CM/ 827

Presidencia de la República Oriental del Uruguay

MINISTERIO DEL INTERIOR
MINISTERIO DE RELACIONES EXTERIORES
MINISTERIO DE ECONOMÍA Y FINANZAS
MINISTERIO DE DEFENSA NACIONAL
MINISTERIO DE EDUCACIÓN Y CULTURA
MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS
MINISTERIO DE INDUSTRIA, ENERGÍA Y MINERÍA
MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL
MINISTERIO DE SALUD PÚBLICA
MINISTERIO DE GANADERÍA, AGRICULTURA Y PESCA
MINISTERIO DE TURISMO Y DEPORTE
MINISTERIO DE VIVIENDA, ORDENAMIENTO TERRITORIAL Y MEDIO AMBIENTE
MINISTERIO DE DESARROLLO SOCIAL

Montevideo, 07 ABR 2014

VISTO: lo dispuesto por el artículo 149 de la Ley N° 18.719, de 27 de diciembre de 2010 y por el Decreto Nº 452/009, de 28 de setiembre de 2009;

RESULTANDO: **I)** que en el referido Decreto se determina la "Política de Seguridad de la Información para Organismos de la Administración Pública", con el propósito de desarrollar, implantar, mantener y mejorar continuamente un "Sistema de Gestión de Seguridad de la Información";

II) que en su artículo 1° se establece que las Unidades Ejecutoras de los Incisos 02 al 15 del Presupuesto Nacional, deberán adoptar en forma obligatoria una Política de Seguridad de la Información;

CONSIDERANDO: **I)** que a los efectos de dar cabal cumplimiento a lo dispuesto en la norma referida, es sustancial estandarizar los nombres de dominio de la Administración Central de forma tal de garantizar la transparencia y la seguridad;

II) que es fundamental garantizar a los ciudadanos, a los organismos y a sus funcionarios, la existencia de correos electrónicos institucionales seguros, motivo por el cual es imprescindible establecer los lineamientos mínimos de seguridad para el intercambio entre los mismos;

III) que la seguridad de la información es fundamental para el desarrollo del gobierno electrónico, por lo que resulta necesario que la Administración cuente con lineamientos para la implementación y uso de centros de datos seguros;

IV) que la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) tiene cometidos de fiscalización en materia de seguridad de la información, pudiendo apercibir directamente a los organismos que no cumplan con las normas y estándares en tecnología de la información establecidas por la normativa vigente, en lo que refiera a seguridad de los activos de la información, políticas de acceso, interoperabilidad e integridad de datos, tal como surge del artículo 74 de la Ley N° 18.362 de 6 de octubre de 2008;

V) que en cumplimiento de las disposiciones normativas vinculadas con la transparencia, la seguridad, el relacionamiento con la ciudadanía en el menor tiempo posible, es que se considera conveniente la elaboración de planes de acción tendientes a una ágil adecuación a los estándares que se indicarán como pertinentes;

ATENTO: a lo precedentemente expuesto, y a lo dispuesto en el artículo 168 ordinal 4º de la Constitución de la República;

EL PRESIDENTE DE LA REPÚBLICA
- actuando en Consejo de Ministros -
DECRETA:

Artículo 1º.- Los organismos de la Administración Central deberán utilizar nombres de dominio "gub.uy" o "mil.uy", éste último para el Ministerio de Defensa y sus dependencias, para todos los servicios vinculados con Internet, prohibiéndose la utilización de cualquier otro nombre de dominio, de acuerdo con los "Lineamientos

para la gestión y uso de nombres de dominio de Internet", que se anexa y forma parte del presente Decreto (Anexo I).

Artículo 2º.- Los organismos de la Administración Central para el ejercicio de sus funciones deberán utilizar sistemas de correos electrónicos institucionales con nombre de dominio ".gub.uy" o ".mil.uy", prohibiéndose la utilización de cualquier otro nombre de dominio, de acuerdo con los "Lineamientos para la implementación y uso de servicios de correo electrónico seguro", que se anexa y forma parte del presente Decreto (Anexo II).

Los funcionarios de los organismos de la Administración Central en el ejercicio de sus funciones estarán sujetos a igual prohibición.

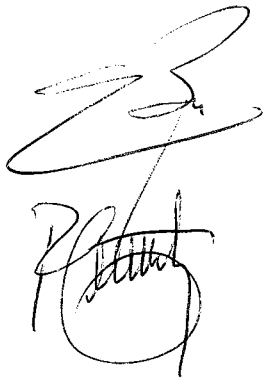
Artículo 3º.- Los sistemas informáticos (art. 3º del Decreto Nº 451/009 de 28 de setiembre de 2009) de la Administración Central deberán estar alojados en centros de datos seguros situados en territorio nacional, exceptuándose aquéllos que no constituyan un riesgo para el organismo, de acuerdo con los "Lineamientos para la implementación y uso de centros de datos seguros", que se anexa y forma parte del presente Decreto (Anexo III).

