REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

EL MINISTRO

RESOLUCIÓN No. 121/2017

POR CUANTO: El Acuerdo No. 7380 del Consejo de Ministros, de fecha 28 de febrero de 2013, en su numeral Tercero del Apartado Primero, establece que el Ministerio de Comunicaciones es el organismo encargado de proponer, y una vez aprobada, ejecutar y controlar la política sobre el uso del ciberespacio, así como planificar, implementar, reglamentar, administrar y controlar el sistema de medidas necesarias para su defensa y realizar las coordinaciones internacionales requeridas a ese fin.

POR CUANTO: La Resolución No. 127 del ministro de Comunicaciones, de fecha 24 de julio de 2007, aprobó y puso en vigor el "Reglamento de Seguridad para las Tecnologías de la Información", en el que se establece que en todas las redes informáticas se tienen que implementar mecanismos de seguridad de forma tal que se garantice la protección de las mismas, por lo que resulta procedente establecer las medidas básicas para configurar los servidores de correo electrónico de las redes de datos del país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas, en el inciso a), del Artículo 100 de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Establecer las medidas básicas para configurar los servidores de correo electrónico que se deben implementar en las redes de datos del país debidamente autorizadas, en lo adelante las redes, las cuales se refieren a continuación:

1. Control de acceso a los puertos 25, 443 y 587 en entrada/salida.

2. Implementación de reglas anti-relay (protección contra correos no solicitados).

3. Control de resolución inversa.

4. Política de trazas de auditoría.

5. Número máximo de destinatarios en una transacción SMTP (Simple Mail Transfer Protocol en inglés – protocolo para la transferencia simple de correo en español).

6. Tamaño máximo de mensaje.

7. Definición de registros SPF (*Sender Policy Framework en inglés- convenio de remitentes en español)*.

Ave. Independencia No.2 e/ 19 de Mayo y Aranguren, La Habana, Cuba. Telef. (+537) 859-9205 / (+537) 859-9206
Fax: (537) 859-9232 Correo electrónico: despacho@mincom.gob.cu

8. Chequeo de registro SPF en el flujo de entrada.

9. Control de destinatarios existentes.

10. Control de flujo SMTP.

11. Sincronización de tiempo.

12. Acceso cifrado.

13. Servicio Antivirus.

14. Autenticación.

15. Servicio de cambio de contraseña.

16. Servicio antispam (método para prevenir el correo basura).

Las aclaraciones requeridas relacionadas con la implementación de las medidas básicas para configurar los servidores de correo electrónico, se establecen en el Anexo Único de la presente Resolución como parte integrante de la misma.

SEGUNDO: El titular o representante legal de la red de datos es responsable por la implementación en sus redes, de las medidas básicas que por la presente se establecen para configurar los servidores de correo electrónico.

TERCERO: A los efectos de la presente, los términos que se relacionan tienen el significado siguiente:

1. **Ataque informático:** Intento de acceso o acceso a una red informática mediante la explotación de vulnerabilidades existentes en su seguridad.

2. **Riesgo informático:** Probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en las redes.

3. **Red de datos:** Red de telecomunicaciones cuya infraestructura de red está instalada en una misma localidad o en distintas localidades geográficas e interconectadas entre sí por enlaces de telecomunicaciones públicos y propios, que satisface las necesidades de transmisión de datos de su titular.

4. **Resolución inversa de IP:** Proceso en que a partir de la dirección IP de un dispositivo, se intenta llegar al nombre asociado a este.

5. **Sistemas de Nombres de Dominios (DNS):** Es el sistema empleado en Internet para asignar y usar universalmente nombres unívocos para referirse a equipos, portales o sitios conectados a la Red.

6. **Servidor de nivel base**: Servidor que presta el servicio de correo electrónico y almacena los buzones de los usuarios de una red.

7. **Servidor de primer nivel**: Servidor encargado de recibir todo el correo electrónico destinado a un grupo de dominios y distribuirlo a cada uno de los subdominios, de igual manera reciben el correo procedente de los subdominios y lo reenvían a los destinatarios finales.

8. **Vulnerabilidad informática:** Aspecto de la aplicación que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático y califica su nivel de riesgo.

CUARTO: Los directores de las oficinas territoriales de control, el director de Inspección, el director general de la Oficina de Seguridad para las Redes Informáticas y el director general de Informática del Ministerio de Comunicaciones, quedan encargados de instrumentar las medidas para el control y fiscalización de lo dispuesto en la presente Resolución.

QUINTO: Los titulares de las redes privadas de los órganos de la Defensa, se exceptúan del cumplimiento de lo establecido en la presente Resolución, y quedan sujetos a lo dispuesto en sus normas jurídicas.

SEXTO: La presente Resolución entra en vigor a los noventa (90) días posteriores a la fecha de su publicación en la Gaceta Oficial de la República de Cuba.

NOTIFÍQUESE a los directores generales de Informática y de la Oficina de Seguridad para las Redes Informáticas, a los directores territoriales de control y al director de Inspección, todos pertenecientes al Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, al director general de Comunicaciones, al director de Regulaciones y al director del Centro de Comunicaciones, todos pertenecientes al Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 5 días del mes de abril de 2017.

Maimir Mesa Ramos
Ministro

LIC. PEDRO PAVEL GARCIA SIERRA, DIRECTOR JURÍDICO DEL MINISTERIO DE COMUNICACIONES
CERTIFICO: Que la presente Resolución es copia fiel y exacta del original que obra en los archivos de esta Dirección a mi cargo.
La Habana, 5 de abril de 2017

Anexo Resolución No. 121/2017

ACLARACIONES DE LAS MEDIDAS BÁSICAS PARA CONFIGURAR LOS SERVIDORES DE CORREO ELECTRÓNICO.

1. Control de acceso a los puertos 25, 443 y 587 en entrada/salida.

   El puerto virtual 25 SMTP controla el acceso para el tráfico tanto de llegada como de salida. El puerto virtual 443 controla el tráfico de información sensible HTTPS (protocolo seguro de transferencia de hipertextos) utilizando cifrado basado en SSL (capa de puertos seguros) o TLS (seguridad en la capa de transporte) para los usuarios y claves. El puerto virtual 587 controla el acceso para SMTP autenticado sobre SSL o sobre TLS. El uso de los puertos 443 y 587 antes mencionados son los recomendados por medidas de seguridad, u otro que se asigne siempre que sea cifrado. La cantidad de servidores que pueden enviar o recibir correo debe limitarse, en correspondencia con las necesidades reales de cada entidad y bajo el principio de la racionalidad. Las computadoras conectadas a la red que utilizan el servicio deben ser configuradas para que reciban/envíen correos electrónicos únicamente a través del servidor establecido en cada entidad.

2. Implementación de reglas Anti-Relay.

   La adopción de medidas anti-relay se considera uno de los pasos básicos para la puesta en marcha de un servicio de correo. De no cumplirse este criterio se corre el riesgo de publicación en múltiples repositorios en Internet, por configuración inadecuada del servicio, para que sea utilizado para el envío de spam.

   Por lo anterior, el servicio de correo solo se brinda para la red predeterminada. La dirección IP para este servicio está claramente definida y solo estas direcciones tienen privilegios concedidos para usar el correo. Lo anterior implica que las direcciones IP de cada red, una vez definidas, pueden establecer conexión SMTP hacia el servidor, aceptando mensajes cuyo destino sea la propia red o dominios delegados[1].

3. Control de resolución inversa.

   Debe definirse la resolución inversa de las direcciones IP asignadas al servicio de correo de primer nivel, encargadas del encaminamiento de entrada y salida de cada red[2].

4. Política de trazas de auditoría.

   Deben almacenarse y conservarse en cada red los ficheros de trazas (logs en inglés) de acuerdo con la legislación vigente, de forma que las mismas permitan

[1] RFC2505/RFC2635.
[2] RFC3172.
RFC (request for comments en inglés) (Petición de comentarios en español) publicaciones del grupo de trabajo de ingeniería de internet (IETF) relacionados con protocolos, procedimientos etc.

la identificación de posibles problemas o incidentes y sirvan como fuente de datos para estudios estadísticos; deben contener al menos los datos siguientes: fecha y hora de la transacción, nombres de los servidores que reciben/envían, identificador (ID) del mensaje, dirección de origen/destino, nombre del servidor que actúa como relay de correo, el estado de la transacción y el tamaño del mensaje.

5. Número máximo de destinatarios en una transacción SMTP.

   Los servidores de correo electrónico deben configurarse para aceptar transacciones con un máximo de 100 destinatarios (RCPT TO)[3] en una sola conexión SMTP. Deben adoptarse las medidas técnicas necesarias para que se bloqueen las transacciones SMTP con más de 100 destinatarios. Los límites (mínimo y máximo) de destinatarios en una sola conexión SMTP deben ser definidos y aprobados por la máxima dirección de cada red privada, en dependencia de los recursos técnicos disponibles.

