



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

Asunción, 7 de noviembre de 2013

VISTO: Que la Dirección de Informática, a través del Departamento de Seguridad Informática, tiene la responsabilidad del establecimiento y aplicación de las políticas de Seguridad Informática y Comunicaciones del Ministerio de Relaciones Exteriores; y

CONSIDERANDO:

Que resulta necesario tener en cuenta el avance y desarrollo en Tecnologías de Información y Comunicación (TICs.), para resolver el Servicio de Transmisión y Comunicación de Datos de la Red del Ministerio de Relaciones Exteriores, así como la suscripción de distintos acuerdos para la protección de la información que se genera en esta Secretaría de Estado, por lo cual es fundamental arbitrar los medios para lograr un mejor aprovechamiento y administración de ese recurso y activo de la Institución.

Que ante la generalización del uso de herramientas TICs para el desarrollo y cumplimiento de las actividades a cargo de las distintas Representaciones Diplomáticas y dependencias dentro del Ministerio de Relaciones Exteriores, y la proyección de ese uso, que puede visualizarse a partir de la demanda que actualmente genera la Función Pública, la Dirección de Informática ha considerado apropiado reglar su uso en este momento por diversas razones, entre las que puede citarse la sistematización de los servicios institucionales.

Que como consecuencia de las políticas de modernización del Estado impulsadas por el Gobierno Nacional, las reformas tendientes a implementar el Gobierno Electrónico y el uso de elementos TICs., cada vez más funcionarios del Ministerio de Relaciones Exteriores tendrán acceso al uso de las Tecnologías de la Información y las Comunicaciones, lo que amerita el dictado de normas y procedimientos para su mejor uso.

Que en este sentido y por las características del uso del software licenciado y libre, el Ministerio de Relaciones Exteriores debe establecer un marco normativo que defina el uso permitido, el uso aceptable, el uso indebido, el uso prohibido y las responsabilidades, para evitar un uso que resulte violatorio y perjudicial para sus funcionarios o para la institución.

Que en el marco de reglas claras y precisas que determinen un uso permitido y prohibido de los recursos TICs., es posible autorizar ciertos usos personales que tengan por finalidad aumentar la calidad del trabajo y ayudar a la Institución a retener a funcionarios calificados.

Que la introducción de este tipo de normativa posibilitará avanzar en la implementación de políticas de seguridad, contingencia y uso de hardware y software.

No _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Frutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

-2-

Que en virtud de las proyecciones establecidas por la Dirección de Informática para las futuras actualizaciones o nuevas instalaciones de las TICs.

Que el Ministerio de Relaciones Exteriores está impulsando con diferentes Instituciones Públicas un Equipo de Respuesta ante Incidentes Informáticos (Csirt), principalmente para el desarrollo de uso consiente de elementos informáticos de hardware y software, acuerdos internacionales para el desarrollo de una estrategia interamericana integral de seguridad para combatir amenazas cibernéticas con los Estados miembros de Organización de Estados Americanos (OEA), con el objeto de crear una cultura de Seguridad Cibernética.

Que la implementación de esta política brindará a la Institución la posibilidad de generar mecanismos de seguridad de la información generada para alcanzar negociaciones con diferentes organismos nacionales e internacionales.

Que la normativa propuesta ha sido incorporada tanto en el ámbito privado como en el público, en la legislación de otros países, con positiva repercusión, pues han permitido minimizar los riesgos en el uso de Redes de Datos, evitando la instalación de sistemas o software no autorizados, impidiendo la incorporación voluntaria o involuntaria de virus o sistemas dañinos, peligrosos, o que generen responsabilidad por su uso no autorizado.

Que en su redacción y corrección han participado la Secretaria General y la Dirección Informática y que por Dictamen VMAAT/DAL/N° 216/13 del 22 de agosto de 2013, la Dirección de Asuntos Legales manifiesta que no pone objeción de fondo ni forma para que este proceso siga su curso a través de los canales pertinentes, a los efectos su formalización mediante la suscripción de la respectiva Resolución por parte del Señor Ministro de Relaciones Exteriores.

Que la presente medida se dicta en uso de las facultades conferidas por la Ley Orgánica del Ministerio de Relaciones Exteriores.

Nº _____

ES COPIA

(FDO): Eladio Loizaga





Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

-3-

POR TANTO, en ejercicio de sus atribuciones legales,

EL MINISTRO DE RELACIONES EXTERIORES

RESUELVE:

- Art. 1° Aprobar las políticas sobre el uso responsable de los recursos de Tecnologías de Información y Comunicación, de conformidad con el texto que, como Anexo, forma parte integral de la presente Resolución.
- Art. 2° Sus disposiciones serán de aplicación en todo el ámbito del Ministerio de Relaciones Exteriores, dentro del cual se comprende las distintas dependencias dentro del Ministerio de Relaciones Exteriores y las Representaciones Diplomáticas y Oficinas Consulares en el exterior, y alcanzará a todos los funcionarios permanentes, comisionados, contratados, temporario o pasante y que tuvieren cualquier otro modo de relación laboral o de aprendizaje con la Institución. Será de aplicación, asimismo, a toda persona que utilice los recursos de Tecnologías de Información y Comunicación, cualquiera fuere la relación contractual que lo uniere con los mencionados organismos.
- Art. 3° Las políticas sobre el uso responsable de recursos de Tecnologías de Información y Comunicación, serán aplicadas a partir de los 90 días corridos posteriores a su publicación en la Página Web del Ministerio de Relaciones Exteriores, periodo durante el cual, la Autoridad de Aplicación, a través de las aéreas competentes, dará amplia difusión a su contenido.
- Art. 4° La Secretaria General, a través de la Dirección de Informática, será la Autoridad de Aplicación del Régimen, facultándose para realizar las auditorias y/o inspecciones para verificar su cumplimiento. Cuando la complejidad de las mismas así lo amerite, podrá requerir la realización de auditorias externas.
- Art. 5° Encargar a los Directores Generales, Directores o Encargados, Jefes de Departamentos y Jefes de Misión, a velar por el cumplimiento de las disposiciones del presente reglamento.
- Art. 6° Comunicar a quienes corresponda y archivar.

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL


Patricia Frutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

POLÍTICAS DE USO RESPONSABLE DE RECURSOS INFORMÁTICOS

1. OBJETIVOS

Esta norma tiene por propósito definir la política administrativa sobre el Uso Responsable de los Recursos de Tecnologías de Información y Comunicación, de los productos y activos ya sean tangibles o intangibles que provee el Ministerio de Relaciones Exteriores a las distintas dependencias en el Servicio Local y Exterior.

2. ALCANCE

Las normas de seguridad serán de aplicación a todas las dependencias dentro y fuera del Ministerio de Relaciones Exteriores, y en las Representaciones Diplomáticas y Oficinas Consulares del Paraguay en el exterior.

Será de aplicación, asimismo, a toda persona que utilice elementos de Tecnologías de Información y Comunicación cualquiera fuere la relación que la uniere con el Ministerio de Relaciones Exteriores.

Se aplicará a la utilización de los Servicios de Red y Comunicación, Internet, Sistemas y más específicamente al acceso y operación de dicha red, sistemas específicos y al uso del correo electrónico, cualquiera sea el horario y lugar en que se efectúe.

3. PRINCIPIOS GENERALES

3.1. El acceso a los diferentes sistemas de información y/o tecnologías informáticas que existen en el Ministerio de Relaciones Exteriores constituyen herramientas para mejorar la eficiencia en la prestación de las actividades laborales.

3.2. Los usuarios deberán actuar en forma legal, honesta y responsable, de manera a garantizar la integridad de los recursos de Tecnologías de Información y Comunicación, que el Ministerio de Relaciones Exteriores pone a su disposición para el cumplimiento de sus tareas sean estos tangibles o intangibles.

3.3. Los usuarios deberán actuar de acuerdo a la presente disposición y normas vigentes en la materia, ya sea en su calidad de funcionarios que prestan servicios en el Servicio Local como en el Exterior.

3.4. Los usuarios deberán respetar los términos de los contratos de licenciamiento de software y/o acuerdos contractuales que estén relacionados con los sistemas de información de la Institución o Representaciones Diplomáticas y Oficinas Consulares.

Nº _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Brutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

3.5. Los usuarios deberán utilizar los elementos de Tecnologías de Información y Comunicación, con el cuidado y la responsabilidad que deviene del ejercicio de la función pública.

3.6. Los usuarios deberán respetar los derechos de otros usuarios, la integridad de las instalaciones físicas y sus métodos de control.

3.7. Los sistemas de comunicación, direcciones de correo electrónico, direcciones IP, números de telefonía IP, nombres de dominio, sistemas de software específicos y/o bases de datos y demás recursos pertenecientes a la Institución, constituyen bienes intangibles de valor económico de propiedad del Ministerio de Relaciones Exteriores, por lo que toda utilización de los mismos será considerada como realizada en su representación, salvo que expresamente se dejare aclarado que dicha utilización y sus consecuencias "no constituyen la posición oficial de la Institución".

3.8. El incumplimiento de esta normativa puede resultar en la negación de acceso a los sistemas de información de la Institución, además de la aplicación de las medidas disciplinarias que correspondan en cada caso.

3.9. La Dirección Informática, a través de su departamento de Seguridad de Informática, definirá las normas, procedimientos y acciones, con el propósito de establecer un nivel de acceso adecuado a los recursos y necesidades de la Institución.

4. USUARIOS

4.1. Se definen como Usuarios a todas aquellas personas que tengan acceso a los diferentes sistemas de información o de redes provistos por el Ministerio de Relaciones Exteriores.

4.2. Se entiende que para que estas personas tengan dicho acceso, deberán tener previamente una relación con la Institución a través de sus diferentes modalidades (Funcionario Permanente, Comisionado, Contrato, Temporario o Pasante y toda otra relación laboral o de aprendizaje).

4.3. Se encuentra expresamente prohibido el acceso a la Red Institucional (MRE), Internet o al correo electrónico y Sistemas de Comunicaciones o software del Ministerio de Relaciones Exteriores, a toda otra persona ajena a la Institución, quien autorice dicho acceso, será responsable por todas las consecuencias del accionar del tercero autorizado y responderá administrativa y/o judicialmente, salvo que la autorización este por escrito figurando el nombre, número de identidad, firma, fecha y horario de uso del tercero autorizado.

5. USO PERMITIDO

5.1. Por uso permitido se entiende la utilización de las herramientas de Tecnologías de Información y Comunicación, para el desarrollo y mejor cumplimiento de las tareas propias de la función. La utilización de los diferentes sistemas de información y elementos informáticos es de uso exclusivo para asuntos gubernamentales u oficial.

N° _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL


Patricia Prutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

5.2. Los sistemas de información y equipos pueden ser usados siempre y cuando su utilización esté de acuerdo con las políticas oficiales y no interfiera con las operaciones y gestiones de la Institución, o con la tarea de los demás usuarios.

5.3. En el desarrollo de sus tareas, los usuarios deberán utilizar las herramientas de Tecnologías de Información y Comunicación, para mejorar la eficacia y eficiencia administrativa. Su utilización no podrá tomarse como obstáculo para el incumplimiento de las tareas encomendadas.

6. USO ACEPTABLE

6.1. Se acepta que los usuarios aprovechen en forma limitada los elementos informáticos para un uso personal que derive en su mejor capacitación, jerarquización y/o especialización en sus conocimientos, prácticas y habilidades o para aprovechar los beneficios de la Sociedad de la Información y el Conocimiento.

6.2. El uso aceptable no podrá interferir con las actividades o funciones que el usuario cumple, ni con la misión y gestión oficial que cumplen los funcionarios en la Representaciones Diplomáticas, Oficinas Consulares y dependencias dentro del Ministerio de Relaciones Exteriores.

6.3. Este uso personal limitado debe comenzar fuera del horario de trabajo normal del funcionario, siempre que el recurso se encuentre disponible y no exista otro usuario que precise emplear el recurso para sus tareas laborales y/o de práctica.

6.4. El uso aceptado no se considera un derecho del usuario y se encuentra sujeto al estricto control permanente de la autoridad de aplicación (Directores o Encargados de Departamentos) donde el usuario desempeña sus funciones.

6.5. El uso aceptado puede ser controlado, revocado o limitado en cualquier momento por razón de la función, por cuestiones operativas y/o de seguridad de la Red ya sea por la autoridad de aplicación y/o por las máximas autoridades del Ministerio de Relaciones Exteriores y de la Dirección de Informática.

6.6. No se considera uso aceptable aquel que demande un gasto adicional para la Institución, Representaciones Diplomáticas u Oficinas Consulares, (daños ocasionados al equipo, por su mala utilización o falta de cuidado), excepto el que derive del deterioro normal de los recursos informáticos.

7. USOS PROHIBIDOS

7.1. Se encuentra expresamente prohibido el mal uso de la Red o de cualquier recurso informático (correo electrónico, base de datos, sistemas informáticos, carpetas de archivos etc.), Sistemas de Comunicaciones (mensajería interna/externa, redes sociales, etc.) con fines que infrinjan normas nacionales o internacionales, causen daño o perjudiquen, ofendan o calumnien a la Institución y/o a sus funcionarios.

N° _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Brutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

7.2. La sustracción sin autorización de equipos o periféricos informáticos, y/o cualquier otro medio de soporte que contenga información confidencial (discos compactos, DVD, blueray, disquetes, cintas, pendrive, etc.) constituyen un delito de acción penal pública.

Se encuentra especialmente prohibido el uso de cualquier recurso informático para:

7.3.1. Grabar, modificar o borrar software, información, o bases de datos o registros de la Institución o Representación que contenga Información Confidencial.

7.3.2. Inferir cualquier daño a los equipos o a la información, las configuraciones de sistemas operativos o los aplicativos que se encuentren en ellos instalados.

7.3.3. Acceder sin autorización a los sistemas de información de los diferentes Servidores de Archivos y Computadores de la Institución o Representación.

7.3.4. Acceder, descargar, imprimir, transmitir, distribuir o almacenar material obsceno, discriminatorio, delictivo, ilegal o que de cualquier manera afecte a la moral o las buenas costumbres, salvo que exista debida autorización previa por escrito en la Dirección de Informática de la autoridad competente para la investigación y control de este tipo de ilícitos.

7.3.5. Obtener cualquier tipo de ganancia económica personal, con la Información Confidencial generada por el Ministerio de Relaciones Exteriores.

7.3.6. Difundir ideas políticas, lograr la adhesión a campañas o movilizaciones, captar el voto, enviar o reenviar correo masivo o realizar cualquier otro tipo de práctica de políticas partidarias con los recursos informáticos de la Institución, Representación Diplomática u Oficina Consular.

7.3.7. Revelar o compartir contraseñas de acceso, propias o de terceros, con otros usuarios así como el uso de la identificación, identidad, firma electrónica o digital de otro usuario.

7.3.8. Enviar cualquier transmisión de datos en forma fraudulenta.

7.3.9. Utilizar cualquier sistema de correo electrónico o cualquier tipo de comunicación electrónica con el propósito de acosar, amenazar, molestar o entorpecer a usuarios del Ministerio de Relaciones Exteriores y a terceros.

7.3.10. Utilizar cualquier sistema de correo o cualquier tipo de comunicación electrónica con el propósito de revelar información privada de otras personas, sin su consentimiento.

7.3.11. Utilizar cualquier sistema de correo electrónico o cualquier tipo de comunicación electrónica con el propósito de dañar o perjudicar de alguna manera los recursos informáticos.

N° _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL


Patricia Prutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

7.3.12. Lanzar cualquier tipo de virus, gusano, o programa de computación cuya intención sea hostil, destructiva, o que impacte directamente en el funcionamiento adecuado de los diferentes sistemas, ya sean internos de Institución o Representación Diplomática u Oficina Consular, como sistemas externos de otras Instituciones.

7.3.13. Realizar cualquier actividad contraria a los intereses de la Institución, tales como publicar información reservada, acceder sin autorización a recursos o archivos o impedir el acceso a otros usuarios mediante el mal uso deliberado de recursos comunes.

7.3.14. Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación u otros documentos o propiedades.

7.3.15. Descargar, almacenar, instalar o publicar material ilegal o nocivo a través de los recursos brindados por la Institución.

7.3.16. Almacenar, descargar, videos, música, imágenes, documentos y/o cualquier otro software o archivo protegido por las normas de propiedad intelectual sin autorización en los servidores del Ministerio de Relaciones Exteriores.

N°

7.3.17. Violar cualquier ley o norma, respecto del uso de los sistemas de información así como también realizar cualquier conducta ilegal contraria a la legislación aplicable de cualquier país al que se pueda tener acceso por la Red.

7.3.18. Registrarse a redes sociales, o publicar contenidos particulares en blogs de noticias o cualquier página web utilizando la cuenta oficial del correo electrónico @mre.gov.py.

7.3.19. Copiar o divulgar la lista de direcciones de correo electrónico para uso publicitario.

8. USO INDEBIDO DE LOS SISTEMAS

Bajo ninguna circunstancia el uso de los recursos de Tecnologías de Información y Comunicación por parte de los usuarios deberá influir de manera negativa en el desempeño, la imagen, en las tareas o generar responsabilidades para la Institución.

No se permiten los usos de Internet u otras herramientas tecnológicas y de las comunicaciones, ya sea utilizando equipamiento de la Institución, en ejercicio o en ocasión de las funciones que se realizan dentro del mismo, durante el horario laboral o fuera de él, con fines no autorizados.

Se definen expresamente como usos indebidos las siguientes acciones realizadas:

8.1. Modificar o reubicar equipos de computación, software, información, periféricos y/o cualquier otro medio de soporte de información (discos compactos, disquetes, cintas, etc.) sin la debida autorización de la Dirección de Informática.

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Frutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

- 8.2. Modificar, alterar y/o borrar, sin las autorizaciones correspondientes, la información o las configuraciones de sistemas operativos o los aplicativos instalados.
- 8.3. Acceder sin la debida autorización, mediante los equipos, software o redes de comunicación provistos por la Institución, a sistemas externos que no pertenezcan al Ministerio de Relaciones Exteriores.
- 8.4. Interferir, sin autorización, el acceso de otros usuarios a los recursos de Tecnologías de Información y Comunicación.
- 8.5. Transgredir o eludir las verificaciones de identidad u otros sistemas de seguridad.
- 8.6. Iniciar sesiones de Internet u otra tecnología, sin autorización utilizando recursos de la Institución o de Representaciones Diplomáticas, salvo que estén especialmente autorizados para ello.
- 8.7. Utilizar el correo Electrónico Institucional para enviar cualquier actividad de recreación personal o de promoción de intereses personales (tales como creencias religiosas, hobbies, comerciales etc.).
- 8.8. Almacenar, más allá de lo definido como uso aceptable, archivos personales de cualquier índole en los servidores o en los discos rígidos locales del computador, sin la autorización de la Dirección de Informática.
- 8.9. Instalar o conectar cualquier equipamiento no autorizado como pendrive, modem USB, etc, sin previa autorización o desinfección de virus en las terminales habilitadas por la Dirección de Informática.
- 8.10. Instalar, descargar, utilizar, copiar y/o distribuir software propietario más allá de la autorización escrita, salvo que se utilice con fines de investigación y sin lucro.
- 8.11. Acceder al código fuente de una obra de software sin autorización del autor con la finalidad de modificarlo, salvo que se utilice con fines de investigación.
- 8.12. Instalar programas o procesar sistemas o software libre, sin autorización de la Dirección de Informática.
- 8.13. Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación, u otros documentos o propiedades.
- 8.14. Leer información o archivos de otros usuarios sin su permiso.
- 8.15. Utilizar cualquier sistema de redes sociales y cualquier otro medio online, sin autorización por escrito solicitando el acceso a estos servicios a la Dirección de Informática.

N° _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL


Patricia Frutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

- 8.16. Difundir indebidamente y/o indiscriminadamente la información privada o pública a que tuviere acceso con motivo de la función o actividad que desempeña.
- 8.17. Transmitir publicidad no deseada.
- 8.18. Acceder, descargar, transmitir, distribuir información confidencial, sin autorización por cualquier medio de comunicación.
- 8.19. Utilizar los recursos TICs. con fines recreativos teniendo aun trabajo pendiente.

9. RESPONSABILIDADES

9.1. Responsabilidades Generales

Ningún usuario responsable debe usar la identificación, identidad, firma electrónica, firma digital o contraseña de otro usuario. Asimismo, ninguna persona debe dar a conocer su contraseña o identificación a otro, a excepción de los casos que deban facilitarse para la reparación o mantenimiento de algún sistema o equipo. En este caso y en forma estrictamente circunstancial, sólo deberá hacerlo al personal técnico o informático de la Institución, debidamente identificado, con la posibilidad que posteriormente dicho funcionario solicite al área técnica responsable, la modificación de claves, contraseñas u otro tipo de elemento de seguridad que implique riesgo de acceso por un tercero a los diferentes sistemas de información.

A efectos de evitar inconvenientes relativos a la falta de recursos y garantizar la seguridad física y lógica de los mismos, los usuarios de la red y de Internet tendrán las siguientes responsabilidades:

- 9.1.1. Conocer y dar cumplimiento a las normativas establecidas en la Política de Uso Responsable de Elementos TICs.
- 9.1.2. Seguir las políticas y procedimientos de seguridad establecidas para el uso de los servicios de la red y de Internet y evitar toda práctica que pueda dañar los sistemas de computación y archivos de datos de la Institución, como por ejemplo, aquellos que puedan dar lugar a ataques de virus cuando se recuperen archivos bajados de Internet, por la utilización de redes sociales, intercambio de archivos por mensajería instantánea, correo electrónico o cualquier otro medio.
- 9.1.3. Identificarse adecuadamente en toda comunicación con terceros, indicando su nombre, dirección electrónica e Institución a la que pertenecen.

N° _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Fajuto
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

9.1.4. Tomar conciencia que cuando se utilizan los recursos para comunicarse con terceros, aun siendo equipos particulares, dichos recursos y espacio físico pertenecen a la Institución, Representación Diplomática u Oficina Consular en cuya representación se está actuando.

En caso de emitir opiniones personales, el usuario deberá dejar aclarado que ellas no constituyen la opinión oficial de la Institución, de la Representación Diplomática u Oficina Consular a la cual representa.

9.1.5. Cumplir las indicaciones y pautas establecidas por la Dirección de Informática, para reducir los problemas de seguridad así como el impacto de virus en la red.

9.1.6. Cada usuario de los Sistemas Informáticos desarrollados por la Dirección de Informática, son responsables del correcto y adecuado uso de los mismos. No teniendo responsabilidad la Dirección de Informática en el mal uso de los sistemas o las consecuencias que pudieran ocasionar en el ámbito administrativo y/o Judicial.

La Dirección de Informática se limitará a informar a las autoridades competentes en caso de mal uso de los mismos. Y a establecer mecanismos tendientes a evitarlos.

9.2. Responsabilidades – Utilización Correo-Electrónico

Los usuarios autorizados deberán solicitar previamente a la Dirección de Informática, la autorización necesaria para enviar correos masivos o "en cadena", que no sean de interés para la institución.

9.2.1. Tomar conciencia que el correo electrónico y la cuenta de e-mail proporcionada por la Institución a los usuarios es para el cumplimiento de sus tareas es de titularidad del mismo independientemente del nombre y clave de acceso que fueren necesarias para su utilización.

9.2.2. Asumir la absoluta responsabilidad respecto del contenido de todo mensaje que se envíe utilizando los recursos o medios proporcionados por la Institución.

9.2.3. Transmitir y almacenar información considerada confidencial sólo en caso de encontrarse debidamente autorizados u obligados por la actividad o función que desempeñan, en cuyo caso únicamente lo podrán llevar a cabo mediante el uso de un sistema de encriptación seguro.

9.2.4. Evitar, en todos los casos, la divulgación de sus claves o contraseñas de acceso personales.

9.2.5. Verificar diariamente sus casillas electrónicas, evitando la acumulación de mensajes en ellas. En este sentido se advierte que debido a políticas internas relativas a la administración de los recursos TICs., al exceder determinado volumen dichos mensajes podrán ser eliminados automáticamente, sin previo aviso en caso de bloquear o ralentizar los sistemas de comunicación de la Institución.

No _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Santos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

9.2.6. Es responsabilidad de los superiores notificar a la Dirección de Informática, cuando un usuario que se encontraba a su cargo deja de prestar servicio en la Institución, de manera a eliminar o deshabilitar la cuenta de usuario, correo electrónico y accesos de carpeta.

Se deja constancia que respecto al correo electrónico rige la misma política de monitoreo establecida para Internet y la Red.

Todo mensaje de correo electrónico deberá contener la siguiente advertencia:

"Este mensaje es privado y confidencial y está dirigido únicamente a su destinatario. La indebida distribución, divulgación, copia o uso de este mensaje o su información adjunta está estrictamente prohibida. Si usted no es el destinatario original de este correo electrónico, por favor, avise a la brevedad respondiendo al remitente y elimínelo. La opinión y/o información contenida no constituye necesariamente la opinión oficial del Ministerio de Relaciones Exteriores. La información contenida no está garantizada como libre de error o alteración".

9.2.7. No utilizar la cuenta @mre.gov.py para enviar publicidad o publicar anuncios, comentarios, opiniones personales en sitios públicos o de noticias que no tengan relación con la actividad laboral que desempeña o con el fin de agredir, molestar a otras personas dentro y fuera de la Institución.

9.3. Responsabilidades – Uso de Internet - Redes Sociales – Mensajería Instantánea

9.3.1. Cada usuario que se conecta a Internet utilizando un dispositivo móvil o un recurso informático asume un riesgo de compartir involuntariamente su información, sus recursos y su reputación. Es responsabilidad del Usuario, utilizar con responsabilidad y prudencia las diferentes tecnologías que pueda encontrar en la nube o internet.

9.3.2. Al utilizar Redes Sociales, no incluir suficiente información personal que pueda comprometer su seguridad personal y las de sus colaboradores. Tener en cuenta que las costumbres de los usuarios influyen en el desarrollo de códigos maliciosos, que son aprovechados por los diferentes internautas y cibercriminales.

9.3.3. Al publicar o compartir un archivo en una Red Social tener en cuenta que hay más de 100 millones de Internautas, que pueden visualizar sus datos y contenidos y ser un potencial blanco de ataque, en caso de tratarse de una fotografía tener en cuenta que su publicación, sin el consentimiento de sus involucrados puede tomarse como una acción de violación a la privacidad.

9.3.4. Verificar que su Antivirus, Antispyware, se encuentre actualizado, antes de acceder a cuentas bancarias e información personal.

9.3.5. Tener en cuenta antes de escribir algún comentario que pueda perjudicar, dañar o molestar la imagen de otras personas, que el mensaje puede quedar registrado y puede utilizarse en su contra en acciones administrativas y/o judiciales.

N° _____

ES COPIA

(FDO): Eladio Loizaga





Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

9.4. Responsabilidades – Directores o Encargados de Departamentos.

Los Directores o Encargados de Departamentos tienen la obligación de evaluar y controlar el fiel cumplimiento de esta norma, y toda otra que resulte complementaria.

Los mismos tendrán las siguientes responsabilidades:

9.4.1. Autorizar excepcionalmente el acceso a Internet en días no laborables para propósitos relacionados con la función que el usuario cumple dentro de la Institución.

9.4.2. Difundir entre el personal las restricciones en el uso personal de los recursos con los que cuenta la Institución para acceder a los servicios de Internet, guardando copia de las respectivas notificaciones.

9.4.3. Asegurar que el personal conozca el Régimen sobre Uso Responsable de Elementos TICs.

9.4.4. Poner en conocimiento del personal las sanciones que les podrían corresponder, (llamado de atención, prohibición de acceso a Internet hasta el inicio de las correspondientes acciones administrativas y/o judiciales), como consecuencia de su incumplimiento.

9.4.5. Solicitar o desautorizar la creación de usuarios, acceso a las carpetas de archivos de la Dirección a su cargo en la Red Institucional, acceso a internet, correo electrónico, autorizar el acceso a páginas web bloqueadas a favor de los funcionarios a su cargo.

9.5. Responsabilidades – Dirección de Informática

9.5.1. Las Gestiones Administrativas y los antecedentes documentales relacionados con los expedientes de los créditos, franquicias fiscales, transferencia de fondos y otras funciones similares realizadas para la Entidad y así como otras funciones que realizan los funcionarios en la Institución, Representaciones Diplomáticas u Oficinas Consulares, serán efectuados y procesados por medios TICs., la Dirección de Informática se encargará de mantener la debida infraestructura, seguridad, mantenimiento y diligencia, de las Tecnologías de Información y Comunicación, para ayudar a la Institución y Representaciones Diplomáticas y Oficinas Consulares a alcanzar sus objetivos y asegurar que las personas con permisos adecuados siempre tengan acceso a la información que necesitan para realizar su trabajo.

9.5.2. La Dirección de Informática brindará las mejores soluciones y actualizaciones en TICs. para la evaluación de proyectos de tecnologías de informática y de telecomunicación; la elaboración, control y monitoreo de funcionamiento de infraestructura Tecnología y el mantenimiento de los equipos de los recursos Informáticos y de Comunicaciones, que permitirán realizar labores vinculadas a procesos de formulación, programación, ejecución, modificación, control y evaluación presupuestaria procesos de registros contables patrimoniales a fin de facilitar las labores de los funcionarios que prestan servicios en la Institución, Representaciones Diplomáticas u Oficinas Consulares.

N° _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Prutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

9.5.3. Los funcionarios que presten servicios en la Dirección de Informática, a través de sus diferentes modalidades (Funcionario Permanente, Comisionado, Contrato, Temporario o Pasante y toda otra relación laboral o de aprendizaje) están obligados a la no divulgación de información confidencial, ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible que pueda dañar el funcionamiento o la continuidad del trabajo del Ministerio de Relaciones Exteriores, el personal que realice algún acto en contra de la Institución, responderá a acciones administrativas y/o judiciales.

9.5.4. La Dirección de Informática contará con una conexión segura y aislada de la red MRE, cuando los usuarios de la Institución necesiten descargar, transmitir, descargar, videos, música, imágenes, documentos y/o cualquier otro software o archivo protegido que necesite análisis para evitar la propagación de virus dentro de la red ministerial.

9.5.5. Recepcionar, distribuir equipos informáticos y otros equipamientos tecnológicos, en coordinación con la Dirección Administrativa, en base a las necesidades en las distintas dependencias en el Servicio Local y Exterior.

9.5.6. Programar las adquisiciones en materia tecnológica y llevar un control de los suministros necesarios para el desarrollo de las actividades.

9.5.7. Evaluar periódicamente el uso óptimo de los equipos informáticos e insumos. Asesorar y capacitar a los usuarios de la Institución en materia de Tecnologías de la Información y Comunicación, mediante la realización de manuales, instructivos, boletines, seminarios, cursos, etc.

9.5.8. Realizar periódicamente el mantenimiento y evaluación de los equipos y recursos informáticos, en las distintas dependencias en el Servicio Local y Exterior.

9.5.9. La Dirección de Informática será la única responsable y tendrá jurisdicción sobre todo lo relacionado a TICs en el Ministerio de Relaciones Exteriores (Servicio Local y Exterior).

10. USUARIOS – DERECHOS

Son derechos de los usuarios:

10.1. Utilizar los recursos informáticos de conformidad con el presente reglamento y disposiciones complementarias.

10.2. Recibir ayuda y asesoramiento por parte del personal del servicio técnico correspondiente de cada Institución, Representación Diplomática u Oficina Consular.

10.3. Formular las sugerencias que estimen oportunas para mejorar el servicio.

No

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Prutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores

Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

10.4. Disponer de los recursos provistos por el Ministerio de Relaciones Exteriores, dentro de las normas correspondientes, para la gestión y la carga de trabajo asignados.

10.5. Acceder a información relacionada con su función.

10.6. Utilizar el correo electrónico, listas de discusión y otros servicios, siempre que tengan relación directa con la función del usuario en la Institución, Representaciones Diplomáticas u Oficinas Consulares.

10.7. Utilizar los recursos TICs. en forma limitada y fuera del horario laboral para su capacitación, sin que dicho uso interfiera con las actividades o funciones que el usuario cumple, ni con la misión y gestión oficial en la Institución, Representaciones Diplomáticas u Oficinas Consulares.

10.8. Acceder a los cursos de capacitación y actualización que el Departamento de Capacitación de la Dirección de Informática implemente en función de las actividades y labores que los usuarios desarrollen.

10.9. Realizar actividades de recreación, sin que afecte su buen desempeño en las tareas que realiza. Al respecto la Dirección de Informática establecerá las franjas horarias de navegación libre, según la autorización de las Altas Autoridades.

11. USUARIOS - DEBERES

Son deberes de los usuarios:

11.1. Contribuir al cuidado y conservación de las instalaciones, equipos y sistemas.

11.2. Notificar al personal del servicio técnico de las anomalías que se detecten, tanto de software como de hardware.

11.3. Respetar las indicaciones que reciban de los responsables de cada área respecto al uso y funcionamiento de los equipos.

11.4. El cumplimiento de las normas y condiciones establecidas en la presente normativa.

11.5. Salvaguardar la confidencialidad de la contraseña o clave (password) y evitar facilitarla a terceros por cualquier motivo. Cada usuario será responsable de las acciones que se reporten ejecutadas con su contraseña o clave (password).

11.6. Informar los casos de sustitución, de manera a asignar al sustituto, un nombre de usuario y una contraseña o clave transitorias y nunca la correspondiente a la persona sustituida.

No

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Frutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

11.7. Sugerir a la Dirección de Informática, las cuentas de correo, nombre de usuario y contraseña o clave, que sugieran o sean temporalmente suspendidas o eliminadas, según corresponda.

11.8. Generar sus propias contraseñas o claves (passwords), cada cierto período de tiempo en la medida que las posibilidades técnicas así lo permitan. Las conformará mediante el empleo de letras mayúsculas, minúsculas y números.

11.9. El período lo establecerá la Jefatura de Redes y Comunicación en consenso con la Jefatura de Seguridad Informática, dependiendo de la sensibilidad de la información de cada sistema.

11.10. Utilizar los recursos informáticos de la institución para no exhibir, copiar, mover, reproducir o manipular de cualquier otra forma, material de contenido atentatorio contra la ética, la moral o las buenas costumbres.

11.11. Informar a la Dirección de Informática en caso de sospechar la presencia de un "virus" en el equipo computacional, para adoptar las medidas pertinentes.

11.12. Bloquear el Acceso de su computador en caso que deba ausentarse, de forma que impida el uso de ese equipo por usuarios diferentes. En caso de compartir el equipo con otros usuarios deberá cerrar sesión de manera a posibilitar el acceso a otros funcionarios.

11.13. No realizar acciones como: remover, cambiar o intercambiar los componentes internos de los recursos informáticos y configurar o reconfigurar, programar o reprogramar e instalar o desinstalar programas (software) en los equipos de la Institución. Esto sin perjuicio de que la Dirección de Informática pueda autorizar expresamente a uno o varios usuarios de la distintas oficinas del Ministerio de Relaciones Exteriores, Representaciones Diplomáticas u Oficinas Consulares para realizar estas labores.

11.14. No utilizar los recursos TICs. de la institución para realizar actividades que comprometan las buenas costumbres, el orden y respeto.

11.15. Emplear únicamente el equipo informático y programas (software) que se le haya asignado o tenga derecho a compartir.

11.16. Observar el debido cuidado al manipular bebidas, alimentos o diferentes sustancias en los lugares donde se encuentren equipos informáticos, para evitar causarles daño o deterioro por causa de descuido o negligencia.

11.17. Evitar dejar encendidas las luces de oficinas, computador y/o monitor al terminar la actividad laboral, no dejar conectados o enchufados cargadores de celulares, notebooks o cualquier dispositivo en la red eléctrica que pueda sobrecalentarse y generar incendios o generar un consumo innecesario de electricidad. Esto a fin de dar cumplimiento al Decreto N° 4.851 del 9 de agosto de 2010, "Por el cual se racionaliza el uso de la energía eléctrica en los Organismos y Entidades del Estado".

Nº _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL


Patricia Erutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

11.18. No realizar acciones como enviar, copiar o facilitar por cualquier medio, información propiedad del Ministerio de Relaciones Exteriores y que por su naturaleza no deba divulgarse a terceros ajenos a la Institución. Lo anterior, excepto que se cuente con la debida autorización por escrito del superior jerárquico con rango no menor al de Viceministro, y en las Representaciones Diplomáticas el Embajador o Encargado de Negocios en su caso y en las Oficinas Consulares el Jefe de la misma.

11.19. Mantener legibles los medios de identificación de los equipos, a fin de facilitar los controles de inventario.

11.20. Procurar el mejor aprovechamiento del recurso de almacenamiento del equipo asignado o el disponible en la red, de forma que no se guarden archivos de cualquier tipo, ajenos a los fines e intereses de la institución.

11.21. Aplicar todos los lineamientos de seguridad que dicte el Departamento de Seguridad Informática y la Dirección de Informática para evitar el ingreso de aplicaciones no deseadas (virus, gusanos, malware, etc.) a los sistemas informáticos de la Institución.

12. MANIPULACIÓN DEL RECURSO INFORMÁTICO.

Corresponde únicamente al personal de la Dirección de Informática u otros funcionarios autorizados por ese Departamento, a abrir, configurar o reconfigurar, programar o reprogramar e instalar o desinstalar programas (software) en los equipos propiedad del Ministerio de Relaciones Exteriores. Asimismo, los componentes internos de los equipos informáticos solamente pueden ser removidos, cambiados o intercambiados por el personal de la Dirección de Informática.

13. SALIDA DE EQUIPO INFORMÁTICO.

Los equipos informáticos no pueden ser trasladados a otras oficinas u otros lugares fuera del ámbito de la oficina a la cual fueron asignados, salvo que se cuente previamente con la debida autorización del Departamento de Patrimonio y de la Dirección de Informática.

14. EQUIPO PROPIEDAD DE TERCEROS.

14.1. Corresponde a la Dirección Informática, en coordinación con el Departamento de Atención al Usuario, autorizar el ingreso a las oficinas del Ministerio de Relaciones Exteriores, de equipos computacionales propiedad de terceros, que se pondrán al servicio de la institución.

14.2. La solicitud de ingreso deberá remitirse a la Dirección de Informática con los documentos que acrediten al tercero como propietario del equipo informático, así como las licencias respectivas de los programas (software) instalados en ese equipo.

No _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Barros
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

14.3. Si la solicitud fuere aprobada, se comunicará a los Departamentos de Atención al Usuario, de Seguridad Informática y de Redes y Comunicaciones, brindando la información suficiente para crear los mecanismos necesarios que autoricen una ubicación oportuna de ese equipo.

14.4. Se podrá aprobar la instalación de otro programa (software) que se requiera para un aprovechamiento óptimo del recurso informático, pero no obstante, el mantenimiento del equipo siempre correrá por cuenta del propietario.

14.5. Para la salida de un equipo informático propiedad de un tercero, de las instalaciones del Ministerio de Relaciones Exteriores, los programas (software) pertenecientes a la institución deberán ser desinstalados por personal autorizado.

15. ADMINISTRACIÓN DE LOS RECURSOS DE SOFTWARE.

AUTORIZACIÓN DE USO.

En caso que los usuarios de los recursos tecnológicos requieran almacenar, instalar, ejecutar, o copiar de Internet programas (software) diferentes al instalado en sus equipos, deberán coordinar previamente con la Dirección de Informática - Departamento de Atención al Usuario, lo anterior, con el fin de evitar riesgos legales o de funcionamiento de los equipos.

16. AUTORIZACIÓN PARA EL DESARROLLO DE APLICACIONES INFORMÁTICAS.

Todo proyecto para desarrollar o implementar aplicaciones informáticas, páginas "web" o cualquier otro servicio informático, requiere de la aprobación, de la Dirección de Informática - Jefatura de Sistemas, Aplicaciones y Web, Jefatura de Redes y Comunicaciones, Jefatura de Seguridad Informática. Este deberá, en caso de aprobarse la solicitud y una vez valorada su viabilidad funcional técnica y presupuestaria, expresar de manera precisa los lineamientos técnicos específicos, según las políticas, procedimientos y reglas previamente definidas.

17. SEGURIDAD - POLITICA DE PRIVACIDAD Y CONFIDENCIALIDAD.

17.1. Todo uso de los recursos TICs. de la Institución se efectúa con el entendimiento de que tal uso es en general inseguro, no privado y no anónimo.

17.2. El personal que utilice equipos del Ministerio de Relaciones Exteriores para acceder a la red e Internet está sujeto a ser monitoreado en sus actividades por parte del Personal de Redes y Comunicaciones, Sistemas Aplicaciones y Web, Atención al Usuario y de Seguridad informática, autorizado a tal efecto. El simple uso de los servicios de Red implica el consentimiento a este monitoreo y a la no divulgación de información confidencial, ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible y que se encuentre claramente marcada como "CONFIDENCIAL". Por cuestiones operativas y de seguridad, debiendo los funcionarios tener en cuenta que la mayoría de las sesiones no son privadas.

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL


Patricia Frutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

17.3. Los administradores de Sistemas y el Personal de Redes y Comunicaciones, y de Seguridad informática, están habilitados para utilizar herramientas de monitoreo para optimizar el uso de los recursos informáticos y para garantizar la seguridad de la Red Ministerial que puede incluir la detección del uso no aceptable de los mismos. Las comunicaciones electrónicas pueden ser mostradas a las Instituciones que estén autorizadas a acceder a las mismas por sus funciones específicas.

17.4. Los usuarios deben tener en cuenta que los administradores de sistemas, Personal de Redes y Comunicaciones, y de Seguridad informática, supervisores están en condiciones de acceder a todas las comunicaciones electrónicas.

17.5. Se deja constancia que de ninguna manera se procederá a la comprobación o interceptación de los contenidos de los correos electrónicos de los funcionarios si no existen razones que afecten o puedan afectar el funcionamiento y/o seguridad de la Red y/o de la Institución al cual representan o bien por orden judicial.

17.6. La información personal del Usuario a la que se tenga acceso como consecuencia de las actividades de control, mejor funcionamiento o seguridad, no podrá ser difundida públicamente excepto que se trate de un uso no autorizado, indebido o prohibido y a los estrictos fines de iniciar la pertinente denuncia administrativa y/o judicial.

18. CONSECUENCIAS POR INCUMPLIMIENTO DE LA NORMATIVA.

18.1. El incumplimiento de la presente normativa dará lugar, según el caso, a la suspensión temporal o privación definitiva del derecho de uso de los sistemas, sin perjuicio de las responsabilidades disciplinarias y de cualquier otro tipo en que se hubiere incurrido.

18.2. La Dirección de Recursos Humanos y el Departamento de Personal de esta Institución o la Comisión Disciplinaria en la que ésta delegue, establecerá la duración de la suspensión o privación del acceso a los sistemas, de acuerdo con el principio de proporcionalidad, atendiendo a la intención, a la naturaleza de los perjuicios ocasionados, la reiteración y reincidencia. En cualquier caso, esta suspensión no podrá ser superior a un año.

18.3. En cuanto a las responsabilidades disciplinarias, las medidas serán acordes a la disposición que establezca la Dirección de Recursos Humanos o el Departamento de Personal, estableciendo un margen de igualdad, por la tipificación de la acción incurrida.

18.4. En caso que corresponda, se deberá efectuar las denuncias administrativas o judiciales por el uso indebido.

18.5. Según el caso, y de comprobarse responsabilidad, el usuario deberá indemnizar a la Institución por cualquier daño y/o perjuicio que pudiera ser considerado de Uso Indebido o Prohibido.

Nº _____

ES COPIA

(FDO): Eladio Loizaga

ES COPIA FIEL DEL ORIGINAL

Patricia Frutos
Directora General de Gabinete
Ministerio de Relaciones Exteriores



Ministerio de Relaciones Exteriores

Resolución N° 1189.-

POR LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y SE REGLAMENTA EL USO DE LOS EQUIPOS INFORMÁTICOS EN EL MINISTERIO DE RELACIONES EXTERIORES.

ANEXO

19. DISPOSICIONES FINALES.

19.1. Para el acceso a los sistemas y recursos informáticos del Ministerio de Relaciones Exteriores, el usuario deberá aceptar la presente normativa y/o futuras modificaciones sobre el Uso Responsable de Elementos TICs., pudiendo ser notificada en forma electrónica. La utilización de los recursos y sistemas TICs implicará su aceptación.

19.2. Cualquier comunicación enviada y/o recibida en forma electrónica podrá ser admisible como medio probatorio en cualquier procedimiento administrativo y/o judicial.

19.3. En todo lo relacionado con la interpretación y cumplimiento de lo aquí establecido, el usuario debe aceptar someterse a las leyes aplicables, y a la jurisdicción y tribunales competentes que defina la Dirección de Asuntos Legales, renunciando a cualquier otra jurisdicción que por razón de sus domicilios presentes o futuros, o por cualquier otra razón pudiere corresponderles.

19.4. Cuando un usuario autorizado termine su relación contractual con la Institución, cualquiera sea la modalidad o circunstancia, ya sea en Representaciones Diplomáticas, Oficinas Consulares o dependencia dentro del Ministerio de Relaciones Exteriores, donde desempeñare su actividad, deberá notificar inmediatamente a la autoridad de aplicación para la eliminación de identificaciones, firmas electrónicas, firmas digitales o contraseñas, con el único objeto de evitar responsabilidades en el futuro. La Dirección de Recursos Humanos o el Departamento de Personal de la Institución informarán asimismo a las áreas responsables, cualquier modificación en la relación contractual de los agentes que tuvieren registro.

19.5. Con la promulgación del presente reglamento quedan derogadas todas las disposiciones legales que se opongan al mismo.

19.6. Determinar que el presente reglamento entra en vigor a partir de los 90 días de la fecha de su aprobación y publicación.

ES COPIA

(FDO): Eladio Loizaga