Artículo 4º.- Los organismos de la Administración Central deberán presentar a AGESIC un Plan de Acción para el cumplimiento de las disposiciones de este Decreto, en el plazo de 90 días desde su publicación.

Artículo 5º.- Se comete a AGESIC la fiscalización del cumplimiento de las normas establecidas en este Decreto, pudiendo contemplar excepciones por razones debidamente fundadas.

Artículo 6º.- Comuníquese, publíquese, etc.

JOSÉ MUJICA
Presidente de la República



Anexo I

Lineamientos para la gestión y uso de nombres de dominio de Internet

Objetivo

El objetivo de esta normativa es el de establecer los lineamientos para el uso y gestión de nombres de dominio por parte de la Administración Central, con el fin de garantizar un adecuado uso de nombres de dominio y la actualización de la información de contacto de sus responsables.

Alcance

Esta normativa tiene como alcance la totalidad de los nombres de dominio de internet utilizados por los organismos de Administración Central y sus dependencias.

Gestión y uso de dominios de internet

Identificación de dominios para portales web institucionales

Los portales Web institucionales de los organismos de la Administración Central y sus dependencias, deben identificarse con la extensión "gub.uy" o "mil.uy", según corresponda.

Identificación de dominios para portales Web de contenido genérico

Los portales Web institucionales de Unidades Ejecutoras, aplicaciones, portales y sitios web correspondientes a proyectos y programas, sitios promocionales y temáticos, incluyendo zonas restringidas de acceso mediante usuario y contraseña disponibles para ciudadanos y funcionarios del organismo (contenidos web) deberán ser subdominios del dominio del inciso correspondiente con excepción de los que justifiquen la necesidad de un dominio autónomo, lo que podrá efectuarse considerando: funciones y competencias, nivel de aprehensión ciudadana, capacidad de mantenimiento del sitio, disponibilidad de recursos o justificación de la necesidad. Dichas excepciones deberán ser validadas por AGESIC.

Se exceptúan a aquellos canales de comunicación que se justifiquen debidamente por su vínculo con la ciudadanía y su carácter público.

Referenciamiento de dominios y sub dominios

En cualquier caso, el portal del organismo jerarca deberá hacer referencia a todos los dominios y subdominios que se correspondan con todos los contenidos web que reporten a éste.

Nombres de Dominio

Los nombres de dominio del organismo o dependencias serán, sus iniciales, su acronismo, o el nombre con el cual se conoce públicamente al mismo y se justifique que sea más representativo que su nombre, acronismo o iniciales.

Información de contacto del responsable técnico del dominio/subdominio

La información de contacto de los responsables de los dominios y subdominios deberá ser comunicada y actualizada en períodos de seis meses a AGESIC.

Anexo II

Lineamientos para la implementación y uso de servicios de correo electrónico seguro

Objetivo

El objetivo de esta normativa es mejorar los niveles de seguridad del envío, recepción y almacenamiento de los servicios de correos electrónicos de dominios gubernamentales, con el fin de garantizar un adecuado nivel de confidencialidad de los mismos.

Alcance

Esta normativa tiene como alcance la totalidad de los servidores de correo electrónico implementados en dominios "gub.uy" o "mil.uy" (en adelante, dominios gubernamentales), las comunicaciones realizadas por éstos hacia servidores de terceros, y todos los correos electrónicos recibidos o enviados por los mismos.

Componentes implicados

Modelos de cifrado

Los correos electrónicos deben ser protegidos tanto en su generación, almacenamiento, como así también durante su transmisión y recepción, de manera que se garantice su confidencialidad durante toda su vida. Para ello es necesario aplicar diferentes modelos de cifrado dependiendo del contexto:

1. Cifrado a nivel del mensaje.

Se denomina cifrado de mensaje a un correo electrónico que ha sido cifrado haciendo uso de criptografías asimétricas, utilizando para ello un par de claves privadas/públicas las cuales fueron generadas y compartidas previamente por los usuarios. Estas claves deben ser intercambiadas adecuadamente a fin de evitar falsas identidades. Este

mecanismo también permite añadir una firma electrónica a un mensaje, de esta manera la totalidad del mensaje y el remitente pueden ser verificados.

2. Cifrado a nivel del canal de comunicación.

Se denomina que un canal de comunicación esta siendo cifrado cuando la comunicación entre 2 elementos que intervengan en el intercambio de un correo electrónico hacen uso de protocolos de transmisión que implementen algoritmos criptográficos robustos basados en estándares internacionales como (SSL, TLS).

MUA

Se denomina MUA (Agente de Correo de Usuario por sus siglas del inglés) al cliente de correo electrónico desde el cual el usuario gestiona los mensajes: creación, borrado, envío, lectura. El MUA es utilizado para enviar y descargar correo electrónico, a través del MTA correspondiente (ver punto siguiente)

Dentro de esta categoría se pueden identificar dos tipos de MUA bien definidos, por un lado los clientes pesados como por ejemplo (Outlook, Thunderbird, Mail, etc.), y por otro lado denominados clientes livianos o Web Mail los cuales son accedidos haciendo uso de un browser web. Éstos se encuentran alojados en un servidor web.