6. Tamaño máximo de mensaje.

   El tamaño máximo del mensaje debe ser controlado, formando parte de la configuración de los servidores de primer nivel. El tamaño máximo del mensaje debe ser definido en cada institución atendiendo a sus propias características.

7. Definición de registros SPF.

   Debe definirse en cada red su zona del Sistema de Nombres de Dominio (DNS en inglés) los registros SPF (*Sender Policy Framework- convenio de remitentes en español)* de todos los dominios bajo su responsabilidad, asociándolos a los nodos de correo que efectúen el encaminamiento de salida SMTP (servidores de primer nivel)[4].

   Esto posibilita que se ponga a disposición de todos los servidores de correo con los que se intercambia mensajería la relación de servidores autorizados a estos fines. Lo anterior disminuye la probabilidad de materialización de posibles ataques y/o el aumento de la carga en el servicio por mensajes devueltos.

8. Chequeo de registro SPF en el flujo de entrada.

   Deben configurarse en cada red los servidores de primer nivel para que se lleven a cabo los correspondientes chequeos SPF del correo entrante. Este criterio establece en todo caso la posibilidad de analizar los mensajes entrantes a la red para determinar si se cumplen los registros SPF publicados por el responsable del dominio. Deben establecerse de igual forma las acciones a ejecutar ante los mensajes que no superen el test aplicado.

[3] RFC2821.
[4] RFC4408.

9. Control de destinatarios existentes.

   Deben aplicarse en cada red los mecanismos de rechazo en los servidores de nivel base para los mensajes dirigidos a destinatarios no existentes.

10. Control de flujo SMTP.

    Debe disponerse en cada red de mecanismos de control de flujo en las transacciones SMTP internas y externas. Estos mecanismos permiten controlar el número de correos enviados por una IP en un intervalo de tiempo determinado.

11. Sincronización de tiempo.

    En el servicio de correo electrónico se configura correctamente la zona horaria y deben sincronizarse todos los servidores de correo electrónico de las organizaciones tanto de primer nivel como nodos intermedios y servidores de almacenamiento[5] con un servidor de la propia red u otro que ofrezca el servicio, se puede utilizar NTP *(Network Time Protocol en inglés - protocolo de red de tiempo en español*).

12. Acceso cifrado.

    Debe considerarse en cada red ofrecer el servicio basado en protocolos de recogida de mensajes con cifrado SSL/TLS[6] (POPs, IMAPs)[7] y un servicio de correo saliente SMTP con TLS, así como acceso al correo por Web vía HTTPs para los usuarios externos. Debiendo tramitar la aprobación, de conformidad con la legislación vigente, acerca de la utilización de cualquier tipo de aplicación o servicio soportado que implique el cifrado de la información.

13. Servicio Antivirus.

    Debe disponerse en cada red de un servicio antivirus que analice tanto los mensajes entrantes como los salientes en los servidores de correo. De igual forma, se deben establecer las acciones a ejecutar en cada caso detectado (eliminación del adjunto infectado sustituyéndolo por un aviso, puesta en cuarentena del mensaje completo, eliminación, aviso al remitente, entre otras).

14. Autenticación.

    Debe implementarse en cada red la autenticación con el fin de elevar los niveles de seguridad y eficacia del servicio de correo electrónico, prevenir la fuga de datos, así como de disminuir la posibilidad de que su dominio sea utilizado como "puente" para el envío de correos masivos, puede implementarse SMTP.

[5] RFC3172/ RFC4330.
[6] SSL/TLS protocolos para establecer comunicaciones seguras usando certificados digitales.
[7] POPs, IMAPs protocolos de internet que permiten el acceso a cuentas de correo de su espacio WEB.

15. Servicio de cambio de contraseña.

    El servicio debe ofrecer al usuario la posibilidad de cambiar su contraseña, de forma autónoma e inmediata, sin intervención de un tercero y con el objetivo de garantizar la privacidad de la misma. De igual forma debe exigir los requisitos para la utilización de contraseñas como método de autenticación establecidos en la legislación vigente.

16. Servicio antispam.

    Debe disponerse en cada red de un servicio antispam que analice los mensajes entrantes y actúe sobre aquellos que considere spam según la política interna establecida y su correspondencia con la legislación vigente al respecto.