PROYECTO DE RECOMENDACIÓN TÉCNICA: ESPECIFICACIONES PARA LA CREACIÓN, ESTRUCTURACIÓN Y USO DEL CORREO ELECTRÓNICO INSTITUCIONAL EN LOS ÓRGANOS Y ENTES DEL ESTADO.

Índice de contenido

Capítulo I: Exposición de Motivos.

1. Nombre del proyecto

"Especificaciones para la Creación, Estructuración y Uso del Correo Electrónico Institucional en los Órganos y Entes del Estado".

2. Diagnóstico

En la actualidad, con la expansión y crecimiento logrado por las tecnologías de información, el uso de las comunicaciones electrónicas forma parte de la cotidianidad de las servidoras y servidores públicos. Por si fuera poco, el marco legal venezolano, ha otorgado validez a los mensajes de datos con la misma eficacia probatoria que la atribuida a los documentos escritos.

Bajo este contexto, el correo electrónico institucional se erige como una herramienta de trabajo que permite a las servidoras y servidores públicos agilizar sus procesos internos y mejorar la comunicación con otras instituciones públicas, las ciudadanas y los ciudadanos. Sin embargo, no existen lineamientos unificados en cuanto a la gestión y uso del correo electrónico institucional en los órganos y entes de la Estado, que contribuyan a agilizar el intercambio de información en las instituciones y entre éstas y los ciudadanos , así como al uso eficiente y racional de dicho recurso.

3. Antecedentes

Para la realización de la presente recomendación técnica se tomó como referencia el documento de Recomendación de Norma Técnica de Formularios Electrónicos resultante de la mesa de trabajo constituida en el año 2009 por la Oficina de Normalización del Centro Nacional de Tecnologías de Información (CNTI).

4. Justificación

El presente proyecto de recomendación técnica pretende homogeneizar la imagen del Estado Venezolano en cuanto a las comunicaciones que se hagan a través del correo electrónico institucional en las instituciones públicas en el marco del cumplimiento de sus competencias, funciones y procesos, según lo establecido en la Ley sobre Mensajes de Datos y Firmas.

5. Base normativa.

5.1. Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas.

5.2. Ley Especial Contra Los Delitos Informáticos.

5.3. Decreto con Rango, Valor y Fuerza de Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los Órganos y Entes del Estado.

5.4. Providencia Administrativa No 009-10 publicada por SUSCERTE sobre Normativa de

Clasificación y Tratamiento de la Información en la Estado.

Capitulo II: Generalidades

1. Objeto

El presente proyecto de recomendación técnica tiene por objeto estandarizar la creación, estructuración y condiciones de uso de los correos electrónicos institucionales como herramienta de comunicación e intercambio de información destinada a la optimización de la gestión electrónica en el ejercicio de la función pública, con el fin de racionalizar y maximizar el uso de dicho recurso, agilizar la comunicación intra e interinstitucional y garantizar el derecho de la ciudadanía a la participación y a obtener oportuna respuesta de sus trámites y demás asuntos de su interés, conforme los principios de celeridad, eficacia, eficiencia, transparencia, economía y prescindencia de formalidades no esenciales.

2. Ámbito de aplicación

La presente propuesta de recomendación técnica está dirigida a los órganos y entes del Poder Público Nacional, Estadal y Municipal, las personas de derecho público nacionales, estadales y municipales y demás entes de carácter público, así como, a las universidades públicas nacionales autónomas y experimentales, centros y colectivos de investigación y desarrollo y cualquier otra institución de los sectores universitario, académico, científico o tecnológico de naturaleza pública.

3. Definiciones

A los efectos del presente proyecto de recomendación técnica, se entenderá por:

3.1. **Alias:** Nombre que se declara dentro del servidor de correo, para direccionar información entre una o varias cuentas de correo asociadas a través de éste; podrán recibir información una o varias cuentas de correos suscritas al alias.

3.2. **Autenticidad:** Certeza respecto de la persona a quien se le atribuye la autoría de un mensaje de datos o firma electrónica.

3.3. **Clasificación de la información:** Valoración del contenido de los mensajes de datos como elemento determinante para el acceso de estos en función de sensibilidad y/o relevancia de la información, pudiendo ser: de uso público, de uso interno, confidencial y estrictamente confidencial.

3.4. **Código malicioso:** Serie de instrucciones que ejecutan rutinas de programación para causar daños en las plataformas tecnológicas con el propósito de usurpar identidades, enviar correo masivos, propagación de virus, extracción de información, denegación de servicios, demás fraudes electrónicos y delitos informáticos.

3.5. **Correo electrónico:** Servicio que permite el intercambio de mensajes de datos mediante sistemas de comunicación electrónicos, a través del uso de receptores interconectados,

de forma expedita, entre un número indeterminado de destinatarios, sin distingo de su ubicación geográfica.

3.6. **Mensaje de datos no deseado (Spam):** Mensaje de datos enviado generalmente por un emisor desconocido y de forma masiva usualmente para colapsar la red o con fines comerciales.

3.7. **Criptografía:** Rama inicial de las matemáticas y en la actualidad también de la informática, que hace uso de métodos y técnicas con el objeto principal de hacer ilegible, cifrar y proteger un mensaje o archivo por medio de un algoritmo, usando una o mpas claves.

3.8. **Criptología**: Ciencia que estudia la transformación de un determinado mensaje en un código de forma tal que a partir de dicho código solo personas autorizadas sean capaces de recuperar el mensaje original.

3.9. **Destinatario:** Persona a quien va dirigido el Mensaje de Datos.

3.10. **Documento electrónico:** Todo soporte de información producida, recibida, enviada, almacenada, organizada, usada y procesada por medios electrónicos o migrada a estos, a través de un tratamiento automatizado y que requiera de una herramienta específica para ser legible o recuperable.

3.11. **Emisor**: Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.

3.12. **Esteganografía:** Rama de la criptología que estudia y aplica las técnicas que permiten ocultar mensajes u objetos dentro de otros impidiendo así la detección de la información por parte de un tercero.

3.13. **Firma electrónica:** Información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

3.14. **Generador de respuesta automática:** función que le permite al usuario el envío de respuestas automáticas a correos electrónicos entrantes.

3.15. **Lista de distribución de correo:** Servicio controlado y moderado por un administrador, asociado al correo electrónico que permite la distribución masiva de información entre múltiples usuarios previamente suscritos haciendo uso de un alias.

3.16. **Mensajes de datos:** Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

3.17. **Nombre de dominio:** Es aquel que representa un identificador común a un grupo de computadoras o equipos conectados a la red, constituyendo una forma simple de dirección de Internet diseñados para permitir a los usuarios localizar de una manera fácil sitios en Internet.

3.18. **Redes inalámbricas abiertas:** puntos de acceso inalámbricos sin validación de un proveedor que garantice la confiabilidad de su uso.

3.19. **Servidora y Servidor Público:** toda persona investida de funciones públicas, permanentes o transitorias, remuneradas o gratuitas, originadas por elección, nombramiento, designación o contrato otorgado por la autoridad competente, que desempeñe actividades o funciones en nombre o al servicio de los órganos y entes del Estado.

3.20. **Usuario:** toda persona que utilice el servicio de Correo Electrónico.

Capitulo III: De la Creación del Correo Electrónico Institucional

1. Servicio de correo electrónico

Se recomienda que cada órgano y ente de la Estado cuente con un servicio de correo electrónico institucional que le permita agilizar sus procesos internos, así como mejorar la comunicación entre ellos, con otras ramas de los poderes públicos y las ciudadanas y los ciudadanos. Para el logro de dicho objetivo, es indispensable la creación de una cuenta de correo electrónico institucional por cada servidora y servidor público que preste servicios a la institución.

2. Configuración del nombre de usuario.

El establecimiento de un esquema similar para la creación de las cuentas de correo electrónico institucionales, garantiza la uniformidad y estandarización de los mismos por parte de los órganos y entes de la Estado. A tal efecto, se recomienda implementar la siguiente configuración:

1. Inicial del primer nombre	2. Primer apellido	3. Símbolo	4. Dominio de segundo nivel (Acrónimo o siglas del órgano o ente del Estado)	5. Dominio genérico de primer nivel	6. Dominio de primer nivel en código de país
j	perez	arroba (@)	Ej. CNTI	.gob/ .mil/ .edu/ .org/ .com	**.ve**

3. Duplicidad en el nombre de usuario

Para evitar la duplicidad en los nombres de usuarios y garantizar la unicidad de los mismos, es imprescindible establecer políticas internas dirigidas a atender las posibles variables complementarias que permitan la diferenciación de cada nombre de usuario. En este sentido, se recomienda adoptar el siguiente esquema de solución:

1. Inicial	2. Primer	3. Inicial	4. Símbolo	5. Dominio de segundo	6. Dominio genérico de primer	7. Dominio de primer

del primer nombre	apellido	del segundo nombre o apellido		nivel (Acrónimo o siglas del órgano o ente del Estado)	nivel	nivel en código de país
j	perez	z	arroba (@)	AEj. CNTI	.gob/ .mil/ .edu/ .org/ .com	.ve

En el caso de los órganos y entes del Estado cuya organización disponga de multiplicidad de sedes a nivel nacional, o estén conformados por un considerable número de servidoras y servidores públicos, podrán asignar una codificación complementaria de cuatro caracteres numéricos ubicados antes del símbolo arroba (@) en la estructura de la cuenta del correo electrónico institucional, considerando la variable que se presenta a continuación:

1. Inicial del primer nombre	2. Primer apellido	3. Inicial del segundo nombre o apellido	4. Codificación Numérica	5. Símbolo	6. Dominio de segundo nivel (Acrónimo o siglas del órgano o ente del Estado)	7 Dominio genérico de primer nivel	8. Dominio de primer nivel en código de país
j	perez	z	1256	arroba (@)	Ej. CNTI	.gob/ .mil/ .edu/ .org/ .com	.ve

Sin menos cabo de lo señalado anteriormente, los órganos y entes podrán establecer, en sus políticas internas, cualquier otra forma de configuración del correo electrónico institucional que permita identificar de una forma ágil, segura y certera a cada servidora y servidor público.

4. Cuentas de correo electrónico colectivas

Se recomienda la creación adicional de cuentas de correo electrónico institucionales colectivas para uso interno o externo que atiendan a las funciones, servicios específicos y necesidades asociadas a las unidades administrativas de cada órgano y ente de.

5. Configuración de cuentas de correo colectivas

En caso de ser necesaria la creación de cuentas de correo electrónico institucionales colectivas, se deben establecer en las políticas internas mecanismos que permitan identificar de forma ágil, segura y certera a la institución y los servicios específicos que se presten a través de éstas, recomendándose como primera alternativa de configuración la siguiente:

1. Nombre del Servicio o unidad organizativa	2. Símbolo	3. Dominio de segundo nivel (Acrónimo o siglas del órgano o ente del Estado)	4. Dominio genérico de primer nivel	5. Dominio de primer nivel en código de país
Ej. presidencia despacho consultoríajuridica contrataciones compras comunicaciones	arroba (@)	AEj. CNTI	.gob/ .mil/ .edu/ .org/ .com	.ve

6. Asignación de clave de acceso

Los órganos y entes del Estado deben asignar la contraseña inicial a fin de garantizar el acceso al correo electrónico, la cual debe ser cambiada inmediatamente por la servidora y el servidor público, conforme a lo dispuesto en el artículo 46 de la presente recomendación técnica.

Capítulo IV: De la estructura de los Correos Electrónicos Institucionales

7. Formato Texto plano

La utilización del formato de texto plano en toda la estructura del correo electrónico institucional garantiza la accesibilidad y compatibilidad con cualquier plataforma receptora.

8. Conformación

La estructura de los correos electrónicos institucionales estará conformado por los siguientes elementos:

8.1. Encabezado: destinatario y asunto
8.2. Cuerpo.
8.3. Firma.

9. Encabezado.

En el encabezado de los correos electrónicos institucionales, además del destinatario deberá completarse obligatoriamente el campo del asunto.

10. Campos opcionales del destinatario

Los servidores y servidoras públicas podrán enviar un correo electrónico a más de un destinatario. En el caso de requerirse poner en conocimiento a otros destinatarios distintos de los receptores principales, se incluirán las respectivas direcciones en el campo denominado “con copia” (CC). Siempre que sea necesario garantizar la privacidad de las direcciones de correos entre los destinatarios deberán utilizar el campo “con copia oculta” (CCO). El campo “responder a” debe usarse para incorporar un destinatario diferente al emisor del correo electrónico institucional.

11. Asunto

En el asunto del correo electrónico, la servidora o el servidor público deben indicar de forma clara y sintetizada el contenido del correo electrónico, evitando el uso de frases imprecisas en su descripción. Los órganos y entes del Estado deben contemplar en sus políticas internas las mejores prácticas para tales fines.

12. Cuerpo

El correo electrónico institucional es un instrumento de comunicación formal destinado a apoyar funciones en el ámbito laboral de las servidoras y servidores públicos y como tal debe ser utilizado. Su contenido debe ser puntual y concreto; a tal fin se evitará el uso de:

12.1. Lenguaje coloquial, peyorativo y ofensivo.
12.2. Figuras o iconos que representen emoción.
12.3. Mayúsculas sostenidas.
12.4. Signos repetitivos de exclamación, puntuación e interrogación.
12.5. Fuentes privativas.
12.6. Fondos decorativos o de colores.

Así mismo, en su redacción se deben contemplar las reglas de ortografía y considerar la utilización del corrector ortográfico.

13. Firma

La firma del correo electrónico institucional debe contener la identificación institucional de la servidora o servidor público en formato texto plano, indicando la siguiente información:

13.1. Nombre y apellido.
13.2. Cargo.
13.3. Datos de la unidad administrativa de adscripción.
13.4. Nombre del órgano o ente.
13.5. Números telefónicos de oficina y celular institucional.
13.6. Derecho de uso, de conformidad con lo previsto en el apartado 23.

En caso de que el órgano o ente lo considere necesario y por razones de organización institucional, podrán incorporarse otros datos como parte de la firma del correo electrónico institucional.

Capítulo V: De las Condiciones de Uso

14. Condiciones de Uso

Es indispensable que los órganos y entes del Estado definan sus políticas internas de administración y condiciones de uso del correo electrónico institucional de acuerdo con sus necesidades, lo establecido en la presente recomendación técnica y demás normativa aplicable.

15. Gestión de cuentas de correo colectivas

La cuentas de correo colectivas deben contar con una herramienta de gestión que facilite a los administradores la habilitación y deshabilitación de miembros, la suscripción y desuscripción de cuentas, filtrar contenido de correos, ocultar las direcciones de correo de los suscriptores.

16. Notificación de políticas de uso

Los órganos y entes del Estado deben notificar al servidor público en el momento de su ingreso a la institución, sobre las Condiciones de Uso del correo electrónico institucional, establecidas a tales efectos.

17. Titularidad de la cuenta de correo.

La titularidad del correo electrónico institucional corresponde al órgano o ente del Estado que la haya creado, independientemente del nombre y clave de acceso que sean necesarias para su uso. En virtud de ello, el titular está facultado para acceder a la información cursada por ese medio, con fines estrictamente institucionales.

18. Uso legítimo

El correo electrónico institucional asignado a una servidora o un servidor público bajo derecho de uso exclusivo, debe ser utilizado únicamente por elloss, como una herramienta de comunicación para las gestiones inherentes al órgano o ente de adscripción; que tendrá la misma eficacia probatoria que los documentos físicos. Las cuentas de correo electrónico colectivas se administrarán conforme a los lineamientos de cada órgano o ente del Estado.

19. Función del Correo Electrónico Institucional

El correo electrónico institucional es una herramienta de trabajo que debe ser utilizado con fines y objetivos relacionados con las funciones propias a la actividad administrativa de los órganos y entes del Estado. En consecuencia, se deben adoptar las políticas necesarias que prohibiban usar el correo electrónico institucional para:

19. 1. Atender asuntos personales, diligencias, negocios y otros de carácter e interés particular.
19. 2. Gestionar, promover u ofrecer servicios ajenos a las funciones propias de la institución.
19. 3. Enviar o reenviar correos electrónicos que puedan contener códigos maliciosos, suplantación de identidad, correos tipo cadenas, chistes, burlas, entre otros.
19. 4. Enviar o reenviar correos electrónicos con mensajes discriminatorios, intimidatorios o de acoso, material fraudulento, con contenido sexual explícito, obsceno, difamatorio o ilícito.

20. Clasificación de la Información

Los correos electrónicos institucionales deben indicar expresamente en el texto, el tipo de información y de los documentos que contienen, según la clasificación y tratamiento, establecida por la autoridad competente en materia de seguridad de la información electrónica, diferenciando así si se trata de información “estrictamente confidencial”, “confidencial”, “de uso privado” o “de uso público”. Las figuras geométricas respectivas podrán ser incorporadas en el texto del documento adjunto.

21. Tratamiento de la Información

Toda información transmitida por el correo electrónico institucional debe ser debidamente resguardada por su emisor y por su destinatario. Su divulgación, utilización indiscriminada o contraria a los fines

institucionales, predefinida o no como estrictamente confidencial, está sometida al régimen sancionatorio aplicable de conformidad con la Ley. El ejercicio de las acciones a que hubiere lugar por parte de los órganos o entes de la Estado, estarán determinadas según el daño y la naturaleza del acto lesivo, pudiendo resultar objeto de sanciones disciplinarias, administrativas, civiles y/o penales.

22. Disponibilidad de la función de confidencialidad

Los órganos y Entes del Estado deben implementar en su plataforma tecnológica los mecanismos que permitan la activación de la función de confidencialidad de la información por parte de la servidora o servidor público emisor del correo electrónico institucional.

23. Derecho de Uso de Información Institucional

La remisión de correos electrónicos institucionales debe considerar aspectos relacionados con las políticas de uso de la información institucional, tales como privacidad y confidencialidad, incluyéndolas en una nota al pie de página, tal y como se sugiere a continuación:

> "Este mensaje y sus adjuntos se dirigen exclusivamente a su destinatario, puede contener información *(estrictamente confidencial/ confidencial/ de uso privado/ de uso público)* y es para uso exclusivo de la persona o entidad de destino. Si no es usted el destinatario a quien va dirigida la información, queda notificado que la lectura, utilización, transmisión, divulgación o la reproducción total o parcial sin autorización, está prohibida y sancionada de conformidad con la legislación vigente. Si ha recibido este mensaje por error, notifíquelo al emisor y proceda a eliminarlo de su buzón."

24. Respuesta automática

En caso que la servidora o el servidor público se ausente de la institución por motivo de permisos prolongados, vacaciones, comisión de servicio, u otras razones que así lo ameriten, deberá activar el generador de respuestas automáticas informando a todo aquel emisor que le remita un correo electrónico, que en virtud de su ausencia deberá comunicarse con otra dirección de correo, la cual señalará expresamente, desactivando el generador a la fecha de su reincorporación; o en su defecto redireccionar la recepción de correos a otra cuenta destino seleccionada para tal fin.

A tal efecto, se recomienda a los órganos y entes del Estado implementar la funcionalidad de activación del generador de respuesta automática en los servidores y clientes de correo, a fin de que la servidora y el servidor público pueda disponer del mismo cuando sea necesario.

25. Capacidad del almacenamiento del correo electrónico.

Es indispensable que los buzones de correo electrónico dispongan de una capacidad de almacenamiento definida según las políticas internas de cada órgano y ente del Estado, la cual deben ser notificada a las servidoras y servidores públicos.

26. Mecanismos informativos de almacenamiento.

Se recomienda la implementación de mecanismos que le permitan a los usuarios estar informados del nivel de almacenamiento alcanzado en su buzón de correo electrónico.

27. Limite del tamaño de los mensajes de datos y el uso de archivos adjuntos.

A fin de racionalizar y maximizar el uso de los servidores de correo, se recomienda que la regulación interna del uso del correo electrónico institucional contenga, sin menoscabo de otras políticas que se establezcan, los siguientes extremos en cuanto a deberes y obligaciones de uso:

27.1. Cuando sea indispensable remitir documentos que estén disponibles en una página web, se debe enviar un enlace al mismo en lugar del documento como adjunto.

27.2. Los archivos que se adjuntan en los correos electrónicos deben, en lo posible, comprimirse con el software adecuado cuando esta compresión suponga un ahorro significativo de espacio, evitando así la degradación del servicio de correo y la saturación involuntaria de las casillas de los usuarios.

27.3. En los casos que sea necesario el envío de archivos adjuntos de gran tamaño o que están dirigidos a varias personas, se recomienda la implementación de servicios de envío de documentos, los cuales permiten enviar en el texto sólo enlaces a los documentos finales. De este modo, no se multiplicará por el número de destinatarios el espacio ocupado por el documento original y se evita que el envío sea rechazado por sobrepasar las limitaciones impuestas por el servicio de correo, así como saturar los buzones.

27.4. No debe permitirse en los correos electrónicos el uso de fondos prediseñados o imágenes innecesarias , toda vez que incrementan el tamaño del mensaje.

27.5. Las firmas automáticas y cualquier otro tipo de texto de inclusión automática debe ser lo más esquemática posible. En este sentido, no se recomienda incluir imágenes o información innecesaria sino limitarlas los datos de contacto esenciales.

28. Correos maliciosos

Las servidoras y servidores públicos deben eliminar sin ser leídos los correos no deseados o con contenido malicioso que ingresen a su bandeja de correo electrónico. Asimismo, se debe notificar tal circunstancia inmediatamente a los administradores de correo de la institución.

A tal efecto, es fundamental implementar una política informativa sobre el buen uso de la plataforma de correo institucional haciendo énfasis en el manejo de correos no deseados o con código malicioso a fin de evitar posibles ataques informáticos que comprometan la plataforma tecnológica.

29. Desactivación

Es importante la desactivación inmediata las cuentas de correo electrónico institucionales de las servidoras y los servidores públicos que cesen en sus actividades laborales, procediendo a efectuar el respaldo de la información contenida en dichas cuentas. Una vez garantizado el respaldo se debe suprimir definitivamente la cuenta de correo electrónico.

30. Respaldo de la Información

El respaldo de la información contenida en los correos electrónicos debe realizarse de manera organizada, útil, confiable y oportuna de acuerdo a las políticas internas de resguardo de la información, garantizando su disponibilidad y acceso de conformidad con lo establecido en la ley.

Capítulo VI: De la interacción electrónica de los servidores públicos con la ciudadanía

31. Cuentas de correo electrónico de atención a la ciudadanía

Es indispensable que los órganos y entes del Estado dispongan de cuentas de correo electrónico de atención a la ciudadanía, mediante las cuales puedan recibir consultas, opiniones, solicitudes, quejas y reclamos. Las servidoras y los servidores públicos están obligados a dar respuesta oportuna y veraz, de acuerdo con los principios y valores contemplados en la Constitución de la República Bolivariana de Venezuela y demás normativa vigente.

32. Gestión de cuentas a la ciudadanía

Por razones de especifidad funcional, la administración y uso de de las cuentas de correo electrónico, dedicadas a la interacción directa con la ciudadanía, debe estar a cargo de las Oficinas de Atención Ciudadana de los órganos y entes del Estado.

33. Estadísticas de atención a la ciudadanía

Se recomienda que cada órganos y ente del Estado, a través de las cuentas de correo electrónico de atención a la ciudadanía, establezcan y dispongan de un sistema de gestión de estadísticas de atención a la ciudadanía , diferenciada en tipo de trámite y tiempo de atención, con la finalidad de fortalecer el Gobierno Electrónico.

Capítulo VII: De las Condiciones de Seguridad Informática

34. Locación del servidor de correo electrónico

Se recomienda que los servidores de correo electrónico estén instalados dentro de las instalaciones de cada órgano o ente del Estado; en caso de no ser posible, se recomienda que el mismo esté alojado en servicios de hospedaje en el territorio nacional.

35. Instrumentos internos

Los órganos y entes del Estado deben regular y garantizar mediante instrumentos internos las condiciones de seguridad de la infraestructura informática necesarias para el acceso a las cuentas de correo electrónico asignadas a las servidoras y servidores públicos. Tales instrumentos consisten en:

35.1. Certificados digitales para la firma y cifrado de mensajes electrónicos del funcionario cuyo origen sea un proveedor de certificados avalado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

35.2. • Clientes de Correo (MUA) homologado y avalado por VENCERT que cuente con soporte S/MIME y OpenPGP.

35.3. • Portal para acceso webmail con soporte HTTPS.

35.4. • Servidores institucionales de correo con certificados digitales incorporados cuyo origen sea un proveedor de certificados avalado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

35.5. • Servidores institucionales de correo con soporte TLS/SSL para el cifrado de transporte y SMTP-AUTH para autenticación de usuarios remotos.

35.6. • Cuentas VPN para garantizar a los Servidoras y Servidores públicos acceso remoto a los Clientes de Correo dentro de la institución.

36. Filtrado de correos electrónicos

Los órganos y entes del Estado deben implementar mecanismos técnicos que filtren y disminuyan la recepción de correos electrónicos no deseados o con código malicioso. En este sentido se recomienda configurar los servidores responsables que funcionen como agentes de transporte de correo (MTA) para que implementen los siguientes controles:

• Rechazar cualquier conexión a los puertos TCP 25 ó TCP 587 desde un origen desconocido o que no tenga un registro PTR asociado a un servicio DNS.

Implementar protección contra la falsificación de direcciones en el envío de correo electrónico a través de la configuración de registros SPF en DNS para la Identificación de los servidores de correo SMTP autorizados para el transporte de mensajes.

• Configurar software de filtro Anti SPAM en el MTA responsable por entregar los correos al Agente de entrega de correo (MDA), también en este caso se recomienda la mejor práctica de separar este MTA del MDA .

Soporte de verificación de remitente contra Listas Grises implementadas localmente.

Soporte de verificación de remitente contra listas negras de servicios externos.

• Configurar software antivirus en el MTA responsable por entregar los correos al Agente de entrega de correo (MDA), se recomienda a este particular la mejor práctica de separar este MTA del MDA .

• Protección contra ataques basados en la vulnerabilidad Smtp Open Relay a través de la Implementación del método de SMTP Autenticado (SMTP AUTH) en el MTA responsable por gestionar el envío de correo.

37. Mensajes cifrados

En caso que los órganos y entes del Estado requieran enviar información clasificada como "estrictamente confidencial", se recomienda el uso de clientes de correo con soporte de la versión 3 del estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME conocido como S/MIME v3, utilizando para el cifrado del mensaje un certificado digital emanado por una entidad certificadora avalada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). Se insiste en la recomendación del uso de S/MIME sobre opciones alternativas como OpenPGP ello por cuanto S/MIME depende de un modelo jerárquico que involucra a una "Autoridad de Certificación centralizada" lo que coadyuva en la distribución de las claves públicas así como también

en la certificación de remitentes.

38. Firma Electrónica

Cuando la servidora o servidor público sea titular de una firma electrónica debidamente certificada por la Superintendencia de Servicios de Certificación (SUSCERTE), deberá utilizarla para la firma del correo electrónico institucional que emita, de conformidad con lo dispuesto en la Ley de Mensajes de Datos y Firmas Electrónicas.

39. Protección de la transferencia de datos de correo electrónico a nivel de la Capa de transporte

Los órganos y entes del Estado deben garantizar que por defecto los servidores de correo electrónico institucionales tienen habilitado de modo obligatorio el cifrado TLS para la protección del mensaje que viaja en texto claro desde el Agente de transporte de correo (MTA) institucional hasta el Agente de transporte de correo MTA destino.

Los órganos y entes del Estado deben garantizar que en los clientes de correo (MUA) configurados en los equipos de computación de las servidoras y servidores públicos se encuentra habilitado por defecto el soporte para cifrado TLS, ello en orden de garantizar la protección del mensaje que viaja en texto claro desde su computador (MUA) hacia el servidor institucional (MTA) también para garantizar la protección del mensaje desde el servidor institucional (MDA) hacia el computador de la servidora y servidor público (MUA).

40. Acceso remoto

Cuando los órganos y entes del Estado permitan el acceso remoto al correo electrónico institucional, deben prever y facilitar los mecanismos necesarios para garantizar la integridad de los mensajes de datos. En este sentido en una comunicación que implique acceso remoto directo al computador de la servidora o servidor público dentro de la institución y con el fin de tener acceso a su cliente de correo (MUA) el órgano/ente debe proveer al usuario una cuenta VPN para tal fin.

41. Acceso externo al correo electrónico institucional.

Las servidoras y los servidores públicos que ingresen a la cuenta de correo electrónico institucional desde dispositivos conectados a una red externa al órgano o ente del Estado, deben hacerlo a través de redes seguras entendiendo por seguras aquellas cuyo propietario es conocido y confiable, que no están abiertas al público y que cuentan con soporte de autenticación y cifrado basados en el protocolo WPA / WPA-PSK. Para fines de esta recomendación técnica los Routers y dispositivos de acceso basados en el protocolo WEP no se consideraran seguros.

Adicionalmente el acceso al buzón de correo institucional deberá suceder por intermedio del cliente del software de correo electrónico utilizado, considerando las facilidades de seguridad nativas del cliente S/MIME, OpenPGP, TLS, etc. Cuando no sea posible utilizar el cliente Específico o sea necesario acceder al buzón de correo a través de redes no seguras (por ejemplo: Internet) se debe utilizar el protocolo HTTPS.

42. Configuración de clave de acceso.

A fin de evitar accesos no autorizados a las cuentas de correo electrónico institucionales, se recomienda el establecimiento de claves alfanuméricas que contengan caracteres especiales, incluyendo minúsculas y mayúsculas, con un mínimo de diez (10) caracteres, las cuales deben ser modificadas

dentro del periodo establecido, conforme a lo dispuesto en el apartado siguiente de la presente recomendación técnica.

43. Vigencia de la clave de acceso

Los órganos y entes del Estado deben establecer el cambio obligatorio de la clave de acceso utilizada por las servidoras y servidores públicos la cual no debe contener más de cinco (5) dígitos iguales a la contraseña anterior, y debe actualizarse en un período máximo de ciento veinte (120) días continuos, a través de los mecanismos informáticos que disponga a tal efecto.