MTA

Se denomina MTA (Agente de Transferencia de Correo por sus siglas en inglés: Mail Transfer Agent) al sistema implantado en el servidor de correo capaz de recibir mensajes desde un MUA, procesarlos convenientemente y entregarlos a sus destinatarios mediante uno o más protocolos de comunicación. Típicamente, el MTA debe ser capaz de comunicarse mediante el protocolo SMTP –o sus extensiones- para enviar y recibir correos y, adicionalmente, suelen comunicarse mediante POP3 o IMAP para que los usuarios puedan gestionar sus buzones de correo.

Requerimientos de seguridad mínimos obligatorios.

Seguridad del servidor de correo

Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite la implementación de estos sobre tecnologías que no garanticen dicho requerimiento.

Seguridad de los canales de comunicaciones

Se debe garantizar que los correos electrónicos en tránsito entre dos MTAs, o entre un MUA y un MTA, no comprometa la confidencialidad de la información cuando esto sea posible.

Entre MTAs de dominios gubernamentales.

La implementación de canales de comunicación cifrados entre MTAs de dominios gubernamentales es mandatoria, y deberá implementarse utilizando SSL v3, TLS 1.0, STARTTLS o superior.

Los MTAs de dominios gubernamentales deberán interrumpir el intento de entrega o recepción de mensajes si este canal cifrado no se puede negociar.

Entre MTAs gubernamentales y MTAs de terceros.

La implementación de canales de comunicación cifrados con SSL v3, TLS 1.0, STARTTLS o superior entre MTAs de dominios gubernamentales y un MTA de terceros deberá ser el método preferido de comunicación.

Cuando el establecimiento de estos canales cifrados no sea posible, se podrá establecer un canal en texto claro.

Entre MUA y MTA de dominios gubernamentales.

La implementación de canales de comunicación cifrados entre MUAs y MTAs de dominios gubernamentales es mandatorio, y deberá implementarse utilizando SSL v3, TLS 1.0, STARTTLS o superior.

Los MTAs de dominios gubernamentales no deberán aceptar la descarga o entrega de correos por parte de MUAs si este canal cifrado no se puede negociar.

Los MTA no deberán aceptar la descarga o consulta de correos electrónicos sobre canales en texto claro.

Seguridad de los MUA

De implementar servicios de webmail estos deben ser implementados sobre el protocolo HTTPS utilizando un certificado de seguridad válido, y deberán estar alojados dentro del territorio nacional.

Los titulares de cuentas de correo de dominios gubernamentales no podrán acceder a sus cuentas desde servicios webmail que no sean el provisto por el organismo.

Cuando la información a transmitir vía email represente un riesgo alto para el organismo se recomienda implementar un modelo de cifrado a nivel de mensaje.

Anexo III

Lineamientos para la implementación y uso de centros de datos seguros

Objetivo

El objetivo de esta normativa es mejorar los niveles de disponibilidad, confiabilidad e integridad de los centros de datos utilizados por el Estado.

Alcance

Esta normativa tiene como alcance la totalidad de los centros de datos que alojen sistemas informáticos de la Administración Central, exceptuándose aquellos sistemas que no representen un riesgo para el organismo.

Requerimientos mínimos de sub sistemas de Infraestructura

Telecomunicaciones

Los sistemas críticos de telecomunicaciones, cableados, routers, switches LAN y switches SAN deben ser redundantes.

Arquitectura y Estructura

El sistema estructural del edificio debe ser de acero o de hormigón. Como mínimo, la estructura del edificio debe estar diseñada para soportar cargas de viento de acuerdo con los códigos de construcción aplicables para la ubicación en cuestión y de conformidad con las disposiciones de las estructuras designadas como instalaciones esenciales (por ejemplo, construcción de Clasificación III del Código Internacional de la Construcción).

Debe prever protección contra los principales eventos físicos, intencionales o accidentales, naturales o artificiales, que podrían causar una falla en el mismo.

Es requerido control de acceso físico, muros exteriores sin ventana, seguridad

perimetral, CCTV y protección contra incendio.

Electricidad

Se debe contar con un sistema generador de energía eléctrica con capacidad suficiente para abastecer todo el centro de datos.

Se debe contar con sistemas de alimentación ininterrumpida redundantes.

Se deben implementar unidades de distribución de energía (PDU) redundantes.

Para energizar los racks se deben implementar circuitos eléctricos redundantes y de tal manera que el fallo de uno de ellos no afecte a más de un rack.

Mecánica

El sistema de climatización debe implementarse con varias unidades de aire acondicionado cuya capacidad de refrigeración combinada mantenga constante la temperatura del espacio crítico y la humedad relativa a las condiciones de diseño.

El sistema de climatización debe contar con una redundancia que garantice los niveles de temperatura y humedad relativa en caso de falla o mantenimiento de uno de sus componentes.

Los sistemas de aire acondicionado deben estar diