucrado en los servicios solicitados así como portar la debida identificación ante los abonados de la empresa. La empresa verifica al culminar una instalación, el correcto cumplimiento del requerimiento efectuando una llamada de comprobación al abonado.

[Handwritten signature]



MINISTERIO DE TRANSPORTES Y COMUNICACIONES
DIRECCIÓN GENERAL DE CONTROL Y SUPERVISIÓN DE TELECOMUNICACIONES

1.2. Acceso del personal autorizado a los nodos de la red.

De acuerdo a la normativa vigente de la empresa, para que el personal autorizado y funcionarios de OSIPTEL o del MTC en visitas de inspección, pueda ingresar a uno de los nodos de la red de la empresa, se requiere de una autorización escrita o vía e-mail, emitida por cualquiera de las gerencias de red a la gerencia de seguridad.

De acuerdo a los procedimientos de seguridad establecidos, las personas deben identificarse y registrarse al momento de ingresar, siendo responsabilidad del personal de seguridad, verificar el permiso otorgado al personal visitante. Al momento de salir, el personal de seguridad debe registrar la salida del personal visitante. En casos extremos, el jefe de seguridad tiene la potestad para permitir el ingreso al personal visitante.

De manera complementaria, la empresa cuenta con un Sistema Inteligente de Seguridad (Tele Vigilancia electrónica a distancia), instalado en diferentes locales de la empresa a nivel nacional, que permite controlar el flujo de movimiento de personal en ambientes restringidos, así como el control de daños a la planta y bienes ubicados dentro de estos.

1.3. Acceso a la información de los clientes de la empresa.

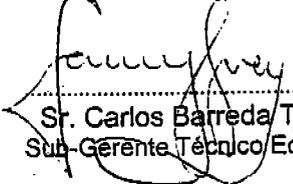
La empresa tiene clasificada de dos maneras la información de sus clientes: pública (No. de abonado, nombre, dirección, etc., siempre que el abonado no haya solicitado la exclusión de la publicación de sus datos en la Guía Telefónica) y no pública. La información declarada como no pública (facturación, estadísticas de llamadas, etc.), es de acceso de los funcionarios de la empresa, la cual únicamente se entrega al abonado titular del servicio o a los usuarios que cuenten con autorización expresa del titular. En caso de detalle de llamadas se requiere además de firma legalizada notarialmente.

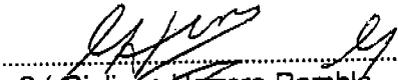
II. OBSERVACIÓN

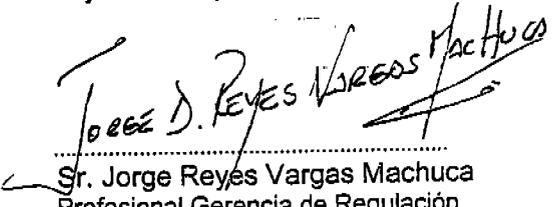
La empresa entregó una copia del informe anual sobre medidas y procedimientos para salvaguardar el secreto de las telecomunicaciones y confidencialidad de la información de la información de los usuarios de los servicios públicos de Telecomunicaciones.

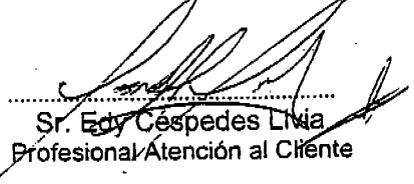
Siendo las 12:30 horas del día 04 de setiembre de 2003, y no habiendo nada más que agregar, se dio por terminada la Verificación Técnica, procediendo a firmar el presente en señal de conformidad, los representantes del MTC y de la empresa:

POR LA EMPRESA:


Sr. Carlos Barreda Tamayo
Sub-Gerente Técnico Económico


Sr. Giuliana Herrera Rambla
Profesional Gerencia de Regulación

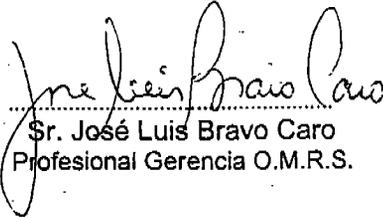

Sr. Jorge Reyes Vargas Machuca
Profesional Gerencia de Regulación

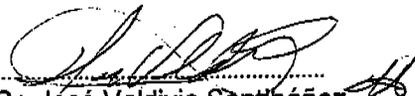

Sr. Eddy Céspedes Livia
Profesional Atención al Cliente



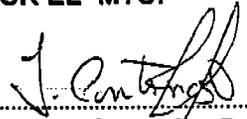
MINISTERIO DE TRANSPORTES Y COMUNICACIONES
DIRECCIÓN GENERAL DE CONTROL Y SUPERVISIÓN DE TELECOMUNICACIONES

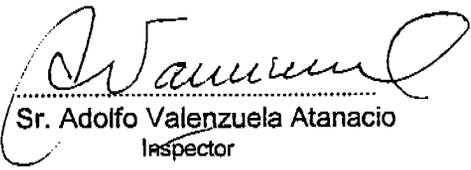

Sra. María Luisa Arrese Rodríguez
Profesional Soporte Comercial


Sr. José Luis Bravo Caro
Profesional Gerencia O.M.R.S.

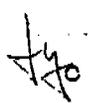

Sr. José Valdivia Santibáñez
Profesional Gerencia O.M.R.S.

POR EL MTC:


Sr. Julio Contreras Ortiz
Inspector


Sr. Adolfo Valenzuela Atanacio
Inspector


Sr. Javier Mansilla Yanqui
Inspector











MINISTERIO DE TRANSPORTES Y COMUNICACIONES
DIRECCIÓN GENERAL DE CONTROL Y SUPERVISIÓN DE TELECOMUNICACIONES

ACTA DE VERIFICACIÓN

SERVICIO PÚBLICO DE TELEFONÍA FIJA LOCAL

En el distrito de Lince, Provincia de Lima, departamento de Lima, siendo las 10:00 horas del día 04 de setiembre de 2003, de conformidad con lo dispuesto en el T.U.O. de la Ley de Telecomunicaciones, D.S. N° 013-93-TCC y su Reglamento General, aprobado mediante D.S. N° 006-94-TCC, y modificatorias; en presencia de los representantes de la Dirección General de Control y Supervisión de Telecomunicaciones (DGCST) por parte del Ministerio de Transportes y Comunicaciones (MTC): Sres. Julio Contreras Ortiz, Adolfo Valenzuela Atanasio y Javier Mansilla Yanqui; y de otra parte los Sres. Jorge Reyes Vargas Machuca, Carlos Barreda Tamayo, María Luz Arrese Rodríguez y José Valdivia Santibáñez, en calidad de representantes de la empresa TELEFÓNICA DEL PERÚ S.A.A. (que para efectos de la presente Acta se denominará "La empresa"), se procedió de oficio al desarrollo de la **Verificación Técnica de las medidas de protección en relación al Secreto de la Telecomunicaciones**, habiéndose constatado lo siguiente:

LOS DATOS GENERALES:

Razón Social	:	TELEFÓNICA DEL PERÚ S.A.A.
Domicilio Legal	:	Av. Arequipa 1155, Sta. Beatriz, Lince
Representante Legal	:	Jorge Melo Vega
Resolución Ministerial	:	D.S. 11-94-TC
Contrato de Concesión firmado el	:	16.05.1994

1.1. Seguridad de las comunicaciones en el lado del cliente.

La responsabilidad de la empresa en el lado del cliente, termina en el block de conexiones. A este se conecta el aparato o el sistema telefónico (teléfono, Central Telefónica, etc.), de propiedad y responsabilidad del abonado. La Planta Externa, conformada por las instalaciones de comunicaciones que van desde el domicilio del abonado hasta la Central Telefónica pública, puede ser accesada a través de las cajas terminales telefónicas, armarios telefónicos o en los buzones telefónicos. Las cajas terminales que concentran los cables que van hacia las ubicaciones de los abonados, han sido instalados en lugares de difícil acceso. Los armarios que concentran los cables que van hacia las cajas terminales, tienen candado en unos casos o sistema de seguridad en otros, requiriendo de un código o del uso de una tarjeta mas una clave de seguridad, para su apertura. Los buzones tienen tapas que han sido selladas con soldadura.

Los servicios de instalación y mantenimiento preventivo de las líneas de abonado, están tercerizados. Las empresas subcontratadas están sujetas a un contrato mediante el cual, tienen la obligación de comunicar la relación del personal técnico involucrado en los servicios solicitados así como portar la debida identificación ante los abonados de la empresa. La empresa verifica al culminar una instalación, el correcto cumplimiento del requerimiento.

1.2. Acceso del personal autorizado a los nodos de la red.

De acuerdo a la normativa vigente de la empresa, para que el personal autorizado y no autorizado pueda ingresar a uno de los nodos de la red de la empresa, se requiere de una autorización escrita o vía e-mail, emitida por cualquiera de las gerencias de red a la gerencia de seguridad. De acuerdo a los procedimientos de seguridad establecidos,



MINISTERIO DE TRANSPORTES Y COMUNICACIONES
DIRECCIÓN GENERAL DE CONTROL Y SUPERVISIÓN DE TELECOMUNICACIONES

el personal autorizado y no autorizado debe identificarse y registrarse al momento de ingresar siendo responsabilidad del personal de seguridad, verificar el permiso otorgado al personal visitante. Al momento de salir, el personal de seguridad debe registrar la salida del personal visitante. En casos extremos, el jefe de seguridad tiene la potestad para permitir el ingreso al personal visitante.

De manera complementaria, la empresa cuenta con un Sistema Inteligente de Seguridad (Tele Vigilancia electrónica a distancia), instalado en diferentes locales de la empresa a nivel nacional, que permite controlar el flujo de movimiento de personal en ambientes restringidos, así como el control de daños a la planta y bienes ubicados dentro de estos.

I.3. **Acceso a la información de los clientes de la empresa.**

La empresa tiene clasificada de dos maneras la información de sus clientes: pública (No. de abonado, nombre, dirección, etc.) y no pública. La información declarada como no pública (facturación, estadísticas de llamadas, etc.), no son de acceso de los funcionarios de la empresa.

II. **OBSERVACIONES**

- II.1.
.....
- II.2.
.....

Siendo las 12:30 horas del día 04 de setiembre de 2003, y no habiendo nada más que agregar, se dio por terminada la Verificación Técnica, procediendo a firmar el presente en señal de conformidad, los representantes del MTC y de la empresa:

POR EL MTC:

POR LA EMPRESA:

.....
Sr. Julio Contreras Ortiz
Inspector

.....
Sr. Jorge Reyes Vargas Machuca
Coordinador de Inspecciones

.....
Sr. Adolfo Valenzuela Atanasio
Inspector

.....
Sr. Carlos Barreda Tamayo
Sub-Gerente Técnico Económico

.....
Sr. Javier Mansilla Yanqui
Inspector

.....
Sra. María Luz Arrese Rodríguez
Supervisor del Área de Soporte Comercial

.....
Sr. José Valdivia Santibáñez
Jefe de Conmutación

Telefonica

CARGO

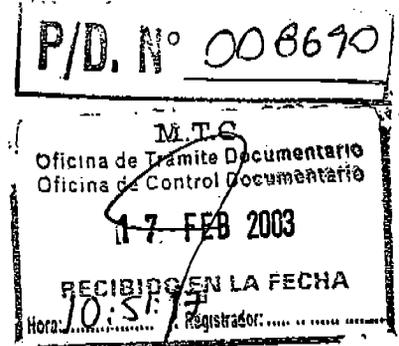
Hortencia Rozas Olivera
Gerente Regulación

Telefónica del Perú S.A.A.
Av. Arequipa 1155 - Piso 8
Lima 1 - Perú
Telfs. : (51 1) 472-8534 / 210-1089
 : (51 1) 210-1087
Fax : (51 1) 471-0064
E-mail : hrozas@tp.com.pe

GGR-107-A-081/OT-03

Lima, 14 de Febrero del 2003

Señor
Luis Ames Sora
Director de Desarrollo de Servicios
de Telecomunicaciones
Ministerio de Transportes y Comunicaciones
Presente.-



Ref.- Oficio N° 690-2003-MTC/15.19.04.1

Por medio de la presente y dando cumplimiento a lo dispuesto por la Directiva N° 002-96-MTC/15.17 aprobada por Resolución Ministerial N° 622-96-MTC/15.17, alcanzamos el informe anual sobre las medidas y procedimientos establecidos por Telefónica del Perú S.A.A., con la finalidad de salvaguardar el Secreto de las Telecomunicaciones y mantener la confidencialidad de la información personal de los usuarios de los Servicios Públicos de Telecomunicaciones.

Cabe destacar que las medidas y procedimientos establecidos en los años precedentes básicamente se mantienen vigentes, salvo algunas medidas adicionales que se han establecido en el presente año y que se detallan en el documento adjunto.

Por otro lado, en las relaciones que tenemos con proveedores que tienen que ver con la prestación de nuestros servicios a los usuarios, se han establecido cláusulas de salvaguarda del secreto y confidencialidad de la información de abonados a los que por razón de la prestación del servicio, podrían tener acceso.

Asimismo es conveniente indicar que para todos los efectos, el área encargada de coordinar la implementación, cumplimiento y supervisión de la salvaguarda del Secreto de las Telecomunicaciones y la Protección de datos de nuestros clientes, es la Gerencia Central de Regulación y Planificación Estratégica, a través de la Gerencia de Regulación.

Finalmente, teniendo en consideración el carácter reservado y confidencial de la información que entregamos adjunta, agradeceremos adoptar las medidas del caso para que dicha información no sea utilizada para fines distintos a los que motivan su entrega; solicitándole que la misma no sea puesta en conocimiento de terceros.

Sin otro particular, aprovecho la oportunidad para reiterarle mis sentimientos de aprecio y consideración.

Atentamente,

INFORMACION RESERVADA

TELEFONICA DEL PERU S.A.A.

**GERENCIA CENTRAL DE REGULACIÓN Y
PLANIFICACIÓN ESTRATÉGICA**

**INFORME ANUAL SOBRE MEDIDAS Y PROCEDIMIENTOS
PARA SALVAGUARDAR EL SECRETO DE LAS TELECOMUNICACIONES Y
CONFIDENCIALIDAD DE LA INFORMACIÓN PERSONAL DE
LOS USUARIOS DE LOS SERVICIOS PÚBLICOS DE
TELECOMUNICACIONES**

AÑO 2003

INFORMACION RESERVADA

GERENCIA DE REGULACIÓN Y PLANIFICACIÓN ESTRATÉGICA

Encargada de coordinar la implementación, cumplimiento y supervisión de la salvaguarda del Secreto de las Telecomunicaciones y la Protección de Datos de nuestros clientes.

CARGO	NOMBRE Y APELLIDOS
Gerente	HORTENCIA ROZAS OLIVERA
Gestor de Negocios	FLOR MONTALVAN DAVILA

En agosto de 1997, la Vicepresidencia Ejecutiva Legal y Organismos Regulatorios, emitió la circular s/n sobre "Cumplimiento de medidas para salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos", la cual sigue vigente y es de aplicación en los respectivos negocios.

INFORMACION RESERVADA

GERENCIA DE SEGURIDAD Y PROTECCIÓN

Procedimientos establecidos en la Gerencia que apoyan a salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos.

PROTECCIÓN DE LA INFORMACIÓN EMPRESARIAL

A continuación los procedimientos establecidos por la Jefatura de Protección de la Información Empresarial que apoyan a salvaguardar el Secreto de las Telecomunicaciones y protección de datos.

Medidas Técnicas:

- Evaluaciones técnicas para verificación de riesgos potenciales de la información física en los diferentes negocios.
- Actividad de supervisión de destrucción de desechos de oficina en los principales locales del grupo Telefónica.

Medidas Organizativas:

- Elaboración de nueva normativa: Clasificación y Tratamiento de la información.
- Normativa sobre el manejo de computadores portátiles en el Grupo.
- Cumplimiento del proceso de destrucción de desechos en las oficinas locales.

Medidas Humanas:

- Capacitación a los trabajadores de las distintas Unidades de Negocios del Grupo Telefónica en medidas para proteger su información.
- Actualización permanente de Base de Datos del Personal Crítico de los Negocios.
- Campaña de comunicación anual en medidas preventivas para proteger la información y la implementación, a nivel nacional, del primer programa de reconocimiento: Escritorios Limpios y Seguros, que tiene como objetivo motivar la participación de los trabajadores en la práctica de conductas seguras para proteger la información. Se diseñaron mensajes preventivos para difundir a través de los diversos medios de comunicación interna: afiches, sistema vantive, vía mail, boletines, etc.
- Diseño del Boletín Segurinot@s, donde se imparten recomendaciones para proteger

INFORMACION RESERVADA

- Empleo de los canales informáticos para la transmisión de mensajes por las PCs a los trabajadores de las Empresas.
- Empleo de los boletines de las Unidades de Negocios para difundir recomendaciones para la Protección de la Información.

JEFATURA CENTRO DE OPERACIONES

Medidas Técnicas

El Sistema Inteligente de Seguridad (SIS)

Sistema de Tele Vigilancia electrónica a distancia, instalado en diferentes locales de la Empresa a Nivel Nacional. La configuración electrónica de este sistema, permite controlar el flujo de movimiento de personal en ambientes restringidos, así como el control de daños a la planta y los bienes ubicados dentro de estos.

Este sistema, está orientado al control de accesos del personal propio y ajeno, así como a la seguridad electrónica, sin que se requiera la presencia permanente de personal.

Dentro de estos dispositivos, con el que cuenta el sistema tenemos:

- Un Centro de Recepción de Alarmas y Tele servicios (CRAT)
- Cámaras de CCTV, instalados en lugares estratégicos..
- Las áreas técnicas responsables tienen un terminal del mismo sistema CCTV.
- Sensores de movimiento (PIRS), ubicados en lugares estratégicos.
- Sensores iónicos.
- Sensores térmicos.
- Sensores magnéticos.

Funcionalidad:

- Gestión remota y centralizada de alarmas.
- Telecontrol de sistemas de extinción de incendios y servicios técnicos.
- Control remoto del acceso de personal autorizado por las Áreas de las Empresas (Identificación visual, oral o electrónica).
- Vigilancia remota, mediante cámaras y micrófonos.
- Base de datos y aplicaciones que facilitan la gestión y explotación del sistema.

Medidas Humanas **Servicios de Seguridad**

Dentro de los servicios de seguridad se encuentran la Vigilancia Privada, Guardianía y los Grupos de Reacción Móviles.

Vigilancia Privada

INFORMACIÓN RESERVADA

de acceso autorizado por las áreas de las Empresas y atención de ocurrencias de seguridad física.

Así mismo, los puestos de vigilancia y Centros de Control cuentan con los procedimientos y la normativa interna vigente.

Grupo Móviles de Reacción

El grupo consiste de un vehículo y un supervisor de vigilancia que atiende las alarmas que reporte el SIS a nivel nacional se cuenta con 17 grupos de reacción a nivel nacional; el 50% dotado con personal policial para cualquier intervención de ser necesario. Así mismo, estos grupos tienen funciones de patrullaje en la Planta Externa a fin de reducir los actos delictivos en contra de la misma.

Sistema de Control de Accesos en Línea

Se cuenta con un sistema de Control de Accesos en Línea, donde las diferentes áreas de la Empresa gestionan y autorizan el ingreso del personal de trabajadores propios y de terceros a los diferentes locales de la Empresa.

Este sistema permite verificar en Lima si el personal que intenta ingresar a los locales, autorizado por las diferentes áreas, tiene o no algún impedimento para su ingreso.

Medidas Organizativas

Procedimientos Operativos

Como complemento al Sistema Inteligente de Seguridad (SIS) y a los Servicios de Seguridad, se cuenta con normas y procedimientos escritos, estas son:

Normas

- Norma de Control de Accesos.
- Prevención del Espionajes Empresarial.
- Procedimiento de actuación para la atención de autorizaciones de acceso.
- Procedimiento de controlar el acceso de personal vinculado a medios de comunicación
- Procedimiento de actuación para el robo de cables aéreos y subterráneos.
- Control de ingreso y salida de personal de Centros de Cómputo.

Por lo antes expuesto, es preciso mencionar que los sistemas implementados permiten efectuar el Control de Accesos, en otras palabras permitir el ingreso sólo del personal autorizado por las áreas de las Empresas, mas no el de verificar los trabajos que se realizan dentro de estos ambientes ni verificar el tipo de herramientas o equipamiento que se empleen ya que la vigilancia y guardianía no disponen de los criterios técnicos para realizar estas tareas.

INFORMACION RESERVADA

GERENCIA DE SISTEMAS DE INFORMACIÓN

1. Procedimientos para salvaguardar el secreto de las telecomunicaciones.

Las medidas aprobadas por la Gerencia de Sistemas para mantener la confidencialidad de la información (que se describen en el punto 2) contribuyen a salvaguardar el secreto de las telecomunicaciones.

2. Relación y contenido de las medidas y procedimientos establecidos para mantener la confidencialidad de la información personal de nuestros usuarios.

Normativa:

La Gerencia de Sistemas de Información, a través de la Jefatura de Seguridad y Testing, ha establecido, la siguiente normativa para mantener la información que Telefónica guarda en los sistemas de información.

1. Políticas de Seguridad de Información.
2. Política para la atención de Solicitudes de Acceso a los Sistemas Corporativos.
3. Normas de Seguridad (para Administradores) contra virus informáticos.
4. Normas de Seguridad (para Usuarios) contra virus informáticos.
5. Normas de Seguridad (para Administradores) en Aplicaciones.
6. Normas de Seguridad (para Usuarios) en Aplicaciones.
7. Normas de Seguridad (para Administradores) en Correo Electrónico.
8. Normas de Seguridad (para Usuarios) en Correo Electrónico.
9. Normas de Seguridad (para Administradores) en acceso a Sistemas operativos, redes y comunicaciones.
10. Normas de Seguridad (para Usuarios) en acceso a sistemas operativos, redes y comunicaciones.
11. Normas de Seguridad (para Administradores) en Internet.
12. Normas de Seguridad (para Usuarios) en Internet.
13. Normas de Seguridad (para Administradores) en la implementación y administración de bases de datos.
14. Normas Generales de Seguridad en el manejo de Computadores Portátiles.

La normativa orientada a los administradores establece los requisitos mínimos que deben implementarse y cumplirse para considerar las aplicaciones como seguras.

La normativa orientada a los usuarios establece las responsabilidades de estos en el uso de sistemas de información.

La normativa indicada se encuentra publicada en la intranet de la compañía para uso interno de los empleados de Telefónica.

Monitorización y revisiones de los Sistemas de Información:

Para mantener el control de los accesos en la red de ordenadores de Telefónica, los que pudieran afectar la confidencialidad de la información, se han implementado las siguientes medidas:

INFORMACIÓN RESERVADA

- Uso de herramientas para la detección de intrusos
- Revisiones periódicas de vulnerabilidades en los computadores y elementos de comunicación de la red corporativa
- Uso de herramientas de detección de cambios en los sistemas operativos de los sistemas de información corporativos
- Revisión y mantenimiento periódico de los niveles de acceso de los usuarios a los sistemas de información.
- Gestión de accesos centralizada, con procedimientos formalizados de creación, modificación y eliminación de accesos.

Medidas de Seguridad de Información en la Gerencia de Sistemas

Cumplimiento de la normativa antes descrita mediante la implementación del Consejo de Arquitectura de la GSI, evaluación del Comité de Seguridad y pruebas a los programas efectuadas por el equipo de Testing, que evalúan el

cumplimiento de los requisitos mínimos de las aplicaciones que ingresan a producción. Formación del grupo CRISIS para la evaluación técnica de problemas de seguridad en los sistemas de información, conformada por los especialistas de las áreas técnicas correspondientes.

Establecimiento de un esquema de seguridad e implementación de herramientas de seguridad de información y auditoría a nivel de red (firewalls) y sistemas operativos.

Medidas de seguridad física en los Centros de Procesamiento de Datos CPD. Sistema

Integral de Seguridad en los CPD, el sistema de seguridad incluye:

1. Sistema automático de extinción en incendios FM200.
2. Sistema de alarmas y sensores contra incendio, intrusión e inundación.
3. Sistema de Control de acceso, mediante huella digital, tarjetas de proximidad, esclusa de ingreso detectora de metales y de peso, y sistema de evacuación de emergencia con puertas de apertura y cierre automáticos (sistema antipánico)
4. Sistema de Vigilancia 7x24 externo e interno mediante circuito cerrado de TV, grabadoras VHS de eventos.
5. Sistema Integrador y Puesto de Control desde donde se monitorean los niveles de seguridad de los sistemas anteriormente descritos así como los sistemas secundarios de UPS, energía, aire acondicionado.
6. Procedimientos de control de acceso y operación de los sistemas de seguridad bajo la supervisión de la Gerencia de Seguridad y Protección.

Contingencia: Se ha implantado un esquema de contingencia para los sistemas de información mediante el cual existe un CPD principal que alberga los actuales sistemas en producción y un CPD secundario, que alberga las plataformas alternas que se utilizarían en una eventual contingencia. Incluye un sistema automatizado (robot) de backup y sistemas de alta disponibilidad de discos.

Plan de Concientización de Seguridad de Información

Realización del Plan de Concientización de Seguridad de Información el mismo que está dirigido a todos los empleados y que considera:

- Distribución y difusión de las normas de seguridad de Información, mediante PANTALLAS de inicio de sesión y publicación en la intranet de la compañía para consulta de los empleados de Telefónica.
- Charlas específicas sobre seguridad en los sistemas para personal *con* puestos críticos, que incluye a ejecutivos, asistentes de gerencia-secretarías, personal de operadores y administradores de los sistemas y personal recién incorporado a la empresa.
- Distribución y difusión de Boletines de Seguridad de sistemas y encartes.
- Presentaciones a las Gerencias sobre Uso de Cuentas de Acceso, incluye:
 - Política para Atención de Solicitud de Acceso a los Sistemas Corporativos.
 - Normas de cuenta de usuario.
 - Recomendaciones para crear una buena clave-ejemplo de claves.
 - Como cambiar la clave de acceso en Windows NT -en Aplicaciones.
 - Cómo bloquear la PC.
 - Procedimiento para solicitar una cuenta de acceso en red-a los aplicativos.
 - Recomendaciones - protegerse de Virus -Conclusiones.
 - Donde reportar fallas.

3. La dependencia y el personal responsable que tiene a su cargo la implementación, cumplimiento y supervisión de las medidas y procedimientos adoptados para salvaguardar el secreto y la confidencialidad de la información.

- La política de seguridad de información define los lineamientos que rigen para asegurar la confidencialidad de la información en los sistemas, estableciendo las funciones de los propietarios y de los custodios de la información.
- En referencia a la confidencialidad de la información contenida en los sistemas han designado a las personas de la relación adjunta como autorizados a definir los accesos y niveles (perfiles) de acceso a las aplicaciones respectivas.

4. La relación de las dependencias y personas responsables de su área, que por la naturaleza de sus funciones tienen acceso a la red pública de telecomunicaciones o a la información confidencial de los abonados.

El personal de operadores y administradores de las aplicaciones tienen, por la naturaleza de sus funciones, acceso a los archivos de programas y de datos.

- El acceso de los operadores y administradores a los sistemas es con cuentas personales auditadas.
- Las cuentas de ADMINISTRADOR propietarias de los sistemas se encuentra en sobre cerrado lacrado y guardado en custodia del Centro de Cómputo. Existe procedimiento de control de uso de las cuentas de ADMINISTRADOR.
- La información confidencial de los abonados se encuentra encriptada a requerimiento de los negocios de Telefónica que así lo han dispuesto.

INFORMACIÓN RESERVADA

- En estos casos es accesible mediante opciones de la aplicación a las cuáles sólo tienen acceso personas que el negocio ha terminado.
- Igualmente, esas opciones tienen implementadas controles de auditoría.
- Los operadores principalmente no tienen acceso a estas opciones, en los que tiene el acceso la opción está auditada.

Personal Responsable:

Sug gerente

Fernando De Los Ríos Boggio

INFORMACION RESERVADA

GERENCIA DE TELEFONIA DE USO PUBLICO

1. Relación y contenido de las medidas y procedimientos establecidos para salvaguardar el secreto de las telecomunicaciones.

En la Gerencia Telefonía de Uso Público, se aplican las medidas y procedimientos corporativos que han sido establecidas por diferentes áreas de la empresa. Paralelamente se aplican las medidas internas que ha diseñado el propio negocio.

1.1 Medidas corporativas

1.1.1 Elaboradas por la Gerencia de Seguridad y Protección, cuya finalidad es proteger la información empresarial y el patrimonio de Telefónica. Entre sus normas destacan las siguientes:

- SSP-008. "Prevención del Espionaje Empresarial".
- SSP-018. "Protección de la información".
- SSP-023. "Prevención del Fraude".

1.1.2 Elaboradas por la Gerencia de Sistemas de Información, cuya finalidad es proteger los sistemas operativos, redes e infraestructura de Telefónica. Entre sus normas destacan las siguientes:

- "Normas de seguridad para los usuarios de aplicaciones".
- "Normas generales de seguridad en el acceso de usuarios a sistemas operativos, redes y comunicaciones".

1.2 Medidas Internas del negocio

Exigencias contractuales a los arrendadores de espacios para teléfonos públicos de interior (TPI) y Locutorios Públicos.

Exigencias contractuales a las empresas que ejecutan trabajos de recaudación, instalación y mantenimiento de equipos terminales, así como a aquellas encargadas de la distribución y comercialización de los productos de telefonía pública.

Procedimientos internos para la atención de pedidos de insatisfacción de nuestros arrendadores y/o usuarios, que garanticen la protección el secreto de las telecomunicaciones.

2. Relación y contenido de las medidas y procedimientos establecidos para mantener la confidencialidad de la información personal de nuestros usuarios.

En los contratos de arrendamiento para la prestación del servicio de telefonía pública en establecimientos, se ha incluido una cláusula específica, sobre la protección del secreto de las telecomunicaciones.

3. Dependencia y personal responsable que tiene a su cargo la implementación, cumplimiento y supervisión de las medidas y procedimientos adoptados para salvaguardar el secreto y confidencialidad de la información.

INFORMACION RESERVADA

Gerencia Telefonía de Uso Público	Jesús Abárzuza Gil
Sub Gerencia Comercial	Nélida Schrader Loechle
Sub Gerencia Post Venta	María Jesús Herrera Portuondo
Sub Gerencia Estrategia y Planificación	José Antonio Cassinelli Sánchez

4. La relación de las dependencias y personas responsables de su área, que por la naturaleza de sus funciones tienen acceso a la Red Pública de Telecomunicaciones o a la información confidencial de los abonados.

Sub Gerencia Comercial: Fernando Silva Chávez, Carlos Ponce Bezold, Ana Váldez Ampuero, Daniel Torpoco Carmen, Alejandro Iglesias Ruiz-Huidobro, Milagros Fernández Valle, Gonzalo Fernández Aguilar.

Sub Gerencia Post Venta: Carlos García Ferreyra, Abraham Quipe Ramírez, Enrique Wu Gondo.

Sub Gerencia Estrategia y Planificación: Ricardo León Venegas

Telefonica

P/D. N° 009191

JORGE MELO-VEGA CASTRO
Gerente Central de Regulación
y Planificación Estratégica

GGR-107-A-126/OT-04

Lima, 13 de febrero de 2004

Ministerio de Transportes y Comunicaciones
TRAMITE
VICE DE COMUNICACIONES
16 FEB. 2004
RECIBIDO
Reg. N° Hora 16:55 PM

M.T.C.
O.T.D.
Ofic. de Control Documentario
16 FEB 2004
RECIBIDO EN LA FECHA
Hora..... Registrador.....

Señor
Juan Antonio Pacheco Romani
Viceministro de Comunicaciones
Ministerio de Transportes y Comunicaciones
Presente.

De mi mayor consideración:

Por medio de la presente y dando cumplimiento a lo dispuesto por la Directiva N° 002-96-MTC/15.17 aprobada por Resolución Ministerial N° 622-96-MTC/15.17, alcanzamos a su Despacho dentro del plazo establecido, el informe anual sobre medidas y procedimientos establecidos por Telefónica del Perú S.A.A., con la finalidad de salvaguardar el Secreto de las Telecomunicaciones y mantener la confidencialidad de la información personal de los usuarios de los servicios públicos de telecomunicaciones.

Cabe precisar que como parte del cumplimiento de nuestra obligación de velar por el Secreto de las Telecomunicaciones y Protección de Datos, hemos desarrollado una serie de políticas y prácticas para su salvaguarda, las cuales varían con el tiempo teniendo en cuenta el constante avance de las tecnologías que se implementan. En tal sentido, hemos actualizado nuestra normativa interna y adicionalmente se ha implementado un programa de capacitación y difusión intensiva de la citada normativa.

Finalmente, teniendo en consideración el carácter reservado y confidencial de la presente información, agradeceremos adoptar las medidas del caso para que dicha información no sea utilizada para fines distintos a los que motivan su entrega; solicitándole que la misma no sea puesta en conocimiento de terceros.

Sin otro particular, quedo de usted.

Atentamente,



M.T.C.
Vice-Ministerio de Comunicaciones
Sub-Mesa de Control Documentario
17 FEB. 2004
RECIBIDO
Reg. N°:
Hora: 16:30. Folio:



TELEFÓNICA DEL PERÚ S.A.A.
Av. Arequipa 1155 piso 8, Lima I
Teléfono (51 1) 266-9010. Fax (51 1) 210-1431

CONFIDENCIAL

TELEFÓNICA DEL PERÚ S.A.A.

**GERENCIA CENTRAL DE REGULACIÓN Y PLANIFICACIÓN
ESTRATÉGICA**

**INFORME ANUAL SOBRE MEDIDAS Y PROCEDIMIENTOS
PARA SALVAGUARDAR EL SECRETO DE LAS TELECOMUNICACIONES Y
CONFIDENCIALIDAD DE LA INFORMACIÓN PERSONAL DE
LOS USUARIOS DE LOS SERVICIOS PÚBLICOS DE TELECOMUNICACIONES**

AÑO 2004

ESTRUCTURA DEL INFORME

El presente informe lo hemos elaborado teniendo en cuenta cada uno de los procesos por los que discurre la información que es necesario salvaguardar.

Cada uno de los procesos se encuentra a cargo de determinadas gerencias, las que son responsables internamente de adoptar las medidas necesarias para cuidar el secreto de las telecomunicaciones y confidencialidad de la información.

En razón de ello, la estructura del presente informe la hemos dividido en las siguientes secciones:

- 1.- Gerencia Central de Regulación y Planificación Estratégica
- 2.- Gerencia de Seguridad y Protección.
- 3.- Gerencia de Sistemas de Información.
- 4.- Gerencia de Facturación y Cobros.
- 5.- Gerencia Central de Red y Operaciones.
- 6.- Gerencia de Telefonía de Uso Público y Rural.
- 7.- Gerencia de Control y Soporte Comercial.
- 8.- Gerencia de Marketing.
- 9.- Gerencia de Larga Distancia
- 10.- Gerencia de Atención al Cliente
- 11.- Telefónica Servicios Comerciales
- 12.- Terra Networks Perú S.A.
- 13.- Telefónica Multimedia
- 14.- Teleatento del Perú S.A.C.

ANEXOS:

- 1.- Nueva Normativa Corporativa sobre el Derecho al Secreto de las Telecomunicaciones
- 2.- Presentación sobre las Medidas Adoptadas por Telefónica del Perú para salvaguardar el Secreto de las Telecomunicaciones.

CONFIDENCIAL

GERENCIA CENTRAL DE REGULACIÓN Y PLANIFICACIÓN ESTRATÉGICA

1.- Medidas adoptadas

En agosto de 1997, la entonces Vicepresidencia Ejecutiva Legal y Organismos Regulatorios, emitió la circular s/n sobre "Cumplimiento de medidas para salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos", la cual sigue vigente y es de aplicación en los respectivos negocios.

Con fecha 16 de enero de este año, la Presidencia Ejecutiva de nuestra empresa emitió la Nueva Normativa Corporativa sobre el Derecho al Secreto de las Telecomunicaciones, la misma que se encuentra vigente a partir de este año y que adjuntamos como anexo al presente documento.

Las referencias legales utilizadas para la elaboración de dicha normativa fueron las siguientes:

- Constitución Política del Perú – Art 2°, Inc. 10
- Código Penal, artículo 161°, 162°
- Decreto Supremo N° 013-93-TCC Art.4°, 87°
- Ley 27697 (Artículo 2°)
- Decreto Supremo N° 06-94-TCC, Art.10°
- Resolución Ministerial N° 622-96-MTC/15.17 Art. 4.1, Art 4.2.
- Contratos de concesión celebrados por Telefónica del Perú con el Estado Peruano sección 8.10.
- Ley de Funciones y Facultades de OSIPTEL - Ley 27336 (Artículo 8)
- Jurisprudencia nacional para la protección del secreto de las telecomunicaciones

Las medidas adoptadas por la empresa, también fueron hechas de conocimiento del MTC a través de una presentación realizada en nuestras oficinas. Adjuntamos copia de dicha presentación.

Durante el transcurso del año 2003, la Gerencia de Regulación y Planificación Estratégica se encargó de supervisar el cumplimiento de las medidas adoptadas.

2.- Personal Responsable

La Gerencia Central de Regulación y Planificación Estratégica es la encargada de coordinar la implementación, cumplimiento y supervisión de la salvaguarda del Secreto de las Telecomunicaciones y la Protección de Datos de nuestros clientes. El personal directamente responsable es el siguiente:

CARGO	NOMBRE Y APELLIDOS
Gerente Central	Jorge Melo - Vega Castro
Gerente	Hortencia Rozas Olivera
Gestor de Negocios	Flor Montalvan Davila

GERENCIA DE SEGURIDAD Y PROTECCIÓN

1.- Medidas adoptadas

Medidas Técnicas:

- Evaluaciones técnicas para verificación de riesgos potenciales de la información física en los diferentes negocios.
- Actividad de supervisión de destrucción de desechos de oficina en los principales locales del grupo Telefónica.

Asimismo se ha implementado el siguiente sistema:

El Sistema Inteligente de Seguridad (SIS)

Sistema de Tele Vigilancia electrónica a distancia, instalado en diferentes locales de la empresa a nivel nacional. La configuración electrónica de este sistema, permite controlar el flujo de movimiento de personal en ambientes restringidos, así como el control de daños a la planta y los bienes ubicados dentro de estos. Este sistema, está orientado al control de accesos del personal, así como a la seguridad electrónica, sin que se requiera la presencia permanente de personal.

Dentro de estos dispositivos, con el que cuenta el sistema tenemos:

- Un Centro de Recepción de Alarmas y Tele servicios (CRAT), en el año 2003, se ha actualizado el software de este sistema a fin de mejorar la gestión.
- Cámaras de CCTV, instaladas en lugares estratégicos; en el año 2003 se ha continuado con la instalación de estos sistemas en locales de la red fija.
- Asimismo, las áreas técnicas responsables tienen un terminal del mismo.
- Sensores de movimiento (PIRS), ubicados en lugares estratégicos.
- Sensores iónicos.
- Sensores térmicos.
- Sensores magnéticos.

Funcionalidad:

- Gestión remota y centralizada de alarmas.
- Telecontrol de sistemas de extinción de incendios y servicios técnicos.
- Control remoto del acceso de personal autorizado por las Áreas de las Empresas (Identificación visual, oral o electrónica).
- Vigilancia remota, mediante cámaras y sistemas de audio.
- Base de datos y aplicaciones que facilitan la gestión y explotación del sistema.

Medidas Organizativas:

Se cuenta con las normas y procedimientos siguientes:

- Norma "Clasificación y Tratamiento de la Información" (NOR-P-5002) cuyo alcance de cumplimiento es para todas las Unidades de Negocio del Grupo de

Telefónica en el Perú, la misma que permitirá conseguir niveles de uso equivalentes para la información con el mismo grado de sensibilidad para la gestión de los negocios en cualquiera de sus líneas de actividad.

- Normativa "Prevención del Espionaje Empresarial" (SS-008) orientadas a la detección oportuna de actividades relacionadas con el espionaje empresarial involucrando información clasificada de carácter estratégico para la empresa, así como los mecanismos necesarios para prevenir y contrarrestar dichas situaciones.
- Norma de Control de Accesos.
- Prevención del Espionaje Empresarial.
- Procedimiento de actuación para la atención de autorizaciones de acceso.
- Procedimiento de controlar el acceso de personal vinculado a medios de comunicación
- Procedimiento de actuación para el robo de cables aéreos y subterráneos.
- Control de ingreso y salida de personal de Centros de Cómputo.
- Cumplimiento del proceso de destrucción de desechos en las oficinas locales.

Medidas Humanas:

- Charlas de capacitación a los trabajadores de las distintas Unidades de Negocios del Grupo Telefónica en medidas para proteger su información.
- Actualización permanente de Base de Datos del Personal Crítico de los Negocios.
- Campaña de comunicación anual en medidas preventivas para proteger la información difundidas a través de los diversos medios de comunicación interna: afiches, sistema vantive, vía mail, boletin Segurinot@s.
- Empleo de los canales informáticos para la transmisión de mensajes por las PCs a los trabajadores de las Empresas.
- Empleo de los boletines de las Unidades de Negocios para difundir recomendaciones para la Protección de la Información.

Servicios de Seguridad

Dentro de los servicios de seguridad se encuentran la Vigilancia Privada, Guardianía y los Grupos de Reacción Móviles.

Vigilancia Privada

Instalada en locales principales y grandes centrales, con consignas precisas para el control de acceso autorizado por las áreas de las Empresas y atención de ocurrencias de seguridad física.

Así mismo, los puestos de vigilancia y Centros de Control cuentan con los procedimientos y la normativa interna vigente.

Grupo Móviles de Reacción

El grupo consiste de un vehículo y un supervisor de vigilancia que atiende las alarmas que reporte el SIS a nivel nacional se cuenta con 13 grupos de reacción a nivel nacional; el 50% dotado con personal policial para cualquier intervención de ser necesario.

Así mismo, estos grupos tienen funciones de patrullaje en la Planta Externa a fin de reducir los actos delictivos en contra de la misma.

CONFIDENCIAL

Sistema de Control de Accesos en Línea

Se cuenta con un sistema de Control de Accesos en Línea, donde las diferentes áreas de la Empresa gestionan y autorizan el ingreso del personal de trabajadores propios y de terceros a los diferentes locales de la Empresa.

Este sistema permite verificar en Lima si el personal que intenta ingresar a los locales, autorizado por las diferentes áreas, tiene o no algún impedimento para su ingreso.

Los sistemas implementados permiten efectuar el Control de Accesos, permitiendo únicamente el ingreso del personal autorizado por las áreas de las empresas.

2.- Personal Responsable

CARGO	NOMBRE
GERENTE DE SEGURIDAD Y PROTECCION	LUIS ENRIQUE CUEVA DIAZ

Luis Enrique Cueva Diaz - Gerente de Seguridad y Protección

CONFIDENCIAL

GERENCIA DE SISTEMAS DE INFORMACIÓN

1.- Medidas adoptadas

Normativa:

Se ha difundido a nivel corporativo la siguiente normativa, la cual establece las pautas a seguir para mantener un estado óptimo de la seguridad en los sistemas de información. Esta normativa para los sistemas de Telefónica comprende los siguientes rubros:

- Funciones y obligaciones del personal en materia de Seguridad de Información
- Clasificación y tratamiento de la información
- Identificación y autenticación
- Control de acceso a los sistemas de información
- Redes y comunicaciones
- Control de software
- Desarrollo de sistemas de información
- Registros de auditoría y monitorización
- Incidencias de seguridad
- Copias de respaldo y recuperación
- Planes de auditoría
- Seguridad integral en los Centros de Cómputo

La normativa indicada se encuentra publicada en la intranet de la compañía, para uso interno de los empleados de Telefónica.

Monitorización y revisiones de los Sistemas de Información:

Para mantener el control de los accesos en la red de ordenadores de Telefónica, los que pudieran afectar la confidencialidad de la información, se han implementado las siguientes medidas:

- Uso de herramientas para la detección de intrusos
- Revisiones periódicas de vulnerabilidades en los computadores y elementos de comunicación de la red corporativa
- Uso de herramientas de detección de cambios en los sistemas operativos de los sistemas de información corporativos
- Revisión y mantenimiento periódico de los niveles de acceso de los usuarios a los sistemas de información.
- Gestión de accesos centralizada, con procedimientos formalizados de creación, modificación y eliminación de accesos.

Medidas de Seguridad de Información en la Gerencia de Sistemas

- Cumplimiento de la normativa antes descrita mediante la implementación del Consejo de Arquitectura de la GSI, evaluación del Comité de Seguridad y pruebas a los programas efectuadas por el equipo de Testing, que evalúan el cumplimiento de los requisitos mínimos de las aplicaciones que ingresan a producción.
- Formación del grupo CRISIS para la evaluación técnica de problemas de seguridad en los sistemas de información, conformada por los especialistas de las áreas técnicas correspondientes.
- Establecimiento de un esquema de seguridad e implementación de herramientas de seguridad de información y auditoría a nivel de red (firewalls) y sistemas operativos.

Medidas de seguridad física en los Centros de Procesamiento de Datos CPD

Sistema Integral de Seguridad en los CPD, el cual incluye:

1. Sistema automático de extinción en incendios FM200.
2. Sistema de alarmas y sensores contra incendio, intrusión e inundación.
3. Sistema de Control de acceso, mediante huella digital, tarjetas de proximidad, esclusa de ingreso detectora de metales y de peso, y sistema de evacuación de emergencia con puertas de apertura y cierre automáticos (sistema antipánico)
4. Sistema de Vigilancia 7x24 externo e interno mediante circuito cerrado de TV, grabadoras VHS de eventos.
5. Sistema Integrador y Puesto de Control desde donde se monitorean los niveles de seguridad de los sistemas anteriormente descritos así como los sistemas secundarios de UPS, energía, aire acondicionado.
6. Procedimientos de control de acceso y operación de los sistemas de
7. seguridad bajo la supervisión de la Gerencia de Seguridad y Protección.

Contingencia: Se ha implantado un esquema de contingencia para los sistemas de información mediante el cual existe un CPD principal que alberga los actuales sistemas en producción y un CPD secundario, que alberga las plataformas alternas que se utilizarían en una eventual contingencia. Incluye un sistema automatizado (robot) de backup y sistemas de alta disponibilidad de discos.

Plan de Concientización de Seguridad de Información

Realización del Plan de Concientización de Seguridad de Información el mismo que está dirigido a todos los empleados y que considera:

- Distribución y difusión de las normas de seguridad de Información,
- mediante PANTALLAS de inicio de sesión y publicación en la intranet de la compañía para consulta de los empleados de Telefónica.
- Charlas específicas sobre seguridad en los sistemas para personal con puestos críticos, que incluye a ejecutivos, asistentes de gerencia-secretarías, personal de operadores y administradores de los sistemas y personal recién incorporado a la empresa.
- Distribución y difusión de Boletines de Seguridad de sistemas y encartes.
- Presentaciones a las Gerencias sobre Uso de Cuentas de Acceso, incluye:
 - Política para Atención de Solicitud de Acceso a los Sistemas Corporativos.
 - Normas de cuenta de usuario.
 - Recomendaciones para crear una buena clave-ejemplo de claves.
 - Como cambiar la clave de acceso en Windows NT -en Aplicaciones.
 - Cómo bloquear la PC.

- o Procedimiento para solicitar una cuenta de acceso en red-a los aplicativos.
- o Recomendaciones - protegerse de Virus - Conclusiones.
- o Donde reportar fallas.

2.- Personal Responsable

El personal responsable que tiene a su cargo la implementacion, cumplimiento y supervisión de las medidas y procedimientos adoptados para salvaguardar el secreto y la confidencialidad de la información, establece las funciones de los propietarios y de los custodios de la información, en base a la política de seguridad establecida.

CARGO	NOMBRE Y APELLIDOS
Sub Gerente de Proyectos	Fernando de los Ríos

El Sub Gerente es el responsable de la confidencialidad de la información contenida en los sistemas, siendo la persona autorizada para definir los accesos y niveles (perfiles) de acceso a las aplicaciones respectivas.

El personal de operadores y administradores de las aplicaciones tienen, por la naturaleza de sus funciones, acceso a los archivos de programas y de datos. Las medidas de seguridad implementadas con dicho personal son:

- El acceso de los operadores y administradores a los sistemas es con cuentas personales auditadas.
- Las cuentas de ADMINISTRADOR propietarias de los sistemas se encuentra en sobre cerrado lacrado y guardado en custodia del Centro de Cómputo. Existe procedimiento de control de uso de las cuentas de ADMINISTRADOR.
- La información confidencial de los abonados se encuentra encriptada a requerimiento de los negocios de Telefónica que así lo han dispuesto.
- En estos casos es accesible mediante opciones de la aplicación a las cuáles sólo tienen acceso personas que el negocio ha terminado.
- Igualmente, esas opciones tienen implementadas controles de auditoría.
- Los operadores principalmente no tienen acceso a estas opciones, en los que tiene el acceso la opción está auditada.

CONFIDENCIAL

GERENCIA DE FACTURACION Y COBROS

1.- Medidas adoptadas

Al igual que en la Gerencia de Sistemas, en la Gerencia de Facturación y Cobros se ha adoptado lo siguiente:

- Cada trabajador posee un "password" y contraseña personalizada, que le garantiza que la información que maneja y guarda en su PC para el cumplimiento de sus funciones, sólo podrá manejarla el usuario.
- Existe un procedimiento escrito y que se cumple fielmente, para guardar información de backup, bajo la modalidad de "Quemador de Discos".
- En el año 2003 la Gerencia, inició el dictado del Curso de Facturación y uno de los temas expuestos a personal de otras Gerencias, se trata sobre las medidas de seguridad que se debe mantener para salvaguardar la protección de datos y el secreto de las telecomunicaciones de nuestros clientes.
- Asimismo, se ha velado de que todo el personal de la Gerencia, cumpla con las medidas generales que Telefónica del Perú ha implantado en su responsabilidad de salvaguardar el "Secreto de las Telecomunicaciones y la Protección de Datos"; como son:
 - La Empresa como parte de las acciones de refuerzo a la difusión, educación y entrenamiento, ha elaborado el Manual "El Secreto de las Telecomunicaciones", al cual se puede acceder mediante la página Web "En Línea" que es un medio informativo de la Gerencia de Recursos Humanos, abierto a todo el personal que labora en la Empresa. Esta normativa interna, incluye acciones claras y procedimientos de seguridad, que se encuentran respaldados por el compromiso individual de sus miembros, en cada una de sus actuaciones profesionales.
 - La empresa a entregado a cada trabajador un documento escrito, en donde se le informa claramente cuáles son los deberes, compromisos y responsabilidades al respecto, indicándose que su incumplimiento será considerado y sancionado como falta grave con la consecuente pérdida del puesto de trabajo (se adjunta copia).
 - Se han adoptado medidas de seguridad física y lógica respecto a los locales, equipos, instalaciones, redes y medios informáticas, y bienes en general donde se custodia información vinculada a los datos protegidos para salvaguardar el secreto de la Telecomunicaciones; medidas que, para verificarlas y/o detallarlas sería conveniente una comprobación "in situ" en cualquier Área de nuestra Empresa.
 - La relación de personas responsables del área, que por la naturaleza de sus funciones tienen acceso a la Red Pública de Telecomunicaciones o información confidencial: Se ha designado a Wayer Osore Villagaray, cargo Supervisor.

2.- Personal Responsable

CARGO	NOMBRE Y APELLIDOS
Supervisor	Wayer Osore Villagaray

GERENCIA CENTRAL DE RED Y OPERACIONES

1.- Medidas adoptadas

Medidas de Seguridad Planta Interna y Externa

- Cámaras.- Se ha implementado el sistema de seguridad neumática en cámaras de registro y soldadura de tapas, asimismo algunos sistemas como: contratapas y tapas especiales con grava, a fin de lograr su inviolabilidad y la seguridad de los cables subterráneos.
- Armarios.- A la mayoría de estos equipos se les ha dotado de un sistema de Tele supervisión y Control que impide el acceso de extraños; el cual detecta cualquier manipuleo, su funcionalidad es vía red de ordenadores o red conmutada, concentrando su gestión y control en nuestro local de Surquillo.
- Elevación de armarios de pedestal a poste, a fin de evitar la accesibilidad a terceros. Implementación de sistemas adicionales de seguridad en los armarios como: sistema 3320, platinas y candado
- Tratamiento como áreas reservadas y restringidas todas aquellas donde se encuentran los equipos y sistemas de Telecomunicaciones, es decir los locales donde se encuentran ubicadas las centrales, medios de transmisión, repetidoras, etc. El acceso a estos locales es previa autorización de los responsables de la Gerencia Operación y Mantenimiento de Redes y Servicios (OMRS) según corresponda y en coordinación con la Gerencia de Seguridad.
- Asimismo el personal que tiene acceso a los Equipos y Sistemas de telecomunicaciones actúa y procede de acuerdo a las leyes vigentes y a la Constitución en lo referente al Secreto de las Telecomunicaciones.
- En todos los sistemas de telecomunicaciones de Conmutación, el acceso a los terminales de operación y mantenimiento se encuentra restringido sólo al personal autorizado. La restricción se realiza mediante el uso de passwords de acceso, los cuales se modifican quincenalmente.
- Como una medida de seguridad adicional al password de acceso a los terminales, se restringe los comandos de modificación de datos de central, definiendo perfiles de usuario de acuerdo a las actividades específicas de las áreas que interactúan con la central.
- A fin de controlar el ingreso y salida de personal a las salas de planta interna se cuenta con un procedimiento específico para el registro obligatorio en el Libro correspondiente, como una medida de seguridad dispuesta por la Gerencia de Operación y Mantenimiento de Redes y Servicios (OMRS).
- Planta Rural: El mantenimiento de la planta esta tercerizada a cargo de Alcatel; según contrato esta obligado a cumplir con el secreto de las telecomunicaciones.

Medidas de seguridad Física y lógica de locales, instalaciones, equipos y redes

- Edificios.- El acceso de personal propio y de subcontratas se efectúa con autorización de la Gerencia de Seguridad, mediante el Sistema de Autorización de Ingresos (CRAT), lo cual es verificado con el carné del trabajador o la copia de la autorización. Es obligatorio detallar las actividades que se van a realizar en el interior de los locales.
- Adicionalmente se tiene el Sistema Inteligente de Seguridad, que comprende la implementación de dispositivos electrónicos de seguridad inteligente en los locales de

Telefónica, tales como detectores de incendios, sensores de intrusión y cámaras de video (Tele vigilancia), ubicados en puntos estratégicos operando permanentemente las 24 horas del día.

- En nuestros locales técnicos de mayor relevancia se cuenta con cercos perimétricos y casetas de guardianía y/o vigilancia.
- Análisis e identificación permanente de sectores y elementos de planta críticos por probabilidad de sustracción de línea.
- Implementación de planes de mejoras de estética de red.
- Reubicación de terminales de fachada a poste y redireccionamiento de acometidas.
- Mejora continua en el proceso de instalación a fin de evitar en lo posible tender acometidas en azoteas (edificaciones carecen de infraestructura para instalaciones y cableados internos).
- Las labores de Supervisión, Operación y Mantenimiento Centralizado de la Planta de Conmutación se realizan a través de los terminales del Sistema de Observación de Centrales (SOC). El sistema SOC está implementado con una red que es independiente de la red corporativa de la empresa. Todas las transacciones realizadas desde estos terminales son registradas, indicando fecha, hora, usuario y acciones realizadas en una base de datos de la plataforma.
- Adicionalmente a las actividades ejecutadas centralizadamente a través del sistema SOC, en provincias se realizan labores de supervisión, operación y mantenimiento a través de terminales locales conectados directamente a las centrales telefónicas. Estos terminales, de manera similar al SOC, cuentan con sus respectivas claves de accesos, restricciones por perfiles de usuario y almacenamiento de todas las transacciones realizadas en la central.
- Periódicamente se realizan inspecciones técnicas a los diferentes nodos de conmutación. La finalidad de las Inspecciones Técnicas es asegurar el correcto funcionamiento de acceso y servicios de información nacional e internacional de Telefónica, así como la adecuada utilización de los recursos humanos y materiales, normas y procedimientos que se utilizan en la conservación de la planta técnica de conmutación telefónica y plataformas de servicios. Dentro del plan de Inspecciones Técnicas esta programado realizar visitas técnicas periódicas de supervisión a las oficinas de Lima y Zonales.

Medidas de seguridad de Tráfico

- Para efectuar las Mediciones de Tráfico se utiliza la Plataforma SGT (Sistema de Gestión de Tráfico) , y existen permisos de acceso con restricciones por perfiles de usuario (password).
- Registros de llamada CDRs (Fuente: Data Warehouse - DWH): Los usuarios son identificados, han firmado un compromiso de mantener la seguridad de la información, los accesos se realizan con el uso de su correspondiente clave de acceso.
- Tráfico Facturado (Fuente: SUT a través del módulo de Conciliación de OMRS): Los usuarios están identificados por el área de producción de Sistemas de Información, el manejo de la información se realiza exclusivamente para la elaboración de los cruces de datos y elaboración de los informes y se manejan permisos de acceso con password.
- Documentación correspondiente al Tráfico: Los informes de tráfico se entrega vía correo electrónico al jefe inmediato.

- Tráfico diario entrante y saliente en minutos, de los teléfonos de uso público del medio rural: Esta información es obtenida por la Gerencia TUP y Rural y remitida exclusivamente para preparar información requerida por el Osiptel, entre otros, de acuerdo al Reglamento de continuidad del servicio de los centros poblados rurales. Los usuarios están identificados y tienen el compromiso de mantener la seguridad de la información.

Medidas de seguridad en protección de Datos

El buen funcionamiento de estas medidas depende de la Gerencia de Seguridad y Protección; en su organización se encuentra la Jefatura Protección de la Información, la que tiene como objetivo atender todos los aspectos relativos a la protección física de las materias y documentos clasificados, que involucran al personal, transporte y transmisión de los mismos, incluyendo a la información que fluye por la red informática. Además cuenta con el Centro de Operaciones de Seguridad para el control de la planta externa.

Registro, atención y tramitación de reclamos de usuarios

Los reclamos que son ingresados a la Gerencia OMRS son atendidos a través de terminales cuya gestión y acceso se encuentra restringido sólo al personal autorizado. La restricción se realiza mediante el uso de passwords de acceso los cuales se modifican mensualmente.

Los reclamos de los arrendadores del servicio de telefonía de uso público de los centros poblados rurales se transfieren actualmente a la contrata que esta a cargo de la Planta Tercerizada, Alcatel, que contractualmente está obligada a salvaguardar el secreto de las telecomunicaciones. A partir del mes de marzo 04, directamente atenderemos dichos reclamos, cuyo tratamiento se hará con personal restringido, usando aplicativos con sus respectivos aditamentos de seguridad.

Medidas adoptadas para capacitar al personal de cada área acerca de su deber de salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos.

Los trabajadores de Telefónica una vez incorporados a la Empresa firman un compromiso de confidencialidad. Igualmente a los trabajadores nuevos se les da charlas de inducción relativas al sistema de seguridad de la Empresa y de las directivas pertinentes a la protección de información empresarial.

Normas y Comunicaciones

Relación de los documentos normativos establecidos para cumplir con la directiva N° 022-96-MT/15.17 del MTC: Procedimiento de inspección y de requerimiento de información en relación al secreto de las telecomunicaciones y la Protección de Datos:

- Medidas para salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos (TBI-I-002-Junio 96).
- Medidas de funciones en M.P.C. (Módulo de Pruebas Centralizadas) y M.D.F. (TB2-M-003- Julio 96). (Nota:MOF actualizado el proyecto se encuentra en proceso)
- Manual del Instalador Reparador de Líneas Telefónicas (GST-M-004-Septiembre 2001).
- Manual del Instalador Reparador de Líneas de Acometida de Televisión por Cable (GST-M-011 Septiembre 2001)
- Manual del Instalador Reparador de CableNet (GST-M-012 Diciembre 2001).
- Manual del Instalador Reparador del servicio líneas ADSL (GORAC-M-015 Diciembre 2003).

CONFIDENCIAL

- Instrucción Supervisión, Coordinación y Control a las Empresas Colaboradoras (GST- I -014 Junio 2001)
- Procedimiento para el Control de Penalización a Contratistas (TB2-P-003- Septiembre 96).
- Cartilla Operativa Reasignación de Facilidades Técnicas (GST-C-019 Octubre- 2002)
- Cartilla Operativa Confiabilidad de Facilidades Técnicas (GST- C-018 -Octubre 2002)
- Cartilla Operativa Asignación Manual por Excepción GST-C-014 -Octubre 2002)
- Procedimiento para Penalización a Contratistas por Cobros Indevidos (OMR2-P-009 - Junio 1997)
- Procedimiento para Control y Supervisión en la ejecución a contratistas de Ordenes de Servicio (OMR2-P-012-noviembre 97)
- Procedimientos para Pequeños Trabajos de Red (GST-P-006-Mayo 2001)
- Penalización a Contratistas por Cobros Indevidos y/o Malas Actuaciones en CATV (GST-P-032 - Octubre 2001)

Para salvaguardar la seguridad de la red pública se ha generado diversos documentos informativos para conocimiento de todas las jefaturas, los mismos que durante el año 2003 han sido difundidos por Intranet:

- Sabes Qué 017-99 (octubre 99) Robo de Cable
- Sabes Qué 004-01 (Mayo 01) Instalaciones Clandestinas y Penalidades CATV
- Sabes Qué 001-02 (Enero 02) Información confidencial que se presenta ante OSIPTEL
- Sabes Qué 016- 02 (Abril 02) Programación del Terminal Inalámbrico
- Sabes Qué 028-02 (Agosto 02) Servicios Especiales para uso del personal Técnico
- Sabes Qué 030-02 (Agosto 02) Identificación de Numeración de Bornes en el TAP pasivo de CATV para interiores.
- Sabes Qué 003-03 (Febrero 03) Identificación de TAPS direccionables en la red de CATV

2.- Personal responsable

Gerencia de Planificación

El personal de esta Gerencia ingresa a la Red Pública de Telecomunicaciones sólo para efectuar pruebas técnicas en las centrales

CARGO	NOMBRE Y APELLIDOS
Jefe Tecnologías de Conmutación	Isaac Palomino Navarro
Jefe Tecnologías de Transmisión	Mario Mendieta Mendieta

Gerencia de Operación y Mantenimiento de Redes de Acceso y Clientes (Gorac):

SUB GERENCIA OPERACIÓN DE REDES DE ACCESO Y CLIENTES LIMA

DEPENDENCIA	NOMBRES Y APELLIDOS	CARGO
Jefatura Operaciones Norte	Jorge Zúñiga Ordóñez	Jefe
Jefatura Operaciones Sur	Cesar Ávila Caro	Jefe

CONFIDENCIAL

Jefatura Operaciones Centro	Elmer Quesnay Díaz	Jefe
Jefatura Operaciones Oeste	Luis García Leveratto	Jefe
Jefatura Operaciones Este	Galo Cavalcanti Saldaña	Jefe
Jefatura Operaciones Centro Oeste	Alberto Tantaruna Medina	Jefe
Jefatura Operaciones Centro Este	Arturo Montenegro Ruiz	Jefe
Jefatura Operaciones CATV Lima	José Rodríguez Parra	Jefe
Jefatura Operaciones Lima-TUP	Carlos García Ferreyra	Jefe
Supervisión Gestión Permisos	Luis García Lazarte	Supervisor

SUB GERENCIA OPERACIÓN DE REDES DE ACCESO Y CLIENTES PROVINCIAS

DEPENDENCIA	NOMBRES Y APELLIDOS	CARGO
Jefatura Operaciones Piura	Jorge Chojeda Cruz	Jefe
Jefatura Operaciones Chiclayo	José Luis López Feliz	Jefe
Jefatura Operaciones Trujillo	Jesús Ramírez Ll	Jefe
Jefatura Operaciones Chimbote	Juan Zavaleta Coral	Jefe
Jefatura Operaciones Iquitos	Hugo Chacaltana Castillo	Jefe
Jefatura Operaciones Huancayo	Efraín Yauri Benites	Jefe
Supervisor Soporte Técnico Ica	Javier Dextre Quijandria	Jefe
Jefatura Operaciones Arequipa	Juan Salvatierra Chirinos	Jefe
Jefatura Operaciones Cusco	Edgar Gallegos Núñez	Jefe
Supervisor Soporte Técnico Tacna	Carlos Villegas Cuaresma	Jefe

SUB GERENCIA SOPORTE DE OPERACIÓN Y PROVISIÓN

DEPENDENCIA	NOMBRE Y APELLIDOS	CARGO
Jefatura Control de Gestión	Javier Quiroz Cárdenas	Jefe
Jefatura Normativa y Sistemas	Juliette Ferrier Hoyle	Jefe
Jefatura Provisión de Servicios	Emilio Gutiérrez Ibaceta	Jefe

SUB GERENCIA CONTROL DE REDES

DEPENDENCIA	NOMBRE Y APELLIDOS	CARGO
Jefatura Centro de Gestión Oper. Residencial	Samuel Rentería Calderón	Jefe
Jefatura Cent. De Gestión Oper. Otros Negocios	Rolando Hinojosa Saavedra	Jefe
Jefatura Asignación	Arturo Rosales Heredia	Jefe
Jefatura Oper.de FIB.OPT. y Calidad de Redes	Freddy Ortiz Magallanes	Jefe

SUB GERENCIA OPERACIÓN DE SERVICIOS ESPECIALES Y PROYECTOS

DEPENDENCIA	NOMBRE Y APELLIDOS	CARGO
Jefatura Operaciones de Cltes.VIP y Negocios	Alejandro Padrón Giraldo	Jefe
Jefatura Desarrollo de Proyectos	Eduardo Radas Aranda	Jefe
Jefatura Operaciones de Serv.Banda Ancha	Bernardo Castro Pulcha	Jefe

CONFIDENCIAL

GERENCIA DE TELEFONIA DE USO PUBLICO Y RURAL

1.- Medidas adoptadas

En la Gerencia Telefonía de Uso Público y Rural, se aplican las normas corporativas establecidas por las áreas competentes de Telefónica del Perú S.A.A., así como las medidas internas dispuestas por el negocio.

1.1. Normas corporativas

1.1.1 Elaboradas por la Gerencia de Seguridad y Protección, cuya finalidad es proteger la información empresarial y el patrimonio de Telefónica del Perú S.A.A., entre las cuales destacan las siguientes:

- SSP-007 "Norma de Control de Accesos"
- SSP-008 "Prevención del Espionaje Empresarial"
- SSP-023 "Prevención del Fraude"
- NOR-P-50002 "Clasificación y Tratamiento de la Información"

1.1.2 Elaboradas por la Gerencia de Sistemas de Información, cuya finalidad es proteger los sistemas operativos, redes e infraestructura de Telefónica del Perú S.A.A., entre las cuales destacan las siguientes:

- NOR-P-50001 "Funciones y Obligaciones en Materia de Seguridad"
- NOR-P-50003 "Identificación y Autenticación"
- NOR-P-50004 "Control de Accesos a los Sistemas de Información"

1.2 Medidas Internas del negocio

1.2.1 Con nuestro personal

- Se han emitido pautas y dictado charlas informativas respecto a la protección del "Secreto de las Telecomunicaciones" y "Confidencialidad de la información" de los abonados y usuarios de Telefónica del Perú S.A.A., así como información de todas las personas con las que se mantiene algún tipo de relación contractual.
- Existen procedimientos internos para el registro, atención y tramitación de los pedidos de insatisfacción que presenten nuestros arrendadores y/o usuarios del servicio, que garanticen la protección del "Secreto de las Telecomunicaciones". Al respecto, debemos precisar que esta información se encuentra registrado en los sistemas corporativos de Telefónica del Perú S.A.A., cuyo acceso se realiza de acuerdo con lo establecido en las normas "Identificación y Autenticación" y "Control de Accesos a los Sistemas de Información".
- En la atención de pedidos de insatisfacción de nuestros arrendadores, se tiene especial cuidado de no facilitar información o detalles completos de las llamadas realizadas desde los equipos terminales. Sólo cuando es preciso resolver alguna diferencia en la recaudación, se muestra un reporte sin incluir el número de destino.
- Las cartas, documentos y contratos pertenecientes al negocio, son almacenados en ambientes adecuados y seguros.

1.2.2 Con todas las personas que mantienen algún vínculo comercial con Telefónica del Perú S.A.A.

- En los contratos de arrendamiento para la prestación del servicio de telefonía pública en establecimientos, así como para la administración de Locutorio Público, se ha incluido una cláusula específica, sobre la protección del "Secreto de las Telecomunicaciones".
- En los contratos de prestación de servicios para la recaudación de teléfonos públicos de exterior (TPE); así como para la distribución y comercialización de los productos de telefonía pública y/o para la instalación, desmontaje y mantenimiento de líneas telefónicas y equipos terminales, se han establecido cláusulas similares a los contratos señalados en el punto anterior. Además, se ha establecido que la responsabilidad de estas empresas, comprende no sólo a sus trabajadores, sino también al personal de sus subcontratistas y/o terceros, de ser el caso.

1.3 Medidas Internas adoptadas para salvaguardar la seguridad de la Red Pública de Telecomunicaciones

Se viene implementado progresivamente un sistema de protección de líneas telefónicas (ALT), el cual permite un monitoreo permanente de las mismas, evitando que se realicen indebidamente llamadas telefónicas a través de algún mecanismo de fraude.

El centro de telesupervisión (SETM) permite monitorear en forma remota, la operatividad de los equipos terminales, cuya información es transferida automáticamente a los sistemas corporativos (Omega, Gestel, Fénix, entre otros). La transferencia de información del SETM se realiza de acuerdo con lo establecido en las normativas "Identificación y Autenticación" y "Control de Accesos a los Sistemas de Información".

2.- Personal Responsable

Gerente Telefonía de Uso Público y Rural	Andrés Castillo Pastor
Sub Gerente Comercial	Nélida Schrader Loechle
Sub Gerente Telesupervisión y Rurales	María Jesús Herrera Portuondo
Sub Gerente Planes y Proyectos Comerciales	José Antonio Cassinelli Sánchez
Sub Gerencia Comercial	Fernando Silva Chávez, Carlos Ponce Bezold, Juan Villafuerte Villanueva, Daniel Torpoco Carmen, Milagros Fernández Valle, Ana Gálvez Rojas, Gonzalo Fernández Aguilar
Sub Gerencia Telesupervisión y Rurales	Pilar Santa María, Enrique Wu Gondo, Miguel Díaz Sánchez, Alejandro Iglesias Ruiz-Huidobro
Sub Gerencia Planes y Proyectos Comerciales	Ramón Gonzáles Biffi, Leonardo Kuan Quiun, Ricardo León Venegas

GERENCIA DE CONTROL Y SOPORTE COMERCIAL

1. Medidas Adoptadas:

Información de tráfico

La información de tráfico fijo local voz, internet y Línea 147, es obtenida de los archivos fuente remitidos por Sistemas y es compartida con el personal responsable de las gerencias que por sus funciones la requieren:

- Gerencia Central de Control
- Gerencia de Telefonía de Uso Público
- Gerencia de Larga Distancia
- Gerencia de Banda Ancha
- Gerencia de Interconexión
- Gerencia de Contabilidad

Al respecto, se adoptan las siguientes medidas:

- Control estricto de claves de acceso de las PC's de los miembros de la gerencia encargados del procesamiento de archivos de tráfico. Todas las claves de acceso están bajo responsabilidad de los jefes, las mismas que son cambiadas cada 15 días.
- Minimización de carpetas compartidas de las PC's. Se ha establecido un mínimo de usuarios responsables por gerencia con acceso a la información de carpetas compartidas, según las necesidades de cada área.

Documentos y bases de datos que contengan la información referida anteriormente.

Se ejecutan las siguientes acciones:

- Depuración constante de los accesos al servidor, donde se consolida la información de tráfico local y los informes periódicos de la gerencia.
- Cumplimiento estricto de las normas sobre el aseguramiento de los documentos físicos no dejando ningún documento sin llave y eliminación de la papelería utilizada
- Generación de copias de respaldo de todas las bases de datos de tráfico.

2. Personal responsable:

CARGO	NOMBRE
GERENTE	FREDDY ACOSTA OCHOA

GERENCIA DE MARKETING

1. Medidas Adoptadas

En la Gerencia Marketing se aplican las medidas y procedimientos corporativos que han sido establecidos por diferentes áreas de la empresa. Paralelamente se aplican ciertas medidas internas particulares relacionadas con la operatividad propia del negocio.

a) **Sub Gerencia de Inteligencia Comercial** es el área encargada de convertir data en información para la toma de decisiones comerciales utilizando como modelo la cadena de valor de inteligencia de cliente. Considera el manejo de las bases de datos de los clientes, información de tráfico, facturación detallada, entre otros.

En esta área se han adoptado las siguientes medidas:

Medidas Humanas / Operativas

Exigencia y control de la campaña de "Escritorios Limpios y Seguros".

Se han establecido perfiles en los sistemas con la finalidad que los accesos a la información sean restringidos acorde con las exigencias de cada negocio.

La información de datos personales se ha restringido a tres (3) personas del área aprobadas por la subgerencia.

Los requerimientos de información confidencial deberán presentar un formato de solicitud, el mismo que deberá ser aprobado por el sub gerente para poder ser atendido.

Para los casos de pedidos recurrentes, el área solicitante deberá designar a una persona de contacto y se contará con las aprobaciones respectivas.

El sistema DWH mantiene restricciones a los usuarios de las Gerencias ajenas a Marketing. En general sólo tendrán acceso a la información del negocio al que correspondan.

Aún cuando el solicitante sea el negocio, el envío de base de datos a los canales (teleatención, imprenta u otros) es exclusividad del área.

b) **Jefatura de Investigación de Mercados** es el área dedicada al desarrollo de estudios de mercado que representan información primaria estratégica y táctica para la compañía.

Se tienen como elementos de información los siguientes entregables:

Documentos impresos

Archivos lógicos

Bases de datos utilizadas como input para la ejecución de trabajos.

Es este sentido se han tomado como medidas de seguridad las siguientes acciones:

Medidas Humanas / Operativas

Exigencia y control de la campaña de "Escritorios Limpios y Seguros".

El acceso a la información relacionada con los estudios de mercado está restringido totalmente a las personas del área.

La entrega de información resultante de estudios se deriva directamente a la persona responsable del negocio que solicita la información.

La información interna de gestión del área está restringida a 4 personas autorizadas por la jefatura.

Exigencias contractuales a los proveedores externos con cláusulas en las que se exige exclusividad.

Exigencias contractuales a los proveedores externos con cláusulas de confidencialidad en los entregables. Los entregables sólo pueden ser recibidos por la Jefatura de Investigación de Mercado. De existir una solicitud directa del negocio, la remisión debe ser de conocimiento de IDM y bajo su aprobación.

El estudio de mercado se remite sólo al negocio involucrado, salvo se vincule a otros o se trate de un estudio integral, en cuyo caso, deberá existir la autorización correspondiente.

CONFIDENCIAL

2. Personal responsable:

Gerencia Marketing	Marco Antonio Merino Montan
Sub Gerencia Inteligencia Comercial	Carlos Graham Sardi / Noemi Maeireizo Uku
Jefatura Investigación de Mercado	Silvia Chumpitaz Segovia

GERENCIA DE LARGA DISTANCIA

1. Medidas Adoptadas:

Las medidas y procedimientos para el control del secreto de las telecomunicaciones en lo correspondiente a Larga Distancia, son las que se aplican en la empresa, tales como:

1. Acceso con user y password a la red informática.
2. Acceso con user y password diferente para cada aplicativo de sistemas que tiene relación con Larga Distancia.
3. Los usuarios que acceden a los aplicativos informáticos no tienen acceso a dispositivos magnéticos donde puedan grabar información; esto según la política de seguridad definida por la Gerencia de Sistemas de Información.
4. Existe un control de personal al ingreso y salida al centro de labores, donde se verifica lo que llevan consigo.

Se accede a los datos de los usuarios por motivos de identificación del cliente, segmentación de los mismos, ventas directas, atención de reclamos, etc. En tal sentido, el personal que tiene contactos con los clientes y sus datos; son prácticamente todas las personas que trabajan en las áreas de Servicio al Cliente y Ventas de Larga Distancia.

Respecto al tema del Tráfico Facturado, Detalle de Llamadas e Información de Abonados, se dispone de un Sistema donde se resguarda información según requerimiento de OSIPTEL para la administración de auditorías. Los módulos incluyen básicamente información de abonados, tráfico facturado y tráfico de Tarjetas Prepago. Las medidas de seguridad implican las siguientes premisas :

Acceso restringido a la información según perfiles respectivos tanto para el Regulador como usuarios de OTF
Manejo encriptado de Folios de Tarjetas HolaPerú.

2. Personal Responsable:

CARGO	NOMBRE
JEFE	JOSE LAREDO GOMEZ

GERENCIA DE ATENCION AL CLIENTE

1. Medidas Adoptadas:

Normativa del Secreto de las Telecomunicaciones

Objetivo

Dar las pautas necesarias para garantizar la seguridad de la Información que está a disposición del personal de la Sub Gerencia Gestión de Reclamos y que es propiedad del cliente, cumpliendo con el Secreto de las Telecomunicaciones.

Alcance

Todo el personal de la Sub Gerencia Gestión de Reclamos.

Definiciones

Se atenta contra la inviolabilidad y el Secreto de las Telecomunicaciones cuando deliberadamente una persona que no es quien cursa la comunicación ni es el destinatario, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, utiliza, trata de conocer o facilitar que él mismo u otra persona conozca la existencia o el contenido de cualquier comunicación cursada a través de las redes de telecomunicaciones, así como de los documentos privados, bases de datos y otros instrumentos que contengan información de carácter personal que obtenga de sus abonados y usuarios en el curso de sus operaciones comerciales.

Se considera como información sujeta a resguardo:

- El contenido de cualquier comunicación, de voz o de datos, cursado a través de cualquiera de las redes telefónicas, electrónicas y otros que la tecnología permita.
- El origen, destino, realización, curso o duración de una comunicación.
- La información del tráfico (detalle de llamadas).
- Los datos codificados y decodificados de los registros de las llamadas.
- Los medios de soporte material o magnético que porta o transmite la comunicación.
- Documentos y bases de datos que contengan la información referida anteriormente.
- Información correspondiente a facturación detallada.
- Información sobre la titularidad de una línea telefónica, con excepción de aquellas líneas cuya titularidad sea de conocimiento público de acuerdo con el ordenamiento legal vigente.
- Información sobre los planes contratados, preferencias comerciales y consumos efectuados por los clientes.
- Otros instrumentos que registren comunicaciones.

Esta información está contenida en:

- Expedientes de reclamos.
- Constancias de reclamos.
- Recibos Telefónicos.

- Contratos.
- Boleta de venta de equipos.
- Grabaciones.
- Inspecciones Técnicas.
- Detalle de llamadas.
- Sistemas
- Otros Medios de Prueba.

Responsabilidades

Todo el personal de la Sub Gerencia Gestión de Reclamos tiene la obligación de resguardar la información a la que tiene acceso para realizar sus labores.

Consideraciones

Se atenta contra el resguardo de la información personal relativa a los clientes o usuarios cuando ésta es entregada, mostrada o comentada a terceros sin el consentimiento previo, expreso y por escrito del abonado o usuario y demás partes involucradas o sin una orden judicial específica motivada del Juez con las garantías previstas en la ley.

No está permitido retirar ningún documento incluido en el punto 4.2, fuera de la empresa.

Se deberá dejar los documentos antes mencionados en lugares seguros, fuera del alcance de terceras personas que puedan dar un mal uso a la información contenida en dichos documentos.

Para el caso del papel reciclado, se deberá cumplir con lo establecido por la Normativa para el reciclado de papeles.

Con respecto a los Password personales se deberá cumplir lo establecido en la Normativa para el Uso de Password N-GR-G-003-04.

Se deberá llevar a cabo trimestralmente, capacitaciones o reforzamientos al personal, acerca del cumplimiento de esta normativa.

Como parte de las Auditorias Internas y para controlar el cumplimiento de esta Normativa, se realizarán Verificaciones mensuales en las distintas áreas de la Sub Gerencia mediante la Lista de Verificación que se adjunta como anexo.

Registros

Lista de Verificación del cumplimiento del Secreto de las Telecomunicaciones.

2. Personal Responsable:

CARGO	NOMBRE
SUPERVISOR	PATRICIA ORTIZ DE ORUE
SUPERVISOR	EDY CÉSPEDES LIVIA
SUPERVISOR	IVAN SILDARRIAGA ACOSTA

TELEFONICA SERVICIOS COMERCIALES

1. Medidas Adoptadas:

- Nuestro Reglamento Interno de Trabajo establece la obligación que tiene el trabajador de guardar total reserva de la información que maneja, así como la prohibición de difundirla.
- Nuestro personal ha sido instruido sobre la restricción en el uso y divulgación de la información y/o documentación de uso interno, especialmente la considerada como confidencial.
- Se realizan capacitaciones periódicas sobre la protección de la información de la empresa y el Secreto de las Telecomunicaciones.
- Nuestros ambientes y archivos han sido acondicionados con dispositivos de seguridad.
- En los Multicentros se han implementado medidas de seguridad para resguardar las instalaciones y equipos informáticos, con el compromiso permanente del personal de vigilancia y asesores comerciales.
- Se han establecido procedimientos para casos de cese de personal en multicentros, con la restricción en el ingreso a los locales de la empresa y la cancelación de los accesos a los sistemas informáticos (Legacies, base de datos, correo electrónico, etc.)
- Hemos establecido limitaciones en el uso de las PC's tales como acceso limitado a correo externo, internet, disketeras y otros.
- Estamos en constante revisión de nuestras operaciones y procesos, dentro de un esquema de mejora continua a fin de garantizar el cumplimiento de las normativas vigentes.

2. Personal responsable:

CARGO	NOMBRE
GERENTE	JAIMÉ RIVERO AGUILAR

TERRA NETWORKS PERÚ S.A.

1. Relación y Contenido de las Medidas y procedimientos establecidos para salvaguardar el Secreto de las Telecomunicaciones

- 1.1 Almacenamiento del contenido de los correos electrónicos de nuestros abonados en servidores alojados en el Centro de Procesamiento de datos de TERRA, el mismo que se encuentra ubicado en un local de propiedad de Telefónica del Perú S.A.A, contando de ese modo nuestras instalaciones y equipos con adecuada seguridad y protección. Adicionalmente, se han implementado en nuestros servidores y equipos las medidas de seguridad lógica que permitan proteger el secreto de las telecomunicaciones, medidas tales como la utilización de "firewalls" e "IDS's" ("Intrusion Detection Systems"), así como la aplicación de reglas de seguridad que impiden o restringen el acceso a nuestros servidores de correo electrónico).
- 1.2 Protección del contenido de los mensajes de correo electrónico cursados por nuestros abonados mediante el uso de un nombre de usuario y una clave personal de acceso (contraseña), los cuales son conocidos única y exclusivamente por el titular de cada cuenta de correo electrónico.
- 1.3 Ningún acceso o conexión a Internet, ni el intercambio de correos electrónicos que es efectuado por nuestros abonados, son monitoreados por TERRA, con lo cual se garantiza la total confidencialidad de las comunicaciones cursadas por nuestros abonados.

2. Relación y contenido de las medidas y procedimientos establecidos para mantener la Confidencialidad de la Información Personal de nuestros Abonados.

- 2.1 Acceso restringido (tanto físico como lógico) a los servidores que alojan la Base de Datos de los abonados a los servicios de TERRA, así como a los documentos, soportes físicos, equipos y programas informáticos que contienen información personal de nuestros abonados o que permiten acceder a la misma. Dichos equipos y documentos son almacenados en locales administrados y gestionados o bien por TERRA o bien por Telefónica del Perú S.A.A., con lo cual las medidas de seguridad proporcionadas a los mismos están garantizadas.
- 2.2 Múltiples niveles de control en el acceso a la información de los abonados, debidamente adecuados a las necesidades de atención que requiera el puesto (restricciones en el acceso a la información personal de nuestros abonados).
- 2.3 En lo que se refiere a la atención de los casos en los que un abonado manifiesta haber olvidado su clave de acceso o contraseña, o ante la solicitud de alguna modificación a la misma, el abonado deberá presentar la documentación que acredite su identidad y -de ser el caso- su representación, así como una solicitud formal para el cambio de sus parámetros (esta solicitud es convenientemente archivada por el personal del Centro de Atención al Usuario de TERRA).
- 2.4 Adecuada selección y constante capacitación del personal encargado de la recepción, registro, tramitación y solución de reclamos de nuestros abonados vinculados con la prestación de los servicios públicos de telecomunicaciones por parte de TERRA. Ello posibilita un mejor control de la información personal de nuestros abonados.

3. Dependencias y personal a cargo de la implementación, cumplimiento y supervisión de las medidas y procedimientos a que se hace referencia en los apartados 1 y 2.

- 3.1 Centro de Atención al Usuario
- César Vásquez Temoche (Gerente)
 - Ivannova Lingán Cubas (Supervisora)
 - Evelin Bellido Carrillo (Administradora de Canales de Venta)

CONFIDENCIAL

- Nicole Mouchard Infantes (Analista)
- Jimena Colmenares da Ponte (Técnico)

- 3.2 Área de Operaciones
- Esteban Tapia Chang (Gerente)
- Lucero Auris Rodríguez (Analista Administrador de Base de Datos y Sistemas de Gestión)

TELFÓNICA MULTIMEDIA S.A.C.

1. Medidas Adoptadas:

Las medidas y procedimientos de seguridad para salvaguardar la confidencialidad de la información personal de los usuarios y el secreto de las telecomunicaciones en nuestra empresa; está implementada de acuerdo a las normas corporativas establecidas.

2. Personal responsable:

CARGO	NOMBRE
JEFE DE ASUNTOS LEGALES Y REGULATORIOS	MAITE VIZCARRA ALARCON

CONFIDENCIAL

TELEATENTO DEL PERÚ S.A.C.

1. Medidas Adoptadas:

Procedimiento para salvaguardar el secreto de las Telecomunicaciones y protección de datos en Atento Perú

1. Recursos Humanos : Contratos y Reglamento de trabajo:
 - El contrato de trabajo que se suscribe con Atento establece (cláusula décima) la obligación del trabajador de guardar reserva sobre la información a la cual tiene acceso y determina las sanciones por violar el secreto a la información.
 - El Reglamento Interno de Trabajo establece la obligación de todos y cada uno de los trabajadores respecto de observar en todo momento el secreto profesional y absoluta discreción en todo lo concerniente a la actividad de la empresa.
 - El Reglamento interno de trabajo es específico sobre seguridad de la información; establece que toda información residente en computadoras que sea sensible, crítica o valiosa tiene controles de acceso para protegerlos de modificaciones, eliminaciones o accesos inapropiados. Es responsabilidad del usuario la confidencialidad de la contraseña de acceso.
 - En el programa de inducción para nuevo personal operador que ingresa a la empresa, se incluye el tema "El secreto de las Telecomunicaciones, Resolución Ministerial N°622-96 MTC/15.17", publicada el 27 de noviembre de 1996 en el Diario Oficial El Peruano"
 - A través del manual de organización se establecen los perfiles de cada puesto y se define una clara comprensión de las funciones y responsabilidades de la comunicación jerárquica.
 - Existen procedimientos de comunicación inmediata a seguridad física e informática de las bajas de personal, para establecer los controles de acceso físico necesario y generar la baja en el sistema.
 - Toda persona que ingresa a la empresa se encuentra debidamente identificada.

2. Operaciones: Control de servicios

- El personal operador no tiene acceso a grabar o guardar información en los puestos de atención. Todos los puestos de operador tienen inhabilitadas las disketeras o no tienen disketera, como medida de seguridad.
- El personal operador que atiende las llamadas de los usuarios no tiene como procedimiento tomar nota de la información, salvo que expresamente se lo solicite los responsables del servicio.
- Toda documentación con información confidencial de Atento, es destruida, este tipo de documentos no es reciclado.
- El personal supervisor y operador es instruido respecto de las cuentas de usuarios, que son estrictamente personales.
- Los procedimientos de servicio establecen que los supervisores deben asegurar que diariamente las PC sean apagada por el personal al final de su jornada, salvaguardando la información de cada campaña.
- El personal que tiene acceso a correo, servidores, tiene la responsabilidad de bloquear las estaciones de trabajo mientras no haga uso de ella.
- La documentación importante de los servicios se archiva en armarios con llave.
- Se ha restringido en todas las posiciones el acceso a Internet, salvo aquellos en los que por el tipo de servicio que gestionan requieren de esta facilidad, pero aún así se les ha restringido a las páginas a las que deben acceder.

- Al terminar la jornada todos los puestos administrativos y de Supervisión quedan bloqueados.
- Sólo se proporciona información a clientes/usuarios con la debida autorización de los responsables y niveles superiores correspondientes.
- En previsión a la distorsión de información solo se atienden solicitudes previa formulación vía correo electrónico.
- En caso de detectarse algún caso de falta al Secreto de las Telecomunicaciones el personal involucrado es separado del servicio y se le aplica el reglamento respectivo.

3. Infraestructura y Equipos: seguridad de red

- La red de servidores de la plataforma de servicios de ATENTO está aislada; forma parte de una intranet particular con numeración IP diferente a la red administrativa y de operadores.
- El ingreso a la sala de soporte está solamente autorizado para los integrantes del área de soporte y mantenimiento; el control de acceso por código de barras está activado en forma positiva sólo para personal del área.
- Las salas de equipos se encuentra monitoreada con dos cámaras de circuito cerrado de TV; el monitoreo es permanentemente por personal de seguridad, para resguardar la integridad de los componentes internos.
- Los terminales de plataforma solo permiten el acceso del personal que labora en dicha área. La misma seguridad se encuentra implementada con los equipos de comunicaciones.
- Las grabaciones de voz realizadas en los sistemas de grabación de Atento están protegidas en un servidor con las respectivas claves de acceso. Los backups de dichas grabaciones están guardados en armarios dentro de la Sala Técnica a la cual sólo tiene acceso personal que labora en dicha área.
- Los registros de llamadas están protegidos dentro de los servidores con las respectivas claves de acceso. Los backups de dichos registros están guardados en armarios dentro de la sala técnica, a la cual sólo tiene acceso personal que labora en dicha área.
- Los registros de llamadas se encuentran codificados en formato binario, el cual requiere de un traductor y conocer su estructura; éstos sólo son conocidos por personal que labora en el área.
- Los registros de llamadas se almacenan en medio magnético (Tape Backup, DVD)
- Los procedimientos de almacenamiento están basados en función a las políticas de seguridad de Atento.
- El Comité de Seguridad de Atento realiza capacitaciones periódicas difundiendo las políticas de seguridad y normas de seguridad orientadas a salvaguardar el secreto de las telecomunicaciones.
- Atento Perú cuenta con un sistema de control de acceso a cada uno de los ambientes de la empresa (sistema de circuito cerrado en áreas claves) monitorizado por personal de seguridad las 24 horas del día y los 365 días del año.
- Las claves de los servidores de Atento son cambiadas cada mes, y éstas son de conocimiento exclusivo del personal administrador de los sistemas.
- Periódicamente se realizan verificaciones del uso de las carpetas compartidas para minimizar el uso.

CONFIDENCIAL

2. Personal Responsible:

CARGO	NOMBRE
GERENTE DE RECURSOS HUMANOS	JOSE ANTONIO IYO VALDIVIA
GERENTE CENTRO CONTACTO CAMANA	VIOLETA FERNANDEZ SERNA
GERENTE CENTRO CONTACTO NARANJAL	ERIKA FERNANDEZ INFANTE
GERENTE DE INFRAESTRUCTURA Y TECNOLOGIA	CESAR MELLADO HURTADO
JEFE DE ASEGURAMIENTO DE CALIDAD	JENNY LESCANO ACOSTA

CONFIDENCIAL

ANEXOS

CONFIDENCIAL

Grupo Telefónica en el Perú

**Normativa Corporativa sobre el
Derecho al Secreto de las Telecomunicaciones**

Lima, 16 de enero del 2004

CONFIDENCIAL

I. Objeto de la normativa

El objeto de la presente normativa es establecer las reglas que todas las empresas constituidas en el Perú que se encuentren, directa o indirectamente, bajo el control de Telefónica, S.A. (Empresas del Grupo Telefónica), deben observar en resguardo al derecho al secreto de las telecomunicaciones. Asimismo, dichas empresas deberán exigir su cumplimiento a los terceros contratados o colaboradores (en adelante los Obligados).¹

II. Definición de secreto de las telecomunicaciones

Para propósitos de esta normativa, se entiende por secreto de las telecomunicaciones lo siguiente (en adelante Secreto de las Telecomunicaciones):

Obligación de carácter constitucional en virtud de la cual las Empresas del Grupo Telefónica se encuentran obligadas a proteger la inviolabilidad de las comunicaciones¹ que se cursen a través de sus redes de telecomunicaciones, así como de los documentos privados, bases de datos y otros instrumentos que contengan información de carácter personal que obtenga de sus abonados y usuarios en el curso de sus operaciones comerciales. Se encuentra comprendida dentro de esta definición:

- El contenido de cualquier comunicación, de voz o de datos, cursado a través de cualquiera de las redes telefónicas, electrónicas y otros que la tecnología permita.
- El origen, destino, realización, curso o duración de una comunicación.
- La información del tráfico.
- Los datos codificados y decodificados de los registros de las llamadas.
- Los medios de soporte material o magnético que porta o transmite la comunicación.
- Documentos y bases de datos que contengan la información referida anteriormente.
- La información correspondiente a la facturación detallada.
- La información sobre la titularidad de una línea telefónica, con excepción de aquellas líneas cuya titularidad sea de conocimiento público de acuerdo con el ordenamiento legal vigente.
- Otros instrumentos que registren comunicaciones.

En cumplimiento de esta normativa, las empresas del Grupo Telefónica y los Obligados se encuentran impedidos de intervenir, interceptar, desviar, sustraer, interferir, cambiar, alterar, publicar, tratar de conocer o facilitar que un tercero intervenga, intercepte, desvíe, sustraiga, interfiera, cambie, altere, publique o trate de conocer la existencia o el contenido de cualquier comunicación o de los medios que lo soportan o transmiten.

¹ Se entiende por comunicación a cualquier forma de transmisión del contenido del pensamiento o de una forma objetivada de éste. (Artículo 2 de la Ley 27697)

III. Aspectos generales

- A. Las Empresas del Grupo Telefónica se encuentran obligadas a proteger el derecho al Secreto de las Telecomunicaciones conforme a los lineamientos establecidos en la presente normativa.
- B. Los gerentes generales y demás gerentes de las Empresas del Grupo Telefónica velarán por el efectivo cumplimiento de la presente normativa.
- C. Los gerentes generales y demás gerentes de las Empresas del Grupo Telefónica deberán informar a todo el personal que labore en sus respectivas empresas o áreas la obligación de proteger el Secreto de las Telecomunicaciones, responsabilizándose de que dicho personal tome conocimiento de la presente normativa, así como de aquellas normativas que correspondan al resguardo de la seguridad de la información en general.
- D. Las personas naturales o jurídicas que presten servicios a las Empresas del Grupo Telefónica y que por la naturaleza de los servicios que brindan deban acceder a información protegida por el Secreto de las Telecomunicaciones deberán ser informados de esta normativa y comprometerse a respetarla.
- E. En concordancia con la definición del acápite II anterior, todo el personal que labora en las Empresas del Grupo Telefónica y los terceros a que se hace referencia en el literal anterior se encuentran absolutamente prohibidos de entregar o revelar a terceros la información protegida por el Secreto de las Telecomunicaciones.
- F. Si en el transcurso de sus actividades los directivos, funcionarios y/o empleados de las empresas encontraran alguna duda sobre la definición del Secreto de las Telecomunicaciones o su aplicación, dichas personas se encuentran obligadas a consultar su alcance a la Secretaría General de Telefónica del Perú S.A.A.. La Gerencia Central de Regulación y Secretaría General mantendrán actualizada la presente normativa.
- G. Todas las áreas de la empresa (directivos, funcionarios y empleados) se encuentran obligados a evaluar permanentemente el riesgo en el manejo de la información protegida por el secreto de las telecomunicaciones. Esta evaluación deberá realizarse respecto de los procesos, sistemas, ambientes, equipos, actuales y futuros. Cada área establecerá el procedimiento dentro de ámbito de resguardo del secreto de las telecomunicaciones.
- H. Todas las áreas de la Empresa (directivos, funcionarios y empleados) deberán tomar conocimiento, cumplir y hacer cumplir, obligatoriamente, las normas de protección y seguridad de la información que se emitan, así como la legislación referida a la protección del Secreto de las Telecomunicaciones y la confidencialidad de la información de los usuarios.

IV. Aspectos laborales

La Gerencia de Recursos Humanos de las Empresas del Grupo Telefónica deberá entregar a toda persona que ingrese a laborar en alguna de las Empresas del Grupo Telefónica (tanto trabajadores de la propia empresa como locadores o terceros contratados) un ejemplar de la presente normativa, debiendo mantener en sus archivos una declaración en el sentido

CONFIDENCIAL

de que cada persona ha revisado, conoce el contenido de la misma y se obliga a respetarla.

- A. Los contratos de trabajo escritos que se celebren con personal de las Empresas del Grupo Telefónica, así como con locadores o terceros contratados, deberán contener cláusulas que obliguen a los trabajadores a proteger el secreto de las telecomunicaciones en los términos de las normativas vigentes.

La Gerencia de Recursos Humanos de cada Empresa del Grupo Telefónica deberá supervisar el cumplimiento de esta obligación.

- B. El incumplimiento de la normativa del secreto de las telecomunicaciones será considerado como falta grave laboral y será sancionado con la medida disciplinaria que corresponda de acuerdo a lo establecido en el Reglamento Interno de Trabajo, sin perjuicio de otras responsabilidades a que hubiera lugar y de la facultad de la empresa de iniciar las acciones legales que estime pertinentes.
- C. Es obligación de las diferentes Gerencias de las empresas del Grupo Telefónica supervisar y controlar el cumplimiento del servicio de los locadores, definir y establecer procesos periódicos de control orientados a prevenir infracciones sobre el secreto de las telecomunicaciones.

V. Obligaciones regulatorias

Las Empresas del Grupo Telefónica que ofrecen servicios de telecomunicaciones se encuentran obligadas a brindar al OSIPTEL y al Ministerio de Transportes y Comunicaciones todas las facilidades necesarias para que éstos cumplan con sus funciones de inspección y verificación permitiendo, entre otros, las visitas a sus locales, instalaciones y revisión de equipos y documentos vinculados con el objeto de la inspección, siempre que fuera necesario, previa coordinación con la Gerencia Central de Regulación Corporativa.

Del mismo modo están obligadas a proporcionar la información que requieran respecto de materias de su competencia, en la forma y plazos establecidos y mantener registros detallados de sus operaciones que permitan auditar eficientemente los montos cobrados a los usuarios por los servicios. Dichos registros serán puestos a disposición de los reguladores, previo requerimiento y coordinación con la Gerencia Central de Regulación Corporativa, salvaguardándose el secreto de las telecomunicaciones.

Existe la obligación de las Empresas del Grupo Telefónica de salvaguardar el secreto de las telecomunicaciones y mantener la confidencialidad de la información personal relativa a usuarios, atendida en el curso de sus negocios, así como informar a los reguladores, las medidas y procedimientos establecidos a más tardar el 15 de febrero de cada año. Esta información se brindará a través de la Gerencia Central de Regulación Corporativa.

Las excepciones al deber de salvaguarda son: (i) el consentimiento previo, expreso y por escrito del usuario y demás partes involucradas, o (ii) una orden judicial específica.

CONFIDENCIAL

Cada Gerencia de Regulación de las Empresas del Grupo Telefónica será encargada de solicitar y consolidar la información sobre el secreto de todas las áreas, a efectos de su envío al MTC, el 15 de febrero de cada año. La Gerencia de Regulación de cada una de las empresas del Grupo Telefónica, será encargada de solicitar la información correspondiente, oportunamente a su negocio y remitirla a la Gerencia Central de Regulación Corporativa, a más tardar el 30 de enero de cada año.

VI. Aspectos de seguridad

Las Gerencias de Seguridad y de Sistemas de Información de las Empresas del Grupo Telefónica deberán supervisar que la adopción de medidas de seguridad física y lógica implementadas por las áreas de las Empresas del Grupo Telefónica respecto de los locales, equipos, instalaciones, redes informáticas y bienes en general en los que se custodie información vinculada con el secreto de las telecomunicaciones sean las más adecuadas y efectivas para dicho resguardo, y designarán un responsable por cada las Empresa del Grupo Telefónica.

El día 15 de febrero de cada año, la Gerencia de Regulación deberá remitir al Ministerio de Transportes y Comunicaciones, un Informe Anual sobre medidas y procedimientos para salvaguardar el secreto de las telecomunicaciones y confidencialidad de la información personal de los usuarios de los servicios públicos de telecomunicaciones (en adelante, el Informe), para lo que deberá consolidar la información que cada área del Grupo Telefónica le remita a más tardar el día 30 de enero de cada año.

Sobre la base de dicho Informe las Gerencias de Regulación de las Empresas del Grupo Telefónica revisarán la necesidad de implementar nuevas medidas o de reforzar las ya existentes.

De ser necesario, las Gerencias de Seguridad y de Sistemas de Información de las Empresas del Grupo Telefónica emitirán normativas especiales para el resguardo de la seguridad de la información en general, cuidando de hacer especial énfasis en medidas para el resguardo de la confidencialidad e inviolabilidad del secreto de las telecomunicaciones, debiendo los Gerentes Generales y Gerentes de las Empresas del Grupo Telefónica asegurarse de su implementación y cumplimiento obligatorio dentro de sus respectivas organizaciones.

VII. Resguardo de la infraestructura de red

La Gerencia Central de Red de Telefónica del Perú o equivalentes de las demás empresas del Grupo Telefónica establecerán las medidas pertinentes para el resguardo de la planta externa e interna en todos aquellos componentes físicos y lógicos, de la planta interna y externa, que de una u otra manera pudieran facilitar la violación del secreto de las telecomunicaciones o el acceso a datos protegidos.

Para tal caso podrán contar con la asesoría de las áreas correspondientes.

CONFIDENCIAL

VIII. Resguardo de los Sistemas y Bases de Datos

Las Gerencias de Facturación, Sistemas, Centros de Cobro, Soporte Comercial y Atención al Cliente de Telefónica del Perú o sus equivalentes de las demás Empresas del Grupo Telefónica, establecerán las medidas pertinentes para proteger la seguridad de los medios informáticos, bases de datos, conexiones de red, de computadoras y otros medios electrónicos en sus componentes de hardware y software que de una u otra manera pudieran facilitar la violación del secreto de las telecomunicaciones o el acceso a datos protegidos.

IX. Aspectos contractuales

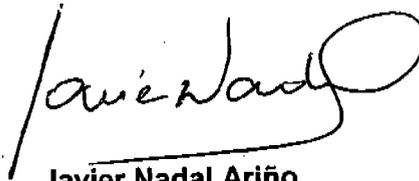
Los contratos que se celebren con personas jurídicas o naturales que por su naturaleza impliquen acceso a información que deba ser protegida en virtud del secreto de las telecomunicaciones, deberán contener cláusulas que obliguen a dichas personas a proteger la información, y que les hagan responsables frente a las Empresas del Grupo Telefónica, por cualquier daño que el incumplimiento genere.

X. Vigencia

La presente normativa deroga las normativas anteriores y particulares de cada Empresa del Grupo Telefónica sobre funciones y obligaciones del personal en materia de resguardo del secreto de las telecomunicaciones, salvo la norma de atención de requerimientos de información de autoridades públicas, aprobada en Comité de Dirección de Telefónica del Perú S.A.A. de fecha 27 de julio 2001.

La presente normativa entra en vigor a partir del día de su aprobación.

Aprobado en la ciudad de Lima a los 16 días del mes de enero de 2004.



Javier Nadal Ariño
Presidente



Jorge Melo-Vega Castro
Gerente Central de Regulación y
Planificación Estratégica



Julia María Morales Valentín
Secretaria General

CONFIDENCIAL

ANEXO

Fundamentos legales para la protección del secreto de las telecomunicaciones

Todo el personal que labora en las Empresas del Grupo Telefónica debe conocer que las empresas que operan en el sector de las telecomunicaciones están obligadas a preservar el secreto de las telecomunicaciones de conformidad con las siguientes normas legales:

A. Constitución Política del Perú

"Artículo 2.- Toda persona tiene derecho (...)

Inciso 10: Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados.

Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen (...)"

B. Artículos 161 y 162 del Código Penal

VIOLACIÓN DE LA CORRESPONDENCIA

"Artículo 161°.- El que abre, indebidamente, una carta, un pliego, telegrama, radiograma, despacho telefónico u otro documento de naturaleza análoga, que no le esté dirigido, o se apodera indebidamente de alguno de estos documentos, aunque no esté cerrado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a noventa días – multa."

INTERVENCIÓN TELEFÓNICA

"Artículo 162°.- El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. (...)."

C. Artículos 4 y 87 del Texto Único Ordenado de la Ley de Telecomunicaciones Decreto Supremo 013-93-TCC

"Artículo 4.- Toda persona tiene derecho a la inviolabilidad y al secreto de las telecomunicaciones. El Ministerio de Transportes, Comunicaciones, Vivienda y Construcción se encarga de proteger este derecho."

"Artículo 87.- Constituyen infracciones muy graves: (...)

CONFIDENCIAL

- 4) La interceptación o interferencia no autorizadas de los servicios de telecomunicaciones no destinados al uso libre del público en general.
- 5) La divulgación de la existencia o del contenido, o la publicación o cualquier otro uso de toda clase de información obtenida mediante la interceptación o interferencia de los servicios de telecomunicaciones no destinados al uso público general (...)"

D. Artículo 2 de la Ley 27697.

"Artículo 2° .- "Se entiende por "Comunicación" a cualquier forma de transmisión del contenido del pensamiento, o de una forma objetivada de éste, por cualquier medio. Para efectos de esta Ley, no interesa que el proceso de transmisión de la comunicación se haya iniciado o no. Se entiende por "medio" al soporte material o energético en el cual se porta o se transmite la comunicación. Para efectos de esta Ley tiene el mismo régimen que la comunicación misma..."

E. Artículo 10 del Reglamento General de la Ley de Telecomunicaciones – Decreto Supremo 06-94-TCC

"Artículo 10°.- Se atenta contra la inviolabilidad y el secreto de las telecomunicaciones, cuando deliberadamente una persona que no es quien cursa la comunicación ni es el destinatario, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, utiliza, trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación.

Las personas que en razón de su función tienen conocimiento o acceso al contenido de una comunicación cursada a través de los servicios públicos de telecomunicaciones, están obligadas a preservar la inviolabilidad y el secreto de la misma.

Los concesionarios de servicios públicos de telecomunicaciones, están obligados a adoptar las medidas más idóneas para garantizar la inviolabilidad y el secreto de las comunicaciones cursadas a través de tales servicios."

F. Artículo 4.1 y 4.2 de la Resolución Ministerial No.622-96-MTC/15.17, que aprueba la Directiva No.002-96-MTC/15.17

"4.1 INVIOABILIDAD Y SECRETO DE LAS TELECOMUNICACIONES

Se atenta contra la inviolabilidad y el secreto de las telecomunicaciones cuando deliberadamente una persona que no es quien cursa la comunicación, ni es el destinatario, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, utiliza, trata de conocer o facilitar que él mismo u otra persona conozca la existencia o el contenido de cualquier comunicación, de acuerdo a lo definido en el artículo 10° del Reglamento General de la Ley de Telecomunicaciones".

"4.2 PROTECCIÓN DE DATOS E INFORMACIÓN PERSONAL

CONFIDENCIAL

Se atenta contra la protección de la información personal relativa a los abonados o usuarios cuando ésta es entregada a terceros i) sin el consentimiento previo, expreso y por escrito del abonado o usuario y demás partes involucradas; o ii) sin una orden judicial específica motivada del Juez con las garantías previstas en la ley.

La obligación de protección de datos está referida única y exclusivamente a la información personal proporcionada por los abonados y usuarios a la empresa operadora en el curso de sus negocios. No se encuentra comprendida en los alcances de esta obligación la información personal que las empresas operadoras deben incluir en las guías de abonados que publiquen."

G. Sección 8.10 de los Contratos de Concesión celebrados por Telefónica del Perú S.A.A. con el Estado Peruano.

" Sección 8.10: Secreto de las Telecomunicaciones y Protección de Datos.

(a) Obligación de Salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos. La EMPRESA CONCESIONARIA establecerá medidas y procedimientos razonables para salvaguardar el secreto de las telecomunicaciones y mantener la confidencialidad de la información personal relativa a los USUARIOS que atienda en el curso de sus negocios. La EMPRESA CONCESIONARIA designará a nivel de la administración de la empresa, el personal que estará a cargo de la implementación, cumplimiento y supervisión de tales medidas. La EMPRESA CONCESIONARIA enviará al MINISTERIO y a OSIPTEL un informe anual sobre las medidas y procedimientos que se hayan establecido en su funcionamiento y sobre los cambios y las mejoras necesarias, debiendo presentar tales informes el 15 de febrero de cada año, comenzando el año siguiente al de la FECHA EFECTIVA.

(b) Ámbito de la Obligación de Secreto y Protección de Datos. La EMPRESA CONCESIONARIA salvaguardará el secreto de las telecomunicaciones y mantendrá la confidencialidad de la información personal relativa a sus USUARIOS, que atienda en el curso de sus negocios, salvo (i) el consentimiento previo, expreso y por escrito del USUARIO y demás partes involucradas o (ii) una orden judicial específica."

H. ENTREGA DE INFORMACIÓN A OSIPTEL VINCULADA CON SU FACULTAD SUPERVISORA

Artículo 8 de la Ley 27336, Ley de Funciones y Facultades de OSIPTEL

"8.1 En ningún caso la autoridad competente puede solicitar información que signifique la violación al derecho al secreto y la inviolabilidad de las

CONFIDENCIAL

comunicaciones, a que se refiere el inciso 10) del Artículo 2° de la Constitución Política del Peru.

8.2 Se atenta contra este derecho, cuando deliberadamente una persona que no es quien cursa la comunicación ni es el destinatario, intenta conocer, alterar, publicar o utilizar el contenido de la misma o facilita que otra persona conozca la existencia o el contenido de cualquier comunicación.

8.3 No constituye violación del derecho al secreto y la inviolabilidad de las telecomunicaciones, ni afecta el derecho a la confidencialidad de la información personal, el acceso que tenga OSIPTEL a la información necesaria para cumplir sus funciones y, particularmente, el ejercicio que haga de las facultades contempladas en el Artículo 15° de la presente Ley. En ningún caso OSIPTEL podrá exigir la presentación de información que revele el contenido de las comunicaciones.”

Jurisprudencia nacional para la protección del secreto de las telecomunicaciones

Sentencia del 9 de marzo de 1998, emitida por la Sala Corporativa Transitoria Especializada en Derecho Público. Exp. N° 170-97: “...secreto de las comunicaciones no se limita al contenido en sí sino que la hacen extensiva a la existencia de cualquier comunicación, que implica la identidad del autor o destinatario del enlace, la oportunidad, frecuencia o prioridad de las comunicaciones, aún con prescindencia de su contenido, pueden inferirse conclusiones que afectan a la privacidad o a la intimidad de los interlocutores...”

CONFIDENCIAL

**EXPOSICIÓN SOBRE
LAS MEDIDAS RAZONABLES ADOPTADAS EN
TELEFONICA DEL PERU PARA LA SALVAGUARDA DEL
SECRETO DE LAS TELECOMUNICACIONES Y DE LA
INFORMACIÓN EN GENERAL**

Lima 10 de noviembre del 2003

INDICE

- 1. Conceptos**
- 2. Antecedentes**
- 3. Compromiso de Telefónica**
- 4. Desarrollo del Contenido**
 - a) Protección contra fraudes en el uso de los servicios de comunicaciones: autenticación y otras medidas.
 - b) Protección contra la interceptación de comunicaciones.
 - c) Protección de instalaciones base: seguridad de acceso e intervención de personal no autorizado.
- Pausa en la presentación**
 - d) Seguridad en la central de conmutación.
 - e) Seguridad de las redes de comunicaciones: "firewalls" u otros.
 - f) Control de personal que supervisa las comunicaciones.
 - g) Otros mecanismos de protección de la información
- 5. Preocupación por recientes iniciativas legislativas.**

1. Conceptos

Telefónica del Perú S.A.A. (Telefónica) ha desarrollado una serie de políticas, normas y prácticas razonables para la salvaguarda del secreto de las telecomunicaciones y de la información en general, las que varían con el tiempo teniendo en cuenta las nuevas tecnologías que se implementan.

A pesar del esfuerzo desplegado y por lo compleja de la actividad no es posible garantizar una protección absoluta.

Secreto de las Telecomunicaciones

“Se atenta contra la inviolabilidad y el secreto de las telecomunicaciones cuando deliberadamente una persona que no es quien cursa la comunicación, ni es el destinatario, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, utiliza, trata de conocer o facilitar que él mismo u otra persona conozca la existencia o el contenido de cualquier comunicación, de acuerdo a lo definido en el Art. 10° del Reglamento General de la Ley de Telecomunicaciones”(RM.N° 622-96-MTC15.17)

1. Conceptos (Cont.)

Protección de datos e información personal

“Se atenta contra la protección de la información personal relativa a los abonados o usuarios cuando ésta es entregada a terceros i) sin el consentimiento previo, expreso y por escrito del abonado o usuario y demás partes involucradas ; o ii) sin una orden judicial específica motivada del Juez con las garantías previstas en la ley.

La obligación de protección de datos está referida única y exclusivamente a la información personal proporcionada por los abonados y usuarios a la empresa operadora en el curso de sus negocios. No se encuentra comprendida en los alcances de esta obligación la información personal que las empresas operadoras deben incluir en las guías de abonados que publiquen.” (RM.N° 622-96-MTC15.17)

2. Antecedentes

Con Oficio N° 1067-2003-MTC/03.01 el Ministerio de Transportes y Comunicaciones menciona la creación de una Comisión para la actualización de la Directiva N° 002-96-MTC/15.17 referida a los procedimientos de inspección y de requerimiento de información relacionados al secreto de las telecomunicaciones y protección de datos y solicita que personal especializado de Telefónica, en temas de mecanismos de seguridad y protección de las comunicaciones efectúen una serie de exposiciones sobre los temas siguientes:

- a) Protección contra fraudes en el uso de los servicios de comunicaciones: autenticación y otras medidas.
- b) Protección contra la interceptación de comunicaciones.
- c) Protección de instalaciones base: seguridad de acceso e intervención de personal no autorizado.
- d) Seguridad en la central de conmutación.
- e) Seguridad de las redes de comunicaciones: "firewalls" u otros.
- f) Control de personal que supervisa las comunicaciones.
- g) Otros mecanismos de protección.

3. Compromiso de Telefónica

• Telefónica está comprometida con la salvaguarda del secreto de las telecomunicaciones y protección de datos y reconoce su importancia, por ello se han definido procedimientos razonables de seguridad y guías para el manejo de la información.

• Difunde y transmite permanentemente las medidas razonables de seguridad a los empleados, así como entrenamiento para la formación de especialistas de seguridad.

• Ha instituido los conceptos básicos de Menor Privilegio (las personas tienen acceso solo a la información que manejan) y el de Separación de Funciones (para actividades e información crítica es necesario el concurso de al menos dos personas autorizadas).

3. Compromiso de Telefónica (Cont.)

- En este sentido, se encuentra vigente la circular sobre "Cumplimiento de medidas para salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos", la cual es de aplicación general en Telefónica.

4. Desarrollo del Contenido

CONFIDENCIAL

a) Protección contra fraudes en el uso de los servicios de comunicaciones

Emprende permanentemente acciones contra:

- Hurto de Línea
- Clonación
- LBO o By Pass
- Suplantación en la suscripción
- Call Back
- PRS (Premium Rate Service) Internacional y Local
- Manipulación de TUP

a) Protección contra fraudes en el uso de los servicios de comunicaciones (Cont.)

RESULTADOS

TIPO DE FRAUDE	DESCRIPCIÓN	Sep-02	Oct-02	Nov-02	Dic-02	Ene-03	Feb-03	Mar-03	Abr-03	May-03
SUPlantación DE SUSCRIPCIÓN	NO DE LINEAS	1	0	15	6	18	1	15	9	3
	FRAUDE DETECTADO (US\$)	135	0	614	1 946	1 212	67	2 191	677	210
	FRAUDE EVITADO (US\$)	14 272	0	12 394	36 691	40 873	1 709	84 420	29 536	9 588
HURTO DE LINEA	NO DE LINEAS	16	31	28	21	17	1	0	6	3
	FRAUDE DETECTADO (US\$)	3 433	7 899	2 604	2 500	2 579	31	0	978	1 093
	FRAUDE EVITADO (US\$)	128 594	649 598	115 450	74 691	65 918	921	0	21 229	22 000
CLON	NO DE LINEAS	0	0	1	1	0	0	0	0	0
	FRAUDE DETECTADO (US\$)	0	0	79	927	0	0	0	0	0
	FRAUDE EVITADO (US\$)	0	0	1 604	55 594	0	0	0	0	0
LBO	NO DE LINEAS	0	0	2	0	0	0	0	1	0
	FRAUDE DETECTADO (US\$)	0	0	31 876	0	0	0	0	49	0
	FRAUDE EVITADO (US\$)	0	0	634 264	0	0	0	0	1 363	0
PRS	NO DE LINEAS	228	269	167	80	72	74	86	97	97
	FRAUDE DETECTADO (US\$)	41 403	47 885	13 077	6 536	5 306	5 133	4 730	4 989	5 568
	FRAUDE EVITADO (US\$)	3 527 803	4 119 553	914 986	252 189	224 637	244 405	469 821	423 101	537 075
MANIPULACIÓN DE EQUIPO	NO DE LINEAS	23	18	14	39	15	14	18	11	21
	FRAUDE DETECTADO (US\$)	2 480	1 608	1 188	1 953	1 465	1 016	785	1 044	1 012
	FRAUDE EVITADO (US\$)	38 030	49 081	33 442	68 758	39 895	36 289	56 640	25 261	33 506

Falta el cálculo del impacto de los Casos de LBO de setiembre y agosto 2003

CONFIDENCIAL

a) Protección contra fraudes en el uso de los servicios de comunicaciones (Cont.)

MEDIDAS PARA PROTEGERNOS DEL FRAUDE EN TELECOMUNICACIONES

Implementación de Sistemas Antifraude para Detección Oportuna.

Técnicas

Implementación de interfaces (ALT) para prevención de robos de líneas en los teléfonos públicos.

Implementación del sistema de control de acceso a armarios en la planta externa.

Procesos informáticos tipo "Bach" para detección de incidencias comunes en la red.

Procedimiento para tratamiento oportuno de incidencia de fraude, bajo software especializado.

Organizativas

Elaboración de normas corporativas orientadas al fraude de las telecomunicaciones.

Planes de inducción sobre la prevención del fraude.

Recursos

Creación de una Sub Gerencia especializada para la lucha contra el fraude en las telecomunicaciones.

Coordinación continua con legales e instituciones externas.

b) Protección contra la interceptación de comunicaciones

- Si se produjera una interceptación es probable que ésta ocurra accediendo a puntos específicos en la planta externa de redes físicas o de hilos de cobre.
- Para efectuarla se requiere conocimiento especializado y equipos.
- Telefónica ha desplegado medidas de protección y seguridad para proteger las instalaciones físicas que albergan las centrales de conmutación y los puntos de las redes de planta externa que podrían calificarse como vulnerables, tales como: MDF, cámaras, armarios, cajas terminales y las líneas de acometida que conectan directamente al domicilio de los usuarios del servicio.

b) Protección contra la interceptación de comunicaciones
(Cont.)

Protección en MDF's.-

Se cuenta con los siguientes sistemas de seguridad:

- **Sistema Inteligente de Seguridad (SIS).**
- **Control de acceso a locales con personal de vigilancia.**
- **Sistema informático de control y autorización de ingreso a los ambientes de MDF's (CAL).**
- **Circuito cerrado de cámaras de video en algunos locales.**

b) Protección contra la interceptación de comunicaciones
(Cont.)

Protección en armarios:

- **Para proteger los armarios, además de ubicarlos o reubicarlos a una altura que evite la manipulación, se ha implementado el reemplazo de candados convencionales por candados con clave y medidas adicionales en planchas de fierro transversal.**
- **En otros armarios se ha implementado un sistema de clave, que consiste en una cerradura computarizada con una tarjeta magnetizada, asignada sólo a personal autorizado. En zonas de alto riesgo se cuenta con sistemas mixtos, esto es, candado con clave de acceso y clave en sistemas.**

b) Protección contra la interceptación de comunicaciones
(Cont.)**Protección en cámaras subterráneas.-**

Se ha implementado diversos sistemas de protección, tales como:

- **Grava**, que permite saturar la cámara con piedra menuda en sus espacios internos. Este sistema es aplicado sólo en Lima y principalmente en zonas alejadas, cuyo mantenimiento es poco frecuente.
- **Contratapa neumática**, ideada para la apertura y el cierre de las cámaras mediante un equipo compresor de aire. Sistema instalado sólo en Lima para zonas urbanas de frecuente mantenimiento y de alto riesgo delincriminal.
- **Soldadura**, que consiste en platinas de fierro soldadas a la tapa y el marco de la cámara, instaladas a nivel nacional en zonas urbanas con alta incidencia de robos y de frecuente mantenimiento.
- **Neumática y soldadura**, que combina los sistemas antes descritos, instaladas sólo en Lima.
- **Concreto**, que es una loza de concreto que permite el encriptado de la cámara, instalado a nivel nacional en zonas alejadas con alto índice delincriminal.

b) Protección contra la interceptación de comunicaciones
(Cont.)**Protección eléctrica de la red**

El objeto de estos sistemas es eliminar los riesgos de descarga eléctrica que pueden afectar a los equipos o dispositivos propios de las redes de telecomunicaciones y a los usuarios, entre los que tenemos:

- i. **Instalación de tomas a tierra**, que consiste en la implementación de pozos a tierra,
- ii. **En forma complementaria a este sistema**, se efectúan periódicamente verificaciones en el estado de las redes, tendientes a ejecutar reconcentraciones, reubicación de líneas, así como predistribución y reubicación de cables, que consiste en el cambio del recorrido de las líneas, cuando se perciba posible exposición a descargas por cercanía a las instalaciones de la red pública de energía eléctrica.

Protección en cajas terminales

- La gran mayoría de cajas terminales han sido instaladas a una altura que evite la manipulación, dificultando el acceso de personas no autorizadas y sin los implementos adecuados.

b) Protección contra la interceptación de comunicaciones
(Cont.)

Medidas de salvaguarda durante la operación y mantenimiento de la red de planta externa.-

- Se cuenta con manuales, procedimientos, cartillas operativas y otros documentos internos.
- El Reglamento Interno de Trabajo, que establece responsabilidades y acciones a seguir para la ejecución de los trabajos propios del quehacer de la Empresa.
- Uso obligatorio de uniforme y carné de identificación para todo el personal técnico.
- Uso de unidades móviles de color corporativo y logotipo de la Empresa.
- Todo trabajo debe estar respaldado por documentos emitidos por personal autorizado.

b) Protección contra la interceptación de comunicaciones
(Cont.)

Documentos Normativos:

- **Medidas para Salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos (TBI-I-002-Junio 96):** Establece que la Gerencia de Operación de Redes de Acceso y Clientes (GORAC), es responsable de la vigilancia de las empresas contratistas y/o colaboradoras (Instalaciones/Reparaciones) y de autorizar el ingreso del personal a los Distribuidores (MDF)/Mesa de pruebas.
- **Manual Jefes de Departamento Post Venta (TB2-M-001-Abril 96):** Establece la responsabilidad directa de las jefaturas en el estricto cumplimiento de las normas de seguridad y control de acceso a centrales de distribuidores y sectores bajo su cargo, incluyendo parámetros de control que fomenten revisiones periódicas de la red de distribución.
- **Manual de Coordinadores Post Venta (TB2-M-002-Abril 96):** Establece que el coordinador es responsable de mantener permanentemente actualizada la relación de personas autorizadas a ingresar en los ambientes de los MDFs; así como de supervisar la ejecución de obras por empresas y organismos ajenos a Telefónica.

b) Protección contra la interceptación de comunicaciones
(Cont.)

Documentos Normativos:

- **Manual del Instalador Reparador de Líneas Telefónicas (GST-M-004-Septiembre 01):** Recomienda que no se instalen cajas terminales en azoteas de edificios, debido a que dicha ubicación facilita la comisión de actos dolosos, tales como robo de línea.
- **Manual de Funciones en M.P.C. (Módulo de Pruebas Centralizadas) y M.D.F. (TB2-M-003-Julio 96):** Establece un control más estricto sobre la documentación; además, especifica que el responsable de MDF debe controlar todas las actuaciones que se realizan en los MDFs. Si los trabajos son realizados por personal de otras áreas o de sus respectivas contratadas, el supervisor del MDF debe tener en todo momento conocimiento de los trabajos que se van a efectuar y del estado de los mismos, manteniendo contactos frecuentes con el responsable de su ejecución y supervisándolos personalmente o delegando un responsable para que lo haga.

b) Protección contra la interceptación de comunicaciones
(Cont.)

Documentos Normativos:

- **Procedimiento para el Control de Penalización a Contratadas (TB2-P-003 - septiembre 96):** Establece que se efectuará la verificación física de los trabajos efectuados por terceros.
- **Procedimiento para el mantenimiento de datos de facilidades técnicas (TB2-P-002-Septiembre 96):** Especifica cuando se detecta una inconsistencia entre la información del sistema y el estado físico (MDF o planta) para actuar en caso de inconsistencia.
- **Procedimiento para Control y Supervisión en la ejecución a contratistas de Ordenes de Servicio (OMR2-P-012 - Noviembre 97):** Establece que la ejecución de órdenes de servicio se llevará a cabo con estricta sujeción a las condiciones establecidas en el contrato respectivo y a los detalles e instrucciones indicados en los documentos que se entregan a las Contratistas.

**b) Protección contra la interceptación de comunicaciones
(Cont.)**

Documentos Normativos:

- **Procedimiento para Pequeños Trabajos de Red (OMR2-P-006 - septiembre 99):** Norma la ejecución de obras que surgen como consecuencia de la necesidad de efectuar trabajos de modificación, adecuación o restauración en instalaciones existentes y que puedan provenir de propuestas efectuadas para atender o mejorar el servicio o para sustituciones de emergencia que pudieran vulnerar el nivel de operatividad de nuestro plantel exterior.
- **Instrucción Calificación a Contratistas (GST-I-002 6ta. Edición (Julio 01):** Define los diferentes conceptos a considerar en la calificación a contratistas a nivel nacional, en los rubros de instalaciones (básica, troncales, circuitos digitales y analógicos, CATV), reparaciones (básica y CATV) y mantenimiento de planta externa. Entre los conceptos a ser calificados se considera la actuación dentro del marco de la ley sobre el secreto de las telecomunicaciones.

**b) Protección contra la interceptación de comunicaciones
(Cont.)**

Documentos Normativos:

- **Cartilla Operativa para Actuaciones en caso de Traslados no Autorizados (GST-C-008 1ra. Edición - Agosto 01):** Establece las actuaciones para el seguimiento y tratamiento de los traslados no autorizados.
- **Documento Interno sobre Inspecciones Técnicas - Seguridad de Planta:** Documento dirigido expresamente a las personas que están a cargo de las inspecciones técnicas (personal supervisor y personal técnico) y difundido al personal técnico de contratistas.
- **Norma de Atención de Requerimientos de Información de Autoridades Públicas (GO-SG-001 julio 01):** Establece los lineamientos, procesos y responsabilidades en la atención de requerimientos de información de autoridades públicas (Poder Judicial, el Ministerio Público, la Policía Nacional y el Congreso de la República, etc.), dentro del marco jurídico relativo a la protección del secreto de las telecomunicaciones.

b) Protección contra la interceptación de comunicaciones
(Cont.)

Documentos Internos- "Sabes Qué?"

- **Sabes Qué 012-97 (noviembre 97):** Actuación para el ingreso y salida a locales implementados con el Sistema Inteligente de Seguridad (SIS).
- **Sabes Qué 004 - 98 (junio 98):** Indica las acciones a seguir en casos de robo de tapas de los buzones o cámaras telefónicas, que ocasionan daños a la infraestructura de Telefónica del Perú y ponen en peligro la seguridad física de las personas que transitan cerca de estas cámaras. Además del número telefónico 102 también se puede dar aviso de la falta de tapa de cámaras a los números telefónicos 103 y 104 que se han sumado a la acción de reposición de tapas robadas.
- **Sabes Qué 017/99 (Octubre 99):** Referido a la habilitación a nivel nacional de un número libre de tasación 0800-1-9000, al cual podrán efectuarse denuncias en caso de observar personas que se encuentren manipulando cables telefónicos, en horarios distintos a los que el personal autorizado realiza sus labores habituales (07:00am / 09:00pm).

b) Protección contra la interceptación de comunicaciones
(Cont.)

Documentos Internos- "Sabes Qué?"

- **Sabes Qué 005- 98 (junio 98):** Para prevenir actos dolosos por parte de falsos clientes que vienen sorprendiendo a Telefónica cometiendo fraudes. Documento dirigido al personal de Telefónica y de las Contratistas.
- **Sabes Qué 020- 99 (noviembre 99):** Refiere la creciente proliferación de equipos telefónicos monederos de diversas procedencias conectados a líneas de telefonía básica. Al respecto la Gerencia de Telefonía de Uso Público ha puesto a disposición dos números telefónicos de marcación abreviada 1425 y 1426 de acceso gratuito a nivel nacional, a través de los cuales se reciben las denuncias correspondientes de lunes a viernes de 08.00 Hrs. a 20.30 Hrs.; sábados y domingos de 08.00 Hrs. a 18.30 Hrs. También se podrá presentar denuncias vía correo electrónico.
- **Sabes Qué 006/00 (junio 00):** Refiere la relación de documentos normativos emitidos por la Gerencia de Seguridad y Protección, indicando además la ruta de acceso a la página web donde están contenidas <http://intranet/seguridad/>

b) Protección contra la interceptación de comunicaciones
(Cont.)

Documentos Internos- "Sabes Qué?"

- Sabes Qué 004 / 01 (mayo 01): Indica las acciones a seguir al detectarse alguna instalación clandestina. Los autores de estas irregularidades, previa identificación, serán severamente sancionados con la aplicación de las medidas disciplinarias respectivas de acuerdo al Reglamento Interno de Trabajo, de tratarse de trabajadores de Telefónica y con la aplicación de multas y penalidades en caso de tratarse de empresas colaboradoras.
- Sabes Qué 005 . 01 (junio 01): Referido a prevenir la comisión de actos dolosos llevados a cabo con la participación de malos técnicos que hacen uso indebido de sus conocimientos de planta y recursos materiales para efectuar conexiones clandestinas del servicio televisión por cable a usuarios no autorizados.
- Sabes Qué 001/ 02 (enero 02): Da a conocer los lineamientos a ser considerados a efectos de lograr la protección de la información confidencial que se emite teniendo en cuenta los grados de información calificados por OSIPTEL.

b) Protección contra la interceptación de comunicaciones
(Cont.)

Documentos Internos- "Sabes Qué?"

- Sabes Qué 008/ 02 "Difusión de Normas de Otras Gerencias" (febrero 02): Su finalidad es difundir las normas externas a la Gerencia Operación de Redes de Acceso y Clientes, incorporando cinco normas en el aplicativo interactivo "AMIGO" y en el Servidor de la red ofimática, en la Carpeta "Normas de otras Gerencias".
- Sabes Qué 008/ 02 "Denuncias por Daños a la Planta" (Mayo 02): Indica las acciones a seguir en los supuestos que, durante las inspecciones realizadas en la planta de telefonía básica y CATV, se detecten robos y cortes de cables aéreos o subterráneos, robos de dispositivos, desaparición de tapas de cámaras, instalaciones clandestinas, puntos de riesgo eléctrico, robo de líneas telefónicas de los clientes, etc.

c) Protección de Instalaciones Base: seguridad de acceso e intervención de personal no autorizado

VISIÓN DE LA PROTECCIÓN

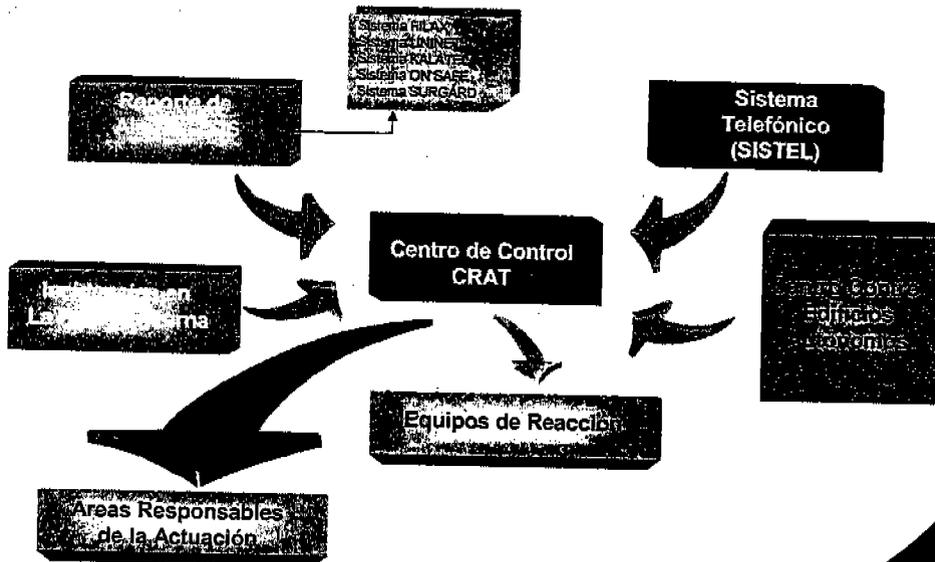
- MEDIDAS RELACIONADAS CON LOS RECURSOS HUMANOS VINCULADAS A LA SEGURIDAD.
- MEDIDAS ORGANIZATIVAS DE SEGURIDAD
- MEDIDAS TÉCNICAS DE SEGURIDAD

c) Protección de Instalaciones Base: seguridad de acceso e intervención de personal no autorizado (Cont.)

RIESGOS PRINCIPALES

- Incendios
- Accesos no autorizados
- Asaltos

i) MEDIDAS TÉCNICAS DE SEGURIDAD



c) Protección de Instalaciones Base: seguridad de acceso e intervención de personal no autorizado (Cont.)

ii) MEDIDAS RELACIONADAS CON LOS RECURSOS HUMANOS VINCULADAS A LA SEGURIDAD.

Servicios de Seguridad

Dentro de los servicios de seguridad se encuentran la Vigilancia Privada, Guardianía, Operadores de Centros de Control y los Grupos de Reacción Móviles.

Vigilancia Privada.-

Instalada en locales principales y grandes centrales con consignas precisas para el control de acceso y atención de ocurrencias.

Así mismo, los puestos de vigilancia y centros de control cuentan con los procedimientos y la normativa vigente.

Guardianía

Instalada en locales del ámbito rural donde no es aplicables el SIS, por las distancias y condiciones geográficas del lugar.

c) Protección de Instalaciones Base: seguridad de acceso e intervención de personal no autorizado (Cont.)

iii) MEDIDAS ORGANIZATIVAS DE SEGURIDAD

Como complemento al Sistema Inteligente de Seguridad (SIS) y a los Servicios de Seguridad se cuenta con normas y procedimientos escritos, estas son:

Normas:

- Norma de Control de Accesos.
- Previsión del Espionaje Empresarial.
- Norma Previsión Contra Las Sustracción De Bienes
- Norma Previsión Contra Robo De Equipos Informaticos
- Norma De Control De Accesos
- Norma Previsión y Lucha Contra Incendio.

POR LO ANTES EXPUESTO. ES PRECISO MENCIONAR QUE LOS SISTEMAS IMPLEMENTADOS PERMITEN EFECTUAR EL CONTROL DE ACCESOS, EN OTRAS PALABRAS PERMITIR EL INGRESO SÓLO DEL PERSONAL AUTORIZADO POR LAS ÁREAS DE LAS EMPRESAS

PAUSA

d) Seguridad en la Central de Conmutación

Control de acceso

- El empleo del Sistema Inteligente de Seguridad – SIS, permite proporcionar toda la información adicional necesaria a fin de evitar el posible riesgo de ingreso de personal no autorizado.
- En la mayoría de los locales existen cámaras de seguridad, de manera que de ingresar personal no autorizado es detectado por el personal operador del sistema.
- El personal que realiza el mantenimiento de las baterías es autorizado por la gerencia a cargo, y sólo este personal autorizado puede acceder a las salas de conmutación.
- Se cuenta con el aplicativo “Control de Acceso a Locales (CAL)”, vía Intranet y administrado por el Centro de Recepción de Alarmas y Teleservicios (CRAT), mediante el cual solamente se facilita el acceso a las centrales al personal autorizado.
- En los casos de locales que contaban con varios accesos a la sala de centrales de conmutación, éstos han sido clausurados, por lo que, en la actualidad, sólo existen una sola vía de acceso.

d) Seguridad en la Central de Conmutación (Cont.)

Orden y Control

- En las centrales cabecera se cuenta con un cuaderno que permite el registro de visitas y ocurrencias.
- El registro de las averías se realiza en forma automatizada mediante el Sistema Integral de Gestión de Incomunicaciones, Incidencias y Averías – SIGINIA.
- Los Manuales de Rutinas de Operación y Mantenimiento se encuentran en Intranet, los cuales pueden consultarse desde los terminales de las centrales y sólo con usuarios con la contraseña correcta.
- Para el acceso a las centrales con la finalidad de cambios de tarjetas defectuosas, se cuenta con un stock en cada central y un stock de tarjetas para fallos críticos y se cuenta con el inventario y control de movimientos respectivo.
- Todas las centrales cuentan con un registro de transacciones o comandos hombre-máquina que guarda la información de aproximadamente un mes.

d) Seguridad en la Central de Conmutación (Cont.)

Acceso a la Información

- Todas las computadoras que se encuentran en las centrales cuentan con acceso restringido por password y usuario.
- El uso de directorios compartidos se realiza también por medio de permisos específicos para casos de acceso remoto. Actualmente dichos directorios sólo son utilizados por usuarios autorizados y solamente contienen información general para las áreas que las utilizan, no se comparte información estratégica y/o confidencial.
- El sistema de control es sólo utilizado por personal autorizado. En los casos de las tecnologías que no cuentan con una funcionalidad que permita el bloqueo por inactividad, los terminales de este tipo de centrales han sido cambiados por PC's las cuales permiten este tipo de bloqueo.

d) Seguridad en la Central de Conmutación (Cont.)

Acceso a la Información

- En principio, el personal que ingresa a las centrales es personal autorizado. A este personal no se le permite salir del entorno del correo corporativo de Telefónica.
- La documentación de las hojas de ruta de conexión y desconexión se encuentran almacenadas ordenadamente en armarios dentro de la sala de supervisión, la cual es de acceso restringido.
- Los cortes y reconexiones por deudas son ejecutados automáticamente por el Centro de Cortes y Reconexiones Automáticas (CCRA), en las centrales digitales de tecnología AXE, 5ESS y S12 y en las centrales NEAX y PRX, esta labor es realizada en forma manual por personal de centrales.
- Todos los números de prueba en las centrales están restringidas para las llamadas a servicio celular, Larga Distancia Nacional (LDN), Larga Distancia Internacional (LDI) y 0808. Cuando se tienen que realizar pruebas específicas de estos servicios, se levanta la restricción, se ejecutan las pruebas y una vez finalizadas, se los restringe nuevamente. Cabe precisar que estas pruebas son realizadas únicamente por personal y hacia números telefónicos, previamente autorizados.

e) Seguridad en las redes de comunicaciones:

“Firewalls” u otros

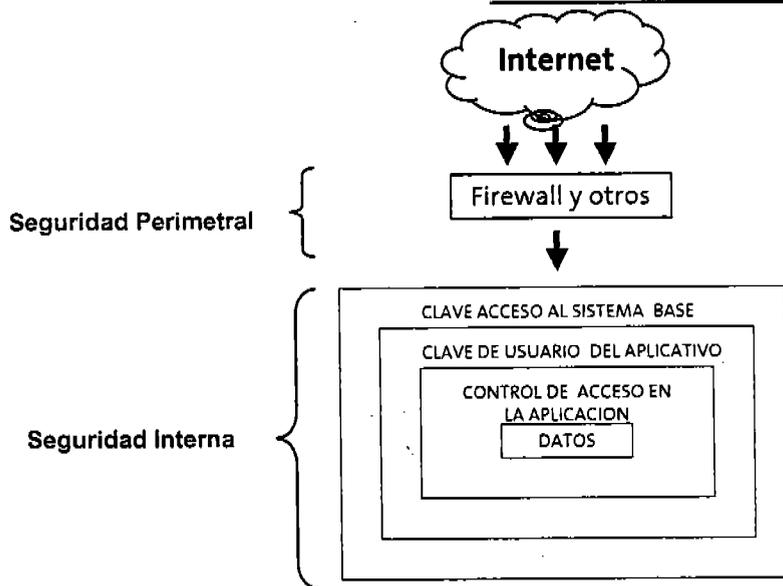
1. Dentro de la red corporativa de ordenadores de Telefónica se han implementado los siguientes elementos o herramientas de seguridad:
 - “Firewall” o Cortafuegos, con este dispositivo se controla el acceso entre las redes (Internet, Extranet e Intranet), usando una política de seguridad. Mediante este dispositivo se fija que usuarios externos pueden entrar a usar los recursos de la red.
 - Sistema de Detección de Intrusos, permite analizar el tráfico entrante y saliente de la red en busca de actividad anormal o señales de intrusión, registrando información útil para un diagnóstico y acción correctiva rápida.
 - Analizadores de Vulnerabilidades, estas herramientas permiten la búsqueda de vulnerabilidades en servidores corporativos y equipos de comunicaciones de forma periódica y los cambios en los sistemas operativos de los sistemas de información corporativos.
 - Servidores VPN, equipos que brindan la encriptación del canal de comunicación.

e) Seguridad en las redes de comunicaciones:

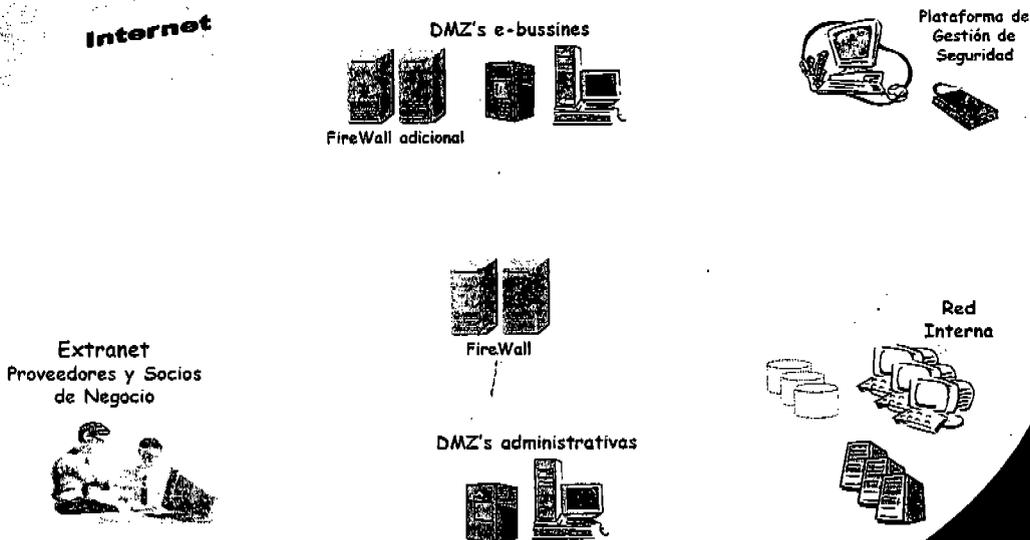
“Firewalls” u otros (Cont.)

- Analizadores de Cambios, con estas herramientas se detectan los cambios en los sistemas operativos de los sistemas de información corporativos
- Medidores de controles de seguridad en sistemas operativos, herramientas para detección de cambios en los sistemas operativos de los sistemas de información corporativos.
- Revisión y mantenimiento periódico de los niveles de acceso de los usuarios a los sistemas de información, lo cual se realiza para controlar y reducir los accesos que ya no se encuentren vigentes.
- Gestión de accesos centralizada, con procedimientos formalizados de creación, modificación y eliminación de accesos.

e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)



e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)



**e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)**

2. Se ha elaborado las políticas y las normas para salvaguardar la seguridad de la información.-
- Se ha establecido la normativa de protección de la información que Telefónica guarda en los sistemas de información, la cuál contempla las mejores prácticas que se ejecutan a nivel mundial.
 - La normativa, establece los requisitos que deben implementarse y cumplirse para minimizar los riesgos a que está expuesta la información en todos los ámbitos por donde fluye.
 - La normativa indicada se encuentra publicada en la Intranet de la compañía para uso interno de los empleados de Telefónica.
 - Se realizan diversas acciones para la difusión y la concientización del personal para su aplicación.

**e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)**

..... Políticas y Normativa Vigente.-

- Funciones y obligaciones de los empleados.
- Clasificación y tratamiento de la información.
- Identificación y autenticación.
- Control de accesos a los S.I.
- Redes y comunicaciones.
- Control de software.
- Desarrollo de sistemas de información.
- Registros de auditoría y monitorización.
- Incidencias de seguridad.
- Copias de respaldo y de recuperación.
- Revisiones de seguridad.
- Ceses de personal.
- Normas generales de seguridad en el manejo de laptop.

**e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)**

3. Medidas razonables adicionales para salvaguardar los niveles de seguridad de información

- Implementación de un "Consejo de arquitectura de sistemas".
- "Testing" de nuevos sistemas que ingresan a etapa productiva y a los cambios que se les realizan.
- Constitución de un "Comité de seguridad de los sistemas", para evaluar el cumplimiento de los requisitos de seguridad informática de las aplicaciones que ingresan a producción.
- Seguimiento de un Plan de "Concientización de la seguridad de información" para todos los empleados.

**e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)**

4. Medidas de Contingencia en los Sistemas de Información

- Se cuenta con un esquema de contingencia para los sistemas de información, con 2 Centros de Procesamiento de Datos (CPD), uno principal que alberga sistemas en producción y un CPD secundario, que alberga plataformas alternas que se utilizarían ante una eventual contingencia. Este esquema incluye un sistema automatizado de "backup" (robot) y sistemas de alta disponibilidad para los discos.

**e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)**

Medidas de Contingencia en los Sistemas de Información (Cont.)

- Se tiene además un Sistema integral de seguridad física en los Centros de Procesamiento de Datos que incluye:
 - Sistema automático de extinción en incendios.
 - Sistema de alarmas y sensores contra incendio, intrusión e inundación.
 - Sistema de control de acceso, mediante huella digital, tarjetas de proximidad, esclusa de ingreso detectora de metales y de peso, y sistema de evacuación de emergencia.
 - Sistema de vigilancia 7x24 externo e interno mediante circuito cerrado de TV, grabadoras VHS de eventos.
 - Sistema integrador y puesto de control, desde donde se monitorean los niveles de seguridad de los sistemas anteriormente descritos, así como los sistemas secundarios de UPS, energía, aire acondicionado

**e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)**

Políticas de salvaguarda de la seguridad en las PC's

- Antivirus cliente en PC's.
- Consola de administración remota.
- Actualización automática.
- Distribución centralizada de antivirus.
- Customización de políticas por negocio.
- Políticas de restricciones según el perfil del usuario.
- Acceso mediante reconocimiento biométrico (huella digital) a algunas estaciones con información crítica para la empresa.

e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)

Administración avanzada y reportes

- Consola basada en políticas de seguridad
- Monitor de actividad y motor de reportes

Protección en el perímetro de Internet

- Servidores de correo electrónico
- Proxy, SMTP
- Gateway

Protección en estaciones y servidores

Administración básica

- Alertas y actualizaciones

Antivirus

Telefónica del Perú S.A.A.
Página 47
Telefónica

e) Seguridad en las redes de comunicaciones:
"Firewalls" u otros (Cont.)

I. Actualización mediante tareas programadas

II. Actualización manual

Telefónica del Perú S.A.A.
Página 48
Telefónica

e) Seguridad en las redes de comunicaciones:

"Firewalls" u otros (Cont.)

- Sólo el personal de operadores y administradores autorizados por la naturaleza de sus funciones, tienen acceso a los archivos de programas y de datos.
- Las cuentas de ADMINISTRADOR de los sistemas operativos se encuentra en sobre cerrado y guardado en custodia en el Centro de cómputo. Existe un procedimiento de control de uso de estas cuentas.
- La información de los abonados es accesible mediante opciones de las aplicaciones, a las cuáles sólo tienen el acceso, las personas que lo requieren debido a las labores que realizan.

f) Control de personal que supervisa las comunicaciones

Salvaguarda de la seguridad de las Operaciones y Seguridad Física

- Existen controles preventivos, detectivos y correctivos tanto a niveles físicos, lógicos como administrativos.
- Los controles administrativos, comprenden por ejemplo la identificación de los empleados mediante el uso de carnets de identificación, prohibición de ingreso fuera de horas de trabajo, salvo autorización previa, etc.
- Los controles físicos comprenden la seguridad física mediante agentes de seguridad, doble puerta para el ingreso a los lugares críticos, sistemas de circuito cerrado de TV.
- Los controles lógicos se refieren a los controles para el ingreso a la operación de los equipos que contienen información crítica, como son las claves, tiempo de conexión, horario de conexión, etc.
- Existe un inventario, control de entrada y salida de equipos, cintas de "backup" y manejo de computadoras portátiles. De la misma manera existe un control de cambios y configuraciones de hardware y software, control de instalación de programas, sistemas antivirus, etc.
- El desecho de papelería así como el tratamiento de dispositivos de almacenamiento para la remanencia de datos es controlado mediante técnicas de destrucción y reutilización de recursos.

f) Control de personal que supervisa las comunicaciones
(Cont.)

Parte legal y ética

- Telefónica se preocupa por difundir permanentemente cuáles son los alcances de la salvaguarda del secreto de las telecomunicaciones y la protección de la información, así como los valores éticos.
- Los controles de seguridad son establecidos de manera uniforme para todos los integrantes de la empresa.
- El manejo de la evidencia ante problemas de seguridad está definido en los procedimientos internos.
- La empresa aplica mecanismos razonables de seguridad y protección de los datos y de la información personal, ante lo cual se ha dispuesto las siguientes medidas preventivas y correctivas según corresponde:
- **CLÁUSULA DE CONFIDENCIALIDAD:** Toda aquella persona que se integra a la empresa debe suscribir un contrato en el que se han incorporado las cláusulas de confidencialidad correspondientes las cuales obligan al trabajador a guardar total reserva de la información que maneja durante la vigencia del contrato y hasta 5 años de concluida su vigencia.

f) Control de personal que supervisa las comunicaciones
(Cont.)

CLÁUSULAS DE CONFIDENCIALIDAD DEL TRABAJADOR

- **OCTAVA.- EL (LA) TRABAJADOR(A)** se obliga a guardar total y absoluta reserva sobre todo tipo de información relacionada con las actividades de LA EMPRESA que no sean de conocimiento público incluidas la calidad, la capacidad y características de los equipos y procedimientos utilizados por ésta, la tecnología aplicada y en general, respecto a todo tipo de conocimiento a que hubiera tenido acceso El (LA) TRABAJADOR(A) por efecto de este contrato, quedando prohibido de utilizar dicha información y conocimiento para sí o para terceros. La obligación contenida en esta Cláusula regirá durante la vigencia del presente contrato e incluso hasta después de cinco (5) años de concluida su vigencia y su incumplimiento generarán las sanciones laborales correspondientes, de ser el caso, y una indemnización por los daños y perjuicios ocasionados.

f) Control de personal que supervisa las comunicaciones
(Cont.)

CLÁUSULAS DE CONFIDENCIALIDAD DEL TRABAJADOR

- DÉCIMA.- En caso que EL(LA) TRABAJADOR(A) tuviera acceso a información personal relativa a los abonados de los servicios públicos que presta TELEFÓNICA y/o la Red Pública de Telecomunicaciones, se obliga a guardar secreto de tal información, cumpliendo de este modo con el secreto de las telecomunicaciones que la Empresa está obligada a observar conforme lo exige la legislación vigente y a la normativa interna.
- CHARLAS Y CAMPAÑAS SOBRE SEGURIDAD DE LA INFORMACIÓN: Durante la permanencia de todo trabajador al interior de la empresa, el trabajador es expuesto a una serie de charlas y campañas de difusión respecto a la seguridad de la información. En ese sentido, durante la primera semana de haber ingresado a la empresa, todo trabajador asiste a una charla de inducción en la que se le dicta una conferencia referida a la "Seguridad de la información".

Nota.- Durante la vigencia de toda relación laboral, los trabajadores se encuentran sujetos a lo dispuesto por el Reglamento Interno de Trabajo el cual establece claramente la obligación de guardar total reserva de la información que maneja así como la prohibición de difundirla. El incumplimiento se sanciona con el despido.

f) Control de personal que supervisa las comunicaciones
(Cont.)

Reglamento Interno de Trabajo

- Artículo 15°.- Constituyen obligaciones de los trabajadores, las siguientes: (...) f) Guardar en todo momento el secreto profesional y mantener absoluta discreción en todo lo concerniente a las actividades de la empresa en general, y en particular, al movimiento de la dependencia en que desempeña sus labores.
- Artículo 19°.- Son prohibiciones para los trabajadores y objeto de sanciones disciplinarias, en caso de inobservancia, las siguientes: Divulgar fuera del ámbito de la empresa cualquier información o documentación de uso interno, especialmente la considerada como reservada, confidencial, estratégica, la que esté protegida por el secreto de las telecomunicaciones y la considerada como secreto industrial o comercial.

f) Control de personal que supervisa las comunicaciones
(Cont.)

Medidas disciplinarias por incumplimiento

Artículo 54º.- Cuando se trate de hechos relacionados a patrimonio, seguridad de la información y secreto de las telecomunicaciones se seguirá el procedimiento que regule para tal efecto las normativas de la empresa y/o las regulaciones de la materia.

Otras disposiciones relacionadas:

Artículo 11º.- La condición de trabajador, será incompatible, sin previa autorización expresa de la empresa, con el ejercicio de toda actividad propia o al servicio de terceros que se desarrolle dentro del horario de trabajo fijado por la empresa o produzca disminución en el rendimiento del trabajador. En ningún caso se autorizará la compatibilidad con trabajos o desempeño de cargos en entidades que fabriquen materiales o exploten servicios de telecomunicaciones o empresas que tengan contratada con la compañía la prestación de algún servicio de cualquier clase. La falta de solicitud previa y de autorización en su caso se considerará como falta grave.

Artículo 61º.- La empresa, en su calidad de propietario o titular del derecho de uso de los aparatos de cómputo que se encuentran en la empresa, está facultado para inspeccionar su contenido directa o indirectamente, así como copiar íntegramente la información que se encuentre dentro de los mismos sin requerir para ello autorización previa del trabajador. Queda terminantemente prohibida la conexión a los sistemas de comunicación de la empresa de cualquier aparato de cómputo de propiedad del trabajador, salvo que cuente con autorización expresa de la empresa. Asimismo, queda prohibido el retiro de información que se encuentre en los aparatos de cómputo de la empresa, sea a través de cualquier medio directo o indirecto.

g) Otros mecanismos de protección de la información

NUESTROS SERVICIOS



EVALUACIONES DE RIESGO



BASE DE DATOS DE PERSONAL CRÍTICO



CHARLAS



SUPERVISIÓN DE DESTRUCCIÓN DE DESECHOS DE OFICINA



INVESTIGACIONES ESPECIALES

CAMPAÑA PROTEGE LO QUE IMPORTA

**[PROTEGE]
LO QUE IMPORTA**

no ventiles la información que te confiamos

PROTEGE

g) Otros mecanismos de protección de la información (Cont.)

PROTECCIÓN DE LA INFORMACION EMPRESARIAL

Proporciona las directrices para garantizar la seguridad de la información, al constituir un activo estratégico imprescindible para la Empresa. Sensibiliza al personal en la valoración de la información que maneja, a fin de que realice conductas seguras

La política abarca a toda la información utilizada por Telefónica.

Es aplicable con carácter obligatorio a las distintas empresas del Grupo Telefónica

NUESTROS SERVICIOS

MEDIOS DE COMUNICACIÓN INTERNA



PRESS RELEASE



BOLETINES DE UNIDADES DE NEGOCIO



PANTALLAS SISTEMA VANTIVE

g) Otros mecanismos de protección de la información (Cont.)

MEDIDAS PARA PROTEGER LA INFORMACIÓN EMPRESARIAL

Técnicas	Evaluaciones técnicas para verificación de riesgos potenciales de la información física en los diferentes negocios
	Actividades de destrucción de desechos en los locales de Telefónica
Organizativas	Elaboración de nuevas normativas: Clasificación y tratamiento de la información
	Cumplimiento del proceso de destrucción de desechos en las oficinas locales
Recursos	Capacitación a los trabajadores del grupo Telefónica en medidas para proteger su información.
	Actualización permanente de la base de datos de personal Crítico de los Negocios
	Campañas de comunicación anual en medidas preventivas para proteger la información.
	Diseño de boletines Segurinet@s donde se imparten recomendaciones para proteger la información
	Empleo de canales informáticos para la transmisión de mensajes para difundir recomendaciones de protección de la información
	Empleo de Boletines de las diferentes Unidades de Negocio para difundir recomendaciones de protección de la información

5. Preocupación por recientes iniciativas regulatorias

- Recientes iniciativas regulatorias pueden comprometer el secreto de las telecomunicaciones y la seguridad de la información, por lo que sugerimos seriamente su reconsideración.
- Este es el caso del Texto Unico Ordenado de las Normas de Interconexión, que permitirían la interconexión en zonas rurales mediante simples líneas telefónicas (Res N° 043-2003-CD/OSIPTTEL) o que exigen que la empresa ponga a disposición de los concesionarios del servicio portador de larga distancia información sobre el tráfico generado a través de nuestras líneas fijas, incluyendo información que puede afectar a los abonados o usuarios (Res.N° 072-2003-CD/OSIPTTEL del 04.08.03)
- La reciente modificación del contrato de concesión de IDT (R.D. N° 536-2003-MTC/17 emitida por la Dirección General de Gestión de Telecomunicaciones) ha considerado como parte de su red una central de conmutación ubicada en New Jersey, lo que afecta la posibilidad de una adecuada supervisión de los procesos de conmutación por la autoridad peruana así como la obtención de información que registra la central.
- Los continuos pedidos de los CDR's (Call Data Register) de los usuarios en diferentes periodos y de servicios por parte de Osiptel.
- Por lo expuesto, sugerimos que todo proyecto normativo sea evaluado a la luz de potenciales afectaciones al secreto de las telecomunicaciones y la seguridad de la información.

Telefónica del Perú S.A.A. (Telefónica) ha desarrollado una serie de políticas y prácticas razonables para la salvaguarda del secreto de las telecomunicaciones y de la información en general, las que varían con el tiempo teniendo en cuenta las nuevas tecnologías que se implementan.

A pesar del esfuerzo desplegado y por lo compleja de la actividad no es posible garantizar una protección absoluta.

P/D. N° 015719



RuralTelecom

Calle 22 # 461 Corpac, San Borja
Teléfono: 475 0685 Fax: 475 1294

GG-0072-2004

Lima, 19 de febrero del 2004

Ministerio de Transportes y Comunicaciones
VICE MINISTRO DE TELECOMUNICACIONES
19 MAR. 2004
RECIBIDO
Hora: N° Hora: 15:30

M.T.C.
O.T.D.
Oficina de Control Documentario
19 MAR. 2004
RECIBIDO EN LA FECHA
Hora: Registrador:

Señores
Ministerio de Transportes y Comunicaciones
Av. 28 de Julio N° 800
Presente

Atención: **Dr. Juan Pacheco**
Viceministro de Telecomunicaciones

Referencia: Oposición a la renovación del plazo de concesión de Telefónica del Perú

Estimado Dr. Pacheco,

Tenemos a bien dirigirle la presente para saludarle e informarle que, mediante Resolución N° 112-2003-CD/OSIPTTEL de fecha 11 de diciembre del 2003, el OSIPTTEL emitió la Ampliación del Mandato de Interconexión entre nuestra empresa, Rural Telecom y Telefónica del Perú, en el cual se establecieron las condiciones económicas y los diferentes escenarios no contemplados en el Mandato de Interconexión N° 079-2002-CD/OSIPTTEL de fecha 13 de diciembre del 2002.

Luego de iniciar las reuniones pertinentes con Telefónica del Perú para ejecutar el citado mandato, fuimos informados por parte de dicha empresa de la supuesta existencia de una "Imposibilidad Técnica" en sus teléfonos públicos que impediría la utilización de monedas para realización de llamadas originadas en su red de TUP's con destino a la red de Rural Telecom, dado que sus teléfonos monederos no tienen la capacidad de programación de las tarifas fijadas por Rural Telecom.

Siendo el Mandato de cumplimiento obligatorio por las partes y no pudiendo ejecutarse debido a la posición de Telefónica del Perú de no cumplir con la totalidad de los escenarios señalados en el Mandato, es que nos vemos en la obligación de transmitirle esta situación e informarles nuestra oposición a la renovación del plazo de concesión a Telefónica del Perú.

Ministerio de Transportes y Comunicaciones
DIRECCION GENERAL DE GESTION
DE TELECOMUNICACIONES
19 MAR. 2004
RECIBIDO

Ministerio de Transportes y Comunicaciones
19 MAR 2004

Esta actitud de Telefónica de incumplir un mandato emitido por el organismo regulador el cual afecta directamente a más 900 poblados rurales con una población estimada de 800,00 mil habitantes, los cuales son los más necesitados de comunicación para su desarrollo, es realmente muy grave y demuestra que dicha empresa no cumple con las disposiciones legales vigentes.

Por los motivos señalados es que reiteramos nuestra oposición a la renovación del plazo de concesión a Telefónica del Perú.

Sin otro en particular, quedamos de usted.

Atentamente,



Franco Gianoli Hanke

Asesor Legal

Rural Telecom S.A.C

cc. Paul Phumpiu – Gerente de Políticas Regulatorias, OSIPTEL

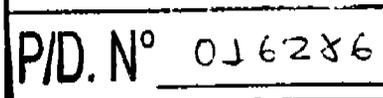
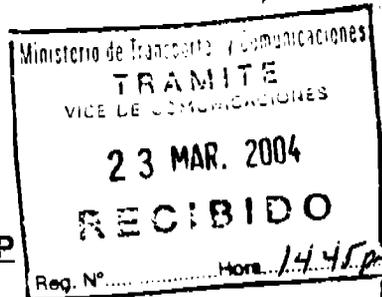


Defensoría del Pueblo

OFICIO N° 038 2004-DP-ASP

Señor
ANTONIO PACHECO ROMANÍ
Vice-Ministro de Comunicaciones
Ministerio de Transportes y Comunicaciones
Av. 28 de Julio N° 800
Lima.-

Lima,



Ref.: Comentarios y Objeciones respecto a la Solicitud de Renovación del Contrato de Concesión de Telefónica del Perú.

De mi consideración:

Es grato dirigirme a usted para saludarlo y remitirle el Informe de la Defensoría del Pueblo en relación a la solicitud de renovación del contrato de concesión de Telefónica del Perú S.A.A.

Al respecto, nuestro informe señala que no obstante cualquier incumplimiento de la empresa concesionaria que OSIPTEL pudiera señalar respecto a determinadas obligaciones contractuales, lo más destacado en relación a la renovación del contrato son determinados vicios de origen en sus disposiciones contractuales.

En efecto, nuestro informe pone de relieve cómo la renovación del contrato no es un mecanismo voluntario para el Estado Peruano, el cual se ha obligado a conceder la prórroga hasta por veinte años adicionales si no demuestra el incumplimiento reiterado de la empresa o que ésta no podrá cumplir con sus obligaciones en el futuro. En la práctica se trata de una prórroga automática que el Estado no puede impedir, salvo en casos de grave incumplimiento de la concesionaria.

Ello significa que bajo la apariencia de un mecanismo de renovación voluntaria de un contrato de veinte años de duración, se encubrió un plazo de 40 años forzosos para el Estado- mayor al máximo legal de 20 años establecido por el artículo 56° del T.U.O. de la Ley de Telecomunicaciones-, lo que perjudica el



Defensoría del Pueblo

interés público que la ley quiere proteger al establecer un plazo máximo para las concesiones de servicios públicos de telecomunicaciones, prorrogable por libre acuerdo entre las partes.

Sin otro particular, expreso a usted mi mayor consideración,

Atentamente,



WILLIAM POSTIGO DE LA MOTTA

Adjunto al Defensor del Pueblo
para los Servicios Públicos (e)

/af.

SOLICITUD DE RENOVACIÓN DEL CONTRATO DE CONCESIÓN DE TELEFÓNICA DEL PERÚ

INFORME

1. Plazo de la Concesión.-

Quando se firmó el contrato de concesión con ENTEL Perú, S.A. y CPT S.A. (hoy Telefónica del Perú S.A.A.), el plazo de la concesión debía vencer a los 20 años de la fecha efectiva de vigencia de la concesión (30 días hábiles siguientes al 16.05.94), es decir, a fines de junio de 2014.

En el año 1999 las partes contractuales renovaron el contrato por 5 años más, debiendo concluir a fines de junio de 2019.

2. Renovación Gradual del plazo de la Concesión.-

Continuando con la opción de Telefónica por la renovación gradual de la concesión, este año debe decidirse su renovación por 5 años más, en cuyo caso el contrato vencerá a fines de junio de 2024. Las sucesivas renovaciones no pueden sumar más de 20 años adicionales a los 20 años del período inicial.

Con fecha 22.12.2003, Telefónica ha solicitado al MTC la renovación gradual por 5 años del plazo para la prestación de los servicios materia de la concesión: (i) Portador Local, Telefónico Local, Telefónico de Larga Distancia Nacional e Internacional y Portador de Larga Distancia Nacional e Internacional en la República del Perú, y (ii) Portador Local y Telefónico Local en el departamento de Lima y la Provincia constitucional del Callao.

3. Comentarios u Objeciones.-

Las personas con interés legítimo podrán formular por escrito sus comentarios u objeciones a la solicitud presentada, dentro del plazo de 60 días calendario computados a partir de la fecha de publicación del aviso

(20.01.2004) en El Peruano, es decir, hasta el sábado 20 de marzo de 2004. El MTC ha otorgado el plazo mayor, ya que conforme al contrato de concesión el plazo debe ser entre 30 y 60 días calendario computados a partir de la publicación del aviso.

El contrato no define lo que debe entenderse por interés legítimo. Podría considerarse como un envío al artículo VI del Título Preliminar del Código Civil que señala que para ejercitar una acción es necesario tener legítimo interés económico o moral, lo cual puede ser interpretado inadmisiblemente de un modo restrictivo de los derechos de los usuarios o potenciales usuarios del servicio.

Los comentarios u objeciones deben presentarse en la Dirección General de Telecomunicaciones (Av. 28 de Julio N° 800, Lima. Telefax (511) 4336888, correo electrónico: serviciospublicosdggg@mtc.gob.pe).

4. Notificación a OSIPTEL.-

Conforme al contrato de concesión el MTC, además de publicar el aviso, debe notificar a Telefónica y a OSIPTEL.

Dentro de un plazo de 60 días calendario de notificado, OSIPTEL debe presentar al MTC y a Telefónica el INFORME DE EVALUACIÓN previsto en el contrato de concesión. El MTC ha otorgado a OSIPTEL el plazo mayor ya que conforme al contrato éste debe ser entre 30 y 60 días calendario desde la notificación.

5. Audiencia Pública.-

Conforme al acápite (a) de la Sección 4.03 del Contrato de Concesión, el aviso publicado en El Peruano (20.01.04) debía señalar la fecha, lugar y hora en la que se llevará a cabo una audiencia pública, no pudiendo dicha fecha ser anterior a 30 ni posterior a 45 días calendario a contar desde el vencimiento del plazo para la presentación de comentarios u objeciones. El MTC NO HA SEÑALADO LA FECHA, EL LUGAR, NI LA HORA. En el aviso el MTC se ha limitado a señalar lo indicado en el contrato respecto a

que convocará a una Audiencia Pública dentro de un plazo no menor de 30 ni mayor de 45 días calendario contados desde el vencimiento del plazo para la presentación de comentarios u objeciones por escrito (20.03.04).

El acápite (a) de la Sección 4.03 del contrato señala que en la audiencia, la empresa, OSIPTEL y cualquier persona con un interés legítimo podrán formular comentarios u objeciones a la solicitud de renovación. El acápite (c) de dicha Sección 4.03 declara que en el plazo establecido en el aviso y en la notificación emitida por el MTC, el MTC citará a una audiencia pública en la cual la empresa, OSIPTEL y las personas con un interés legítimo que hayan presentado comentarios u objeciones por escrito considerados relevantes por el MTC, tendrán el derecho a ser escuchados. Estas limitaciones a la participación en Audiencia colisionan con ciertos derechos reconocidos en la Constitución, como son el de participar en la vida económica de la Nación y el que obliga al Estado a defender el derecho de los consumidores y usuarios garantizando el derecho a la información sobre los bienes y servicios que se encuentran a su disposición en el mercado, debiendo prevalecer la norma constitucional.

6. Aspectos Materia de Evaluación.-

Los aspectos relevantes que serán evaluados por el MTC para una decisión final, y que deben ser considerados por quienes presenten comentarios y objeciones y participen en la audiencia pública, son los que conforme al contrato de concesión deben ser materia de evaluación por OSIPTEL. Estos son:

- a) Cumplimiento de sus obligaciones establecidas en las Cláusulas 6 (Derechos, Tasas y Canon), 8 (Obligaciones de la Empresa Concesionaria) y 9 (Régimen Tarifario General) del Contrato.
- b) Cumplimiento de las reglas de interconexión establecidas en la Cláusula 10 del Contrato.
- c) Cumplimiento de las reglas de competencia establecidas en la Cláusula 11 del Contrato.
- d) Cumplimiento de los mandatos y reglamentos que han sido debidamente emitidos por OSIPTEL, y,

- e) **Haber prestado sus servicios públicos de telecomunicaciones y llevado sus negocios conforme a las leyes del Perú.**

No obstante la importancia que pudiera tener cualquier incumplimiento contractual considerado en sí mismo que OSIPTEL pudiera señalar en su informe de evaluación, lo más grave en relación a la renovación del contrato son los vicios de sus disposiciones contractuales, tal como señalamos a continuación.

7. Decisión del MTC.-

Conforme a lo convenido en el contrato de concesión, dentro de los 30 días hábiles siguientes a la fecha de celebración de la Audiencia, el MTC resolverá la solicitud de Telefónica.

El MTC puede decidir de tres modos distintos:

- a) **Renovar el plazo por 5 años adicionales, siempre que la empresa hubiera cumplido durante los 5 años precedentes con las obligaciones materia del INFORME DE EVALUACIÓN del OSIPTEL.**
- b) **Renovar el plazo por un período menor de 5 años adicionales si la empresa hubiera incumplido con sus obligaciones en un grado tal que no se justifique la denegatoria de renovación.**
- c) **No renovar el plazo debido al incumplimiento reiterado de la empresa de sus obligaciones contractuales o de la existencia de suficientes indicios que permitan afirmar que no podrá cumplirlos en el futuro, salvo que la empresa pueda demostrar que es errónea tal determinación de hechos o de los presupuestos de base de la decisión.**

Como puede apreciarse, el Estado Peruano se ha autolimitado de tal forma que si no demuestra el incumplimiento reiterado de la empresa o que no podrá cumplir con sus obligaciones en el futuro, debe seguir renovando el contrato de concesión hasta por 20 años adicionales. Con ello se desnaturaliza el concepto de "renovación" de un contrato y se establece en la práctica una prórroga automática que no puede impedir el Estado Peruano, sino en casos de incumplimiento reiterado de la concesionaria.

En los contratos suelen existir y son aceptables las reglas sobre resolución de los mismos por incumplimiento de alguna de las partes antes de la terminación del plazo de vigencia del contrato. Estas reglas son distintas a otorgar a una de las partes un derecho de renovación indefinida del contrato mientras no exista incumplimiento del mismo. Los contratos de concesión, así como los de servicios y los de arrendamiento, son por definición contratos temporales que las partes pueden renovar mediante nuevos acuerdos. Algunos contratos –en especial algunos de derecho público– están sujetos a plazos máximos (como son los de concesión de telecomunicaciones que no deben pasar los 20 años conforme al artículo 56 del T.U.O. de la Ley de Telecomunicaciones), que pueden ser renovados por libre acuerdo de las partes. Lo contrario, forzar a una de las partes obstaculizándole las vías para la no renovación, equivale al otorgamiento de un plazo mayor a favor de la otra parte (y en este caso a duplicar el plazo máximo permitido por ley), lo que constituiría un fraude a la Ley de Telecomunicaciones, de fecha anterior al contrato-ley celebrado con ENTEL Perú S.A. y CPT S.A., hoy Telefónica.

La “renovación” de un contrato implica un nuevo acuerdo de voluntades autónomas. Tan es así que cabe renovar un contrato bajo las mismas estipulaciones o modificando las cláusulas originales. Los mecanismos de renovación acordados pueden establecer procedimientos y criterios para la renovación, pero no pueden anular la voluntad autónoma de las partes para llegar a un nuevo acuerdo, pues se estaría desnaturalizando la “renovación” y haciendo que el contrato se haya celebrado originalmente por un plazo mayor de vigencia.

Esta disposición contractual es susceptible de un mayor análisis respecto a su nulidad y podría ser jurisdiccionalmente declarada contraria a Derecho ya que bajo la apariencia de un mecanismo de renovación de un contrato de veinte años de duración, se encubre un plazo mayor concedido en forma ilegítima, lo que perjudica el interés público que la ley quiere proteger al establecer un plazo máximo de 20 años para las concesiones de servicios públicos de telecomunicaciones.

La nulidad de la disposición contractual acarrearía la nulidad de la “renovación” concedida en el año 1999, con lo que el contrato podría estar

finalizando a fines de junio de 2014, salvo una renegociación del mismo que resuelva mediante acuerdo de ambas partes el problema de la vigencia de la concesión suscitado por estas cláusulas contrarias al orden público nacional.

8. Notificación a Telefónica.-

El MTC, antes de emitir la Resolución respecto a la improcedencia de la renovación, notificará a Telefónica los hechos o las bases que sustentan su decisión, a fin que dentro de un plazo de 15 días calendario a partir de la notificación, la concesionaria aporte las pruebas adicionales que estime necesarias.

Esta disposición contractual conduce el tema de la renovación del contrato por el camino de la controversia con el Estado, cuando ello debería ser una decisión autónoma del Estado, mediante la cual llega a un acuerdo con la parte contraria. El Estado renuncia a su derecho a no seguir vinculado contractualmente a una empresa al término del plazo por el que se obligó – y que constituye el plazo máximo de ley-, aceptando, de otro lado, que ese derecho sea discutido en un arbitraje de la Cámara de Comercio.

En nuestra opinión, esta disposición también es contraria al orden público nacional al constituir un modo de contravenir la Ley de Telecomunicaciones.



P/D. N° 015934

ASOCIACIÓN DE CONSUMIDORES Y USUARIOS

Lima, 19 de marzo de 2004

Señor
José Javier Ortiz Rivera
Ministro de Transportes y Comunicaciones.
Presente.

Ministerio de Transportes y Comunicaciones
VICE DUEÑO DE LA INSTITUCIÓN
22 03. 2004
RECIBIDO
Reg. N° hora 9:30 AM

M.T.C.
O.T.D.
Oficina de Control Documentario
22 MAR 2004
RECIBIDO EN LA FECHA
Hora.....Registrador.....

De nuestra consideración:

Es muy grato dirigimos a usted con relación a la publicación en el Diario Oficial "El Peruano", de fecha 20 de enero del 2004, sobre la solicitud de renovación del contrato de concesión de Telefónica del Perú S.A.A. (TdP).

Sobre el particular, presentamos nuestra objeción a que se de procedencia a dicha solicitud, ya que TdP no ha cumplido con sus obligaciones establecidas en sus respectivos contratos de concesión:

En efecto, los contratos de concesión establecen claramente que, para que proceda la solicitud de Renovación, TdP debe haber cumplido las obligaciones establecidas en las Cláusulas 6,8,9,10 y 11; además de cumplir con los mandatos y reglamentos emitidos por OSIPTEL y llevar sus negocios conforme a las leyes del Perú.

ACYU considera que TdP ha incurrido en una larga lista de incumplimientos referidos a las Cláusulas antes citadas. En efecto, de acuerdo a datos que pueden constatarse en OSIPTEL, del total de denuncias presentadas ante ésta Institución, el 98.5% han sido contra TdP. De este total de casos, el 81% se habrían declarado fundados por infracciones a **normas relevantes**. Se consideran normas relevantes aquellos que están contenidos en el Contrato de Concesión o están referidos a faltas muy graves en el Régimen Sancionatorio de la Ley de Telecomunicaciones y su Reglamento.

De éste universo, el 47% corresponderían a transgresiones a la Cláusula 8 del Contrato de Concesión, el 7% por transgresiones a la Cláusula 9, el 4% por transgresiones a la Cláusula 10, el 35% por transgresiones a la Cláusula 11 y el 7% por transgresiones a la Cláusula 17.

Nótese que la Cláusula 8 referida a atenciones de reclamos de usuarios es la más transgredida y que le sigue las transgresiones a la Cláusula 11 que tiene que ver con brindar facilidades para supervisión y cumplimiento de OSIPTEL.

Estas sanciones han merecido multas por encima de los S/. 2'000,000.00, que a la larga pagamos los usuarios junto a las altas tarifas que nos impone un monopolio.

En cuanto a denuncias de parte de los usuarios, en el periodo comprendido entre los años 1995 a 2002, TdP habría sido denunciada en 703,266 oportunidades en primera instancia y ante OSIPTEL en 55,556 oportunidades, de las cuales se han declarado fundadas 24,431, lo que equivale a que el 44% de las denuncias y reclamos interpuestos se declarararan fundadas.

Sumando ambas cifras se tiene un total de 758,822 reclamos contra TdP. Esta cifra es sumamente preocupante, ya que equivale a que casi la mitad de los usuarios que tiene

Calle General Suárez N° 1226, Miraflores. Tl: 441-5772
E-mail: hilerena@infonegocio.net.pe

Ministerio de Transportes y Comunicaciones

FORO GENERAL DE GESTIÓN DE TELECOMUNICACIONES

24 MAR 2004

RECIBIDO

Hora: 11:55 Reg: 2005



ASOCIACIÓN DE CONSUMIDORES Y USUARIOS

TdP (1'600,000 líneas en servicio), se han quejado por lo menos una vez en el quinquenio pasado.

Entre 1994 a 1999 la cantidad de quejas ante el TRASU de OSIPTEL sólo fue de 10,639, lo que equivale a que con relación a la actual cifra de reclamos, para este quinquenio se habría producido un incremento de más de 430%.

Esta realidad es el resultado del incumplimiento de las obligaciones contractuales de TdP. A todas luces no existe ninguna empresa que tenga ese record, con el agravante que tampoco existe un compromiso serio por parte de ésta empresa para poner coto a este muy álgido problema que atinge a los usuarios.

ACYU considera que, junto a éste, existen muchos otros elementos sumamente importantes que deberían dar lugar a que el MTC adopte la decisión de no aprobar la solicitud de ampliación del plazo de concesión de TdP.

En tal sentido, mucho le agradeceremos tener en cuenta esta nuestra posición al momento de realizar el análisis correspondiente.

Quedamos a su disposición para ampliar y exponer con más fundamento este nuestro planteamiento.

Atentamente,

Presidente



Sindicato Unitario de Trabajadores de Telefónica del Perú S.A.

Av. Uruguay 335

FUNDADO EL 23 DE SEPTIEMBRE DE 1931

RECONOCIDO POR R.M. N° 57 DEL 8 DE OCTUBRE DE 1940

Ministerio de Transportes y Comunicaciones
SECRETARÍA DE COMUNICACIONES

Teléfono: 428-9965 ext. 433-7612 e-mail: suttp@suttp.org.pe

P/D. N° 014004

Ministerio de Transportes y Comunicaciones
TRAMITE
VICE DE COMUNICACIONES
11 MAR. 2004 Lima - Perú
RECIBIDO
Reg. N° Hora 15:40 M

S.G. 461

12 MAR 2004

REG: 603 FIRMA: [Signature]
FOLIOS: HORA: 10:30 am
RECIBIDO

Lima, 11 de marzo del 2004

Excelentísimo señor doctor
Carlos Ferrero Costa
Presidente del Consejo de Ministros
PRESENTE.

M.T.C.
O.T.D.
Oficina de Control Documentario
11 MAR 2004
RECIBIDO EN LA FECHA
Hora.....Registrador.....

De nuestra consideración:

Reciba usted el saludo del Sindicato Unitario de Trabajadores de Telefónica del Perú, deseándole grandes éxitos en su gestión por el bien de la nación peruana.

La presente tiene por finalidad solicitar se tome en cuenta la opinión de los trabajadores en la prorroga del Contrato de Concesión entre el Estado Peruano y Telefónica, hecho que, según los medios de comunicación, será firmada en los próximos meses.

Como es de conocimiento público, cuando se privatizó las telecomunicaciones en el Perú, Telefónica fue el ganador a través de una licitación Internacional. Como ganador se comprometió a que por el lapso de 5 años no despediría trabajadores, salvo por programas de renuncia voluntaria aceptado por las partes.

Dicha cláusula de seguridad en el empleo fue parte del contrato de compra venta de las acciones de la Compañía Peruana de Teléfonos S.A. por parte de Telefónica Internacional de España.

Telefónica incumplió dicha cláusula y la modificó por acuerdo de Junta de Accionistas, conminando a los trabajadores a renunciar y los que no aceptaron fueron despedidos. Esta acción Obligó al Sindicato Unitario de Trabajadores de Telefónica del Perú a entablar acciones de amparo por incumplimiento de la cláusula de seguridad en el empleo y por la reposición de los trabajadores despedidos, obteniéndose sentencia favorable que ordenó a Telefónica que no pueda modificar la cláusula de seguridad en el empleo y al mismo tiempo ordenaba la reposición de los trabajadores despedidos; una clara evidencia del incumplimiento del contrato por parte de la empresa.

Sin embargo, el contrato de Gestión y Transferencia de Tecnología obliga a Telefónica del Perú pagarle a Telefónica



Sindicato Unitario de Trabajadores de Telefónica del Perú S.A.

FUNDADO EL 23 DE SETIEMBRE DE 1931

RECONOCIDO POR R.M. Nº 57 DEL 8 DE OCTUBRE DE 1940

Av. Uruguay 335

Tel.: 428-9965 - Telefax: 433-7612 e-mail: suttp@suttp.org.pe

Lima - Perú

Internacional de España el 9% de la utilidad operativa, el 1% de la facturación antes del impuesto, que el acumulado desde el año 1994 a la fecha es de aproximadamente de 1,000 millones de dólares sólo por el contrato de gestión, contrato que se cumple estrictamente.

Por otro lado, cuando Telefónica adquirió los derechos de operación de las telecomunicaciones era una unidad Empresarial, es decir brindaba todos los servicios. A la fecha se ha reestructurado administrativa y operativamente, convirtiéndose en un **grupo económico**, al haber independizado algunas áreas operativas para que sean empresas autónomas llamadas comúnmente filiales, y en las que obligó a los trabajadores a renunciar y pasar a dichas filiales con nuevas condiciones económicas y de trabajo. Esta reestructuración se complementa con la tercerización de los principales servicios de la actividad regular de Telefónica, como son las instalaciones y mantenimiento, dándole esta labor a contratistas principalmente españolas que son meras intermediarias entre sub - contratistas peruanos, los mismos que después contratan a trabajadores que son los que finalmente ejecutan la labor a través de un sistema de labor al destajo sin derechos ni beneficios.

Esta nefasta política continúa acentuándose en Telefónica con el claro propósito de seguir despidiendo trabajadores.

Por ello, señor Primer Ministro, solicitamos se considere dentro de la prorrogación de la concesión a Telefónica la cláusula sexta del contrato de compra venta, emisión, suscripción y entrega de acciones el mismo que da estabilidad a los trabajadores, la cual debe ser vigente hasta la finalización de la concesión otorgada a Telefónica.

Por otro lado, cuando Telefónica solo tenía el 35% de las acciones de ex - CPTSA y ex - Entel Perú, por ello se le otorgó el contrato de gestión y transferencia tecnológica, sin embargo ahora Telefónica posee el 98% del accionariado, es decir la dueña absoluta del negocio, consideramos que dicha cláusula debe ser eliminada.

Por todo ello, señor Primer Ministro, solicitamos que se tomen en cuenta nuestras opiniones para la prorrogación del Contrato de Concesión a Telefónica.

Finalmente, sería prudente llevar a cabo una auditoría Técnico Financiera por el Estado Peruano y ver si Telefónica cumplió con todas sus obligaciones y con todos los artículos del contrato.



Sindicato Unitario de Trabajadores de Telefónica del Perú S.A.

FUNDADO EL 23 DE SETIEMBRE DE 1931

RECONOCIDO POR R.M. Nº 57 DEL 8 DE OCTUBRE DE 1940

Av. Uruguay 335

Telf.: 428-9965 - Telefax: 433-7612 e-mail: suttp@suttp.org.pe

Lima - Perú

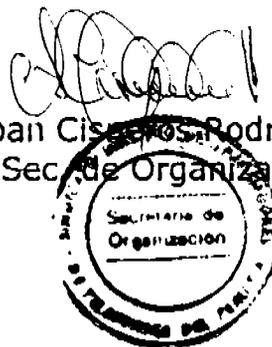
Seguros de la atención a la presente solicitamos a Ud. una entrevista para dar nuestras opiniones referente a la prórroga del contrato de concesión a Telefónica, quedamos de usted.

Atentamente,

Luis López Chau Nava
Secretario General



Esteban Cisneros Rodríguez
Sec. de Organización



Helf Vargas Méndez
Secretario de Defensa



C.C. Sr. Ing° José Ortiz Rivera
Ministro de Transportes y Comunicaciones

C.C. Sr. Edwin San Román Zubizarreta
Presidente de OSIPTEL

C.C. Sr. Doctor Javier Neves Mújica
Ministro de Trabajo y Promoción del Empleo

LLCH/nzd.

DGGT Servicios Publicos

De: Domingo Caceres [ylesase1@congreso.gob.pe]
Enviado: viernes 26 de marzo de 2004 10:08
Para: serviciospublicosdggg@mtc.gob.pe
Asunto: observaciones



OBSERVACIONES.do

Señores, mediante el presente presento las observaciones formuladas por el Congresista Yonhy Lescano Ancieta respecto la solicitud de renovación

del plazo de concesión de telefonica del Perú.
hago presente que este documento se presento a OSIPTEL



Congreso de la República

SUMILLA: PRESENTA OBSERVACIONES

SEÑOR PRESIDENTE MINSTRO DE TRANSPORTES Y COMUNICACIONES

YONHY LESCANO ANCIETA, identificado con D.N.I. 01211014, Congresista de la República, como representante del pueblo y a nombre propio, señalando como domicilio legal el Congreso de la República y como domicilio procesal la Av. Abancay N° 251, me apersono en el proceso de renovación de Contrato de Concesión de Telefónica del Perú, a fin de expresar lo siguiente:

En fecha 22 de enero de 2003, el Ministerio de Transportes y Comunicaciones ha publicado la solicitud de Telefónica del Perú S.A.A. para la renovación gradual del plazo de concesión, al amparo de lo dispuesto por la cláusula cuarta del Contrato de concesión con CPT S.A. ENTEL PERU S.A. (Hoy Telefónica del Perú), aprobado por lo D.S. 011- 94-TCC, y teniendo "LEGITIMO INTERES" presento las siguientes Observaciones:

INCUMPLIMIENTO DE OBLIGACIONES CONTRACTUALES DE TdeP.-

Conforme a lo dispuesto por la cuarta cláusula del Contrato, para que la renovación del contrato proceda se deberá verificar el cumplimiento de las obligaciones contractuales contenidas en las cláusulas 6, 8 y 9, así como el cumplimiento de las reglas de interconexión establecidas en la cláusula 10 y las reglas de competencia a las que se refiere la cláusula 11, por lo que debemos manifestar lo siguiente:

1. Respecto del cumplimiento del pago de derechos, tasas y canon, el Ministerio de Transporte y Comunicaciones deberá informar a la población en forma



Congreso de la República

documentada si la Empresa TdeP ha cumplido con el pago puntual e integro de sus obligaciones, observando las formalidades de ley.

2. No se ha cumplido con lo dispuesto por el artículo 8.06 del contrato, respecto a las obligaciones de expansión, puesto como se establece el en anexo 2, todos los centros poblados con mas de 500 habitantes debieron lograr una densidad de por lo menos un teléfono público, por cada 500 personas; y si bien los cuadros que OSIPTEL ha presentado respecto de expansión telefónica rural muestran que existe una densidad de 6.8 teléfonos por cada 100 personas, en la realidad se puede constatar que en poblaciones como las de la sierra no existen teléfonos en distritos (mucho menos en centros poblados), puesto que es por todos conocido que el número de teléfonos fijos que era de dos millones, ahora es de un millón y medio aproximadamente, debido al elevado costo que significa para el usuario. Es decir que lejos de expandir el servicio, se ha reducido.

3. TdeP no ha cumplido con la cláusula 8.10 sobre la salvaguarda de secretos de telecomunicaciones, puesto que se ha visto involucrada en los hechos de interceptación telefónica (chuponeo) durante el régimen de Alberto Fujimori; de los que inclusive se ha desprendido la denuncia N° 007-2002 que el fiscal especial Oscar Zevallos Palomino presentó a los juzgados anticorrupción contra Vela Martínez y Páucar Carvajal, por delitos contra la libertad, en la modalidad de violación del secreto de las comunicaciones contra las siguientes personas:

José Ramón Vela Martínez - Gerente General de Telefónica del Perú

Antonio Páucar Carvajal - Ex Gerente Gral. de CPT y directivo de Telefónica

Jorge Fontalvo Romero - Jefe de control-Sistema de Seguridad de Telefónica



Congreso de la República

Miguel Corbetto Rodríguez - Jefe del Departamento de Operaciones de Seguridad

Luis Enrique Cuevas Díaz - Gerente de Seguridad y Protección de Telefónica

Rosario Ballón Arias - Secretaria de Telefónica

Víctor Capuñay Ruiz - Trabajador Telefónica

Juan Vega Chumbiauca - Trabajador Telefónica

4. TdeP no ha cumplido su obligación de cooperación de interconexión establecida en las cláusulas 10 10.02. del contrato, puesto que en reiteradas oportunidades ha impedido la interconexión de otras empresas como TELEANDINA S.A.A., NORTEK COMMUNICATIONS S.A.C., AT&T y TIM, tal como se acredita con los reclamos que estas empresas han presentado al organismo regulador y a la Comisión de Defensa del Consumidor del Congreso de la República.
5. **No** se ha cumplido con las reglas de competencia establecidas en la cláusula 11, pues conforme se tiene de la realidad e inclusive de lo expuesto por la sentencia recaída en el expediente 005-2003-AI/TC, sí existe un monopolio y TdeP no ha sido eficientemente supervisada.
6. Existen litigios Judiciales pendientes respecto del Monopolio que Telefónica del Perú ha venido ejerciendo en función al contrato suscrito con el Estado, como el que se inició ante la Primera Sala Contencioso Administrativo, signado con el N° 1299-2001, en el que en primera instancia se ha determinado de forma contundente que sí existe un monopolio en el servicio de telefonía.
7. Telefónica del Perú, ha incumplido el contrato al haber realizado actos de interferencia maliciosa de interconexión, hecho que es de conocimiento de



Congreso de la República

OSIPTEL, puesto que dichos reclamos se han presentado ante el citado Organismo Regulador, como es el caso presentado por NORTEK COMMUNATIONS S.A.C. en el expediente N° 004-2003

8. TdeP ha realizado subsidios cruzados con la aprobación de planes tarifarios pese a que el contrato lo prohíbe.
9. TdeP se viene negando a cumplir LOS MANDATOS y reglamentos que han sido debidamente emitidos por OSIPTEL, puesto que como es de conocimiento público, el año 2001 OSIPTEL calculó el Factor de Productividad otorgándole un valor de 6%. Sin embargo TdeP no estuvo de acuerdo pues considera que el valor es de 3.8%, y con la finalidad de DESACATAR el mandato de OSIPTEL, ha iniciado un PROCEDIMIENTO DE ARBITRAJE, pese a ser conocedor de que OSIPTEL "NO ES PARTE DEL CONTRATO" además que por su función es un ORGANISMO REGULADOR, por lo que sus Resoluciones son actos de derecho público, por lo tanto su impugnación debe realizarse ante el Poder Judicial.
10. La sola presentación ante el Tribunal Fiscal del procedimiento de Arbitraje antes referido, demuestra que TdP considera a OSIPTEL como PARTE del Contrato y no Organismo Regulador, por tanto no acata ni obedece las disposiciones que este emita sino que pretende negociarlas, por lo que se está vulnerando lo dispuesto por la cláusula 4.03.b.iv) del Contrato.

POR LO EXPUESTO:

A usted solicito se tenga en cuenta lo manifestado y se observe la solicitud de renovación del Contrato.

Lima, 15 de marzo de 2004

4



Congreso de la República