

RESOLUCION DIRECTORIO N° 210/2022

POR LA CUAL SE APRUEBA EL REGLAMENTO INTERNO DE USO DEL SERVICIO DE INTERNET Y CORREO ELECTRONICO INSTITUCIONAL.

Asunción, 02 de febrero de 2022

VISTO: El Interno INF-PR/00002/2022 de fecha 24.01.2022 del Departamento de Informática, y;

CONSIDERANDO: Que, por Interno INF-PR/00002/2022 el Departamento de Informática remite un borrador de reglamento donde se establecen las normativas de uso del servicio de internet y correo electrónico institucional.

Que, se somete a consideración del Directorio el borrador de reglamento de uso del servicio de internet y correo electrónico institucional, para su aprobación.

POR TANTO: El Directorio de la CONATEL, en sesión ordinaria del 02 de febrero de 2022, Acta N° 06/2022, y de conformidad a las disposiciones legales previstas en la Ley 642/95 de Telecomunicaciones.

RESUELVE:

- Art. 1° APROBAR** el REGLAMENTO INTERNO DE USO DEL SERVICIO DE INTERNET Y CORREO ELECTRONICO INSTITUCIONAL, que se establece en el anexo a la presente Resolución.
- Art. 2° AUTORIZAR** al Departamento de Informática a tomar las medidas que sean necesarias en virtud a la presente reglamentación y las disposiciones legales vigentes.
- Art. 3° COMUNICAR** a todas las dependencias y cumplir, archivar.



ING. JUAN CARLOS DUARTES DURE.
Presidente
Res. Dir. N° 210/2022

A1128837

REGLAMENTO INTERNO DE USO DEL SERVICIO DE INTERNET Y CORREO ELECTRÓNICO INSTITUCIONAL

CAPITULO I: DISPOSICIONES GENERALES

ART. 1° OBJETIVO

El presente reglamento tiene como objetivo fundamental establecer los lineamientos para el uso correcto del correo electrónico institucional.

ART. 2° DEFINICIONES

A los efectos de la aplicación del presente reglamento los siguientes términos y expresiones tendrán el significado que se indica a continuación:

- a) **FTP** en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectadas a una red TCP, basado en la arquitectura cliente-servidor.
- b) **Se llama spammers** al sujeto o personas que generan Spam. Se llama Spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviado en grandes cantidades que perjudican de alguna o varias maneras al receptor.
- c) **El Simple Mail Transfer Protocol**, es un protocolo de la capa de aplicación. Protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.
- d) **Domain Name System o DNS** es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.
- e) **Mail Transport Agent (Agente de Transporte de Correo)**. El mensaje se envía al servidor de correo electrónico llamado MTA que tiene la tarea de transportarlos hacia el MTA del destinatario.

CAPITULO II: CREACIÓN, TIPOS, VIGENCIA Y ELIMINACION DE CUENTAS

ART. 3° DE LAS CUENTAS

Para la creación de las cuentas el funcionario interesado debe llenar, firmar y remitir al Departamento de Informática el formulario de solicitud de correo, conforme al ANEXO "FORMULARIO DE ADMINISTRACIÓN DE USUARIOS" del presente reglamento.

Para disponer de una cuenta personal en el dominio conatel.gov.py, necesariamente se deberá contar con una relación de dependencia con la CONATEL.

Las cuentas institucionales se crean a petición del Jefe del área respectiva. La solicitud de una cuenta organizativa debe ser realizada por el área respectiva a la unidad que administra el dominio de correo.



Juan Carlos Duarte Dura
Presidente
CONATEL

ART. 4° TIPOS DE CUENTAS

Bajo el dominio “conatel.gov.py”, se pueden distinguir tres tipos de cuentas: Personales, Institucionales y Organizativas.

- a) Cuentas Personales: Identifican las direcciones de correo electrónico de una persona;
- b) Cuentas Institucionales: Están asociadas a los CARGOS. Las cuentas Institucionales predefinidas en la CONATEL se refieren a: Directorio, Gerencia, Departamento, División y Unidad. Una persona tendrá acceso a una cuenta institucional en función de su cargo o de su actividad;
- c) Cuentas Organizativas: Las cuentas organizativas están orientadas fundamentalmente a grupos de trabajo. Pueden ser utilizadas por una o varias personas conjuntamente y son gestionadas por un responsable. Por consiguiente, este tipo de cuentas no están asociadas a cargos o personas.

ART. 5° VIGENCIA DE LAS CUENTAS

- a) Cuentas Personales: Las cuentas personales permanecen mientras dure la relación de dependencia con la CONATEL. En caso de extinguirse dicha relación, la que deberá ser informada por la Gerencia de Capital Humano, la cuenta será eliminada.
- b) Cuentas Institucionales: Las cuentas institucionales permanecen hasta que desaparezcan el cargo o función que las motivó; por lo que serán utilizadas por las personas que ocupan ese cargo o función a lo largo del tiempo. Dado que los usuarios de las cuentas lo hacen en función de su situación, la asignación de personas a cuentas se realiza directamente desde los servidores centrales de la CONATEL y a petición del superior inmediato. La baja de la persona en el cargo o función implica el cambio de la contraseña de la cuenta de correo institucional;
- c) Cuentas Organizativas: Este tipo de cuentas se cancelan o gestionan a petición de las Gerencias, Departamento o grupos, o de la persona responsable de la misma.

ART. 6° PROCEDIMIENTO DE DESACTIVACIÓN Y ELIMINACIÓN DE CUENTAS

- a) Borrado automático de cuentas: Se eliminarán aquellas cuentas de correo electrónico que no han sido consultadas durante un periodo continuado de tres meses. Esto conlleva el borrado de los correos almacenados en dicha cuenta.
- b) Cancelación voluntaria de cuentas: se podrá solicitar el cierre o cancelación de una cuenta de correo. Para ello, su titular deberá realizar la solicitud al Administrador del Sistema de Correo Institucional, quién hará efectiva la solicitud tras la comprobación de su veracidad y la remisión de un correo de confirmación al solicitante dos días antes de efectuar la cancelación de la cuenta de tal manera que el usuario del correo confirme la eliminación definitiva. La cancelación de una cuenta implica la imposibilidad de enviar y recibir nuevos correos y la eliminación de los correos almacenados.



Ing. Juan Carlos Duarte Durán
Presidente
CONATEL

c) Desactivación temporal de cuentas:

- i. El uso inapropiado o el abuso en el servicio de correo electrónico puede ocasionar la desactivación temporal o permanente de las cuentas. Las acciones en este sentido se pueden llevar a cabo en función de las posibles repercusiones en el buen funcionamiento del servicio;
- ii. La desactivación de la cuenta implica la imposibilidad de enviar y recibir nuevos correos mientras no vuelva a ser activada;
- iii. Ante situaciones de grave riesgo para la disponibilidad o continuidad del servicio, se podrá cambiar la contraseña de una cuenta. Esto podría impedir al usuario el acceso al resto de los servicios basados en las credenciales de la Intranet.

CAPITULO III: USO DEL CORREO INSTITUCIONAL

ART. 7° DEL CORREO INSTITUCIONAL

- a) El uso de los servicios de Internet y correo electrónico deberá ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.
- b) El acceso a los servicios de Internet y correo electrónico estarán disponibles para todos los usuarios de CONATEL ya sean estos funcionarios permanentes, funcionarios contratados y pasantes universitarios si las condiciones de infraestructura tecnológica lo permiten.
- c) El correo electrónico institucional es una herramienta de comunicación e intercambio oficial de información y no una herramienta de difusión indiscriminada de información.
- d) Con el fin de realizar una gestión sostenible del espacio ocupado por los buzones de correo de los usuarios, se hace imprescindible aplicar una política de cuotas que limiten el espacio de disco ocupado por dichos buzones. Con este fin, dichas cuentas de correo electrónico se verán sometidas a una restricción de cuota en función a la disponibilidad de espacio en disco.
- e) La capacidad máxima para los buzones puede variar a lo largo del tiempo. Cuando el sistema detecta que la ocupación del buzón de correo es superior al 90% automáticamente envía una notificación al usuario, con el fin de que pueda tomar las medidas pertinentes. Una vez alcanzado el 100% de la cuota asignada, todos los mensajes son rechazados por el sistema, siendo necesario "UN MANTENIMIENTO" del buzón para restablecer la recepción normal de mensaje.
- f) Envío de Mensajes: Se ha de considerar que el correo electrónico enviado circula por distintos servidores de Internet y que éstos imponen libremente restricciones sobre los tamaños admitidos, por lo que cuanto más grande sea el tamaño del mensaje de correo electrónico mayor es la probabilidad de que sea rechazado, impidiendo de este modo, que llegue a su destino.
- g) Tamaño máximo de Correo Electrónico: Para el envío de fichero de gran tamaño, se recomienda el uso del Servicio FTP, que permite el envío de ficheros muy grandes. El correo electrónico Institucional permitirá la recepción y envío de archivos de tamaño inferior a 20 MB; bajo condiciones especiales, previa solicitud y justificación, se podrá destinar mayor espacio en el buzón y en el tamaño de recepción y envío de los mensajes. El tamaño máximo de correo electrónico que se pueden enviar y recibir se podrá modificar sin previo aviso. Asimismo y por razones de disponibilidad del servicio se podrá incluir otro tipo de restricciones, como limitar el número máximo de mensajes enviados desde una cuenta durante un periodo de tiempo.


Ing. Juan Carlos Duarte Durán
Presidente
CONATEL

h) Reserva Institucional: La cuenta de correo electrónico asignada a cada usuario está reservada exclusivamente para uso de la CONATEL y deberá responder a razones de trabajo. No está permitido el envío de correos individuales o masivos cuyo tema no sea de carácter institucional. Los mensajes de correo electrónico no deben contener palabras o frases agresivas, violentas o que vulneren la dignidad de las personas. No enviar correo basura, SPAM indiscriminado, o encadenado no autorizado o consentido previamente por los destinatarios. No están permitidos los mecanismos y sistemas que intenten ocultar la identidad del emisor de correo. Está prohibida la suplantación de identidad de otra persona en el envío de mensajes de correo electrónico.

i) Spam: El Servidor de Correo Institucional dispone de un sistema encargado de eliminar el Spam, basado en listas de reputación de los servicios que envían correos. El sistema ha sido configurado de modo que son eliminados aquellos mensajes considerados Spam con un 99,99% de certeza.

j) Virus: Los Servidores de Correo Institucional analizan todo el tráfico de correo entrante y saliente, y rechazan el envío de mensajes que contienen virus. Cuando un mensaje es rechazado se envía una notificación al destinatario, salvo en el caso de virus que falsifiquen la cabecera de origen

ART. 8° PROBLEMAS QUE AFECTAN EL NORMAL FUNCIONAMIENTO

Son múltiples los problemas de seguridad que pueden afectar el normal funcionamiento del sistema de correo institucional, entre los que cabe destacar:

- a) Robo de identidad. Phishing y Scams;
- b) Virus: virus y sobre todo los gusanos que utilizan técnicas de Spam para propagarse después de infectar una PC;
- c) Combinación de Virus y Spam: Las últimas generaciones de virus se han creado para ayudar a los spammers. Muchos spammers han incorporado código malicioso en su Spam;
- d) Ataques con direcciones falsificadas: Consiste en inundar el servidor de un dominio real con los errores generados por una máquina atacada al procesar Spam para distribuirlo a miles de destinatarios. El spammer coloca como dirección receptora de estos errores un dominio real y un usuario aleatorio. Esto provocará problemas de ancho de banda, colapso del Servidor (colas, disco, etc.). Puede ser considerado un ataque de denegación de servicio.
- e) Generación innecesaria de tráfico SMTP. El envío y encaminamiento de un simple mensaje de correo electrónico implica el uso de varios recursos: conexiones SMTP, consultas DNS, procesamiento por MTA. Los propios errores de SMTP, el Spam, los Virus, etc., generan informes a direcciones falsificadas provocando confusión en los usuarios y generando un exceso de tráfico.



Ing. Juan Carlos Duarte Duque
Presidente
CONATEL

ART. 9° RECOMENDACIONES GENERALES

- a) Contraseña: La contraseña de acceso al correo no debe ser cedida o facilitada a otros usuarios, siendo responsabilidad del propio usuario su custodia;
- b) Encriptación: La transmisión del binomio usuario/clave debe realizarse de forma cifrada mediante la activación de protocolos seguros en los clientes de correo.
- c) Política de copias de seguridad: El Departamento de Informática no realizará copias de seguridad de los buzones, siendo responsabilidad de los usuarios guardar una copia local. Los datos a efectos legales se consideran en tránsito y temporales;
- d) Clientes de correo: Los programas de clientes de correos soportados son: Microsoft Outlook.

Desde el Departamento de Informática y unidades informáticas de la CONATEL, no se solicitará NUNCA a los usuarios la contraseña de los servicios que se ofrecen. Ante una sospecha no se deberá abrir o responder a los mensajes. Ante cualquier duda, deberá contactar con el Administrador del dominio o con el personal TIC del Departamento de Informática.

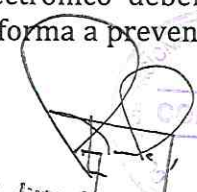
ART. 10° PARA EL ENVÍO DE MENSAJES SE APLICARÁN LAS SIGUIENTES REGLAS:

- a) Se utilizará siempre el campo de Asunto, a fin de resumir el tema del mensaje.
- b) No se enviarán mensajes a personas desconocidas, a menos que se trate de un asunto oficial que las involucre.
- c) No se enviarán mensajes a listas globales, a menos que el propietario sea la persona autorizada por el superior para enviar mensajes que involucren a toda la Institución.
- d) La divulgación de mensajes de interés general (actividades internas, invitaciones, notas luctuosas, entre otros) deberá coordinarse con el área correspondiente el cual definirá el procedimiento para tal fin.

CAPITULO IV: RESPONSABILIDADES

ART. 11° RESPONSABILIDADES DEL DEPARTAMENTO DE INFORMÁTICA

- a) Los servicios de Internet y correo electrónico serán administrados por el Departamento de Informática (DI).
- b) Las restricciones de acceso a Internet, serán definidas en las políticas y procedimientos generales de la CONATEL.
- c) El DI será el encargado de habilitar herramientas de registros de navegación, que permitan crear informes para auditorías.
- d) Para la comunicación oficial de CONATEL se utilizará la cuenta de correo institucional, en la medida de las posibilidades.
- e) El DI asignará las cuentas de correo de acuerdo a las licencias disponibles.
- f) El sistema operativo y el antivirus del servidor principal de correo electrónico deberá mantenerse actualizado con la última versión disponible de software de tal forma a prevenir los accesos no autorizados.



Ing. Juan Carlos Duarte Duró
Presidente
CONATEL

ART. 12° RESPONSABILIDAD DEL USUARIO

Los usuarios son responsables de todas las actividades realizadas con las cuentas de correo electrónico proporcionado por la CONATEL. Esta responsabilidad supone el cuidado de los recursos que integran dicha cuenta y, particularmente, de los elementos, como la contraseña, que pueden permitir el acceso de terceras personas a dicha cuenta, o a otros recursos personales que utilicen ese identificador.

Los Servidores de Correo Electrónico, envían un correo al emisor informando de los problemas surgidos en casos de que no se pueda entregar un correo a un destinatario debido a las siguientes incidencias: caídas imprevistas en las líneas de comunicaciones, límites de almacenamiento en los buzones del usuario receptor, rechazo de mensajes por virus, exceso de tamaño para el servidor que recibe, dirección mal escrita, etc. Es responsabilidad del propio usuario leer los mensajes de retorno que los sistemas de correo le envíen notificándole cualquiera de estas incidencias en la entrega de los mensajes remitidos por él.

- a) El funcionario que tenga acceso a servicios de correo electrónico debe evitar divulgar su cuenta a personas o entes desconocidos.
- b) Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
- c) Los funcionarios deben realizar revisiones periódicas de los mensajes almacenados con el fin de no mantener información innecesaria.
- d) La Gerencia de Capital Humano deberá notificar al DI cuando se deba crear, cerrar o inhabilitar una cuenta de correo electrónico.
- e) El usuario debe atender a los avisos de actualización automática del programa de detección de virus e informar al DI, cuando la actualización no se realice satisfactoriamente.
- f) Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o browser no deberán ser cambiados, excepto por indicaciones del DI.

CAPITULO V: PROHIBICIONES

ART. 13° PROHIBICIONES

Está prohibida la utilización abusiva del correo electrónico y de las listas de distribución incluyendo la realización de prácticas tales como:

- a) Se prohíbe a los funcionarios que tengan acceso al servicio de correo electrónico abrir mensajes de procedencia desconocida.
- b) Está prohibido facilitar, ofrecer o compartir las cuentas de correo a terceras personas.
- c) En caso de que fuera necesario un envío masivo se recomienda usar las listas de distribución o usar el campo de "copia oculta" (Bcc ó Cco) para poner la lista de destinatarios, o bien ponerse en contacto con el DI.
- d) Actividades comerciales privadas.
- e) Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.

- f) El insulto, la amenaza o la difamación a cualquier persona.
- g) Se prohíbe a los empleados formar parte de cadenas de mensajes o SPAM, ya que esto contribuye a la saturación de las redes de telecomunicación y facilita la divulgación de su cuenta de correo y la proliferación de virus en la red.
- Suscribirse a periódicos, revistas, semanarios, buscadores de parejas, chats; ni a ningún otro tipo de actividades o boletines electrónicos que no sea el estrictamente relacionado con el área profesional de trabajo del funcionario.
- h) Descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional del funcionario. El DI procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados. Envío de correos al Exterior.
- i) Los únicos autorizados a enviar correos al exterior desde la Red de la CONATEL son los Servidores de Correo gestionados por los administradores TICs de la Institución. En ningún caso un ordenador personal podrá realizar esta tarea y para enviar correo deberá entregar al Servidor Principal para su posterior procesamiento.
- j) Cortafuego Corporativo del Centro de Datos (FIREWALL) En los cortafuegos corporativos del Centro de Datos, los puertos TCP 25, 465, y eventualmente los puertos 993 y 995 se permitirá únicamente tráfico provenientes desde el Servidor de correo Institucional y bloqueará el tráfico proveniente de otros ordenadores y/o Servidores.

CAPITULO VI: SANCIONES


ART. 14° DE LAS SANCIONES

Los usuarios que infrinjan las previsiones contenidas en este Reglamento serán pasibles del sumario administrativo correspondiente aprobado por la máxima autoridad.

CAPITULO VII: DISPOSICIONES FINALES

ART. 15° DE LA ENTRADA EN VIGENCIA Y VALIDEZ

El presente reglamento tendrá plena validez y vigencia siendo de cumplimiento obligatorio a partir de su aprobación por la máxima autoridad de la Institución y su correspondiente publicación.



Ing. Juan Carlos Duarte Duró
Presidente
CONATEL.



FORMULARIO DE ADMINISTRACION DE
USUARIOS

...../...../.....
FECHA DE SOLICITUD:

MARCAR SISTEMA: GESDOC () – SUMINISTROS () – CRM () – CORREO ()

NOMBRES :

APELLIDOS :

CÉDULA DE IDENTIDAD

CORREO INSTITUCIONAL

GERENCIA :

DEPARTAMENTO :

UNIDAD

CARGO

PISO :

VINCULACIÓN: PERMANENTE () – CONTRATADO () – COMISIONADO () – PASANTE ()

.....
FIRMA DEL USUARIO

.....
FIRMA AUTORIZADA POR
EL SUPERIOR (sello)

USO EXCLUSIVO DEL DEPARTAMENTO DE INFORMATICA

NOMBRE DE USUARIO
PERFIL DE USUARIO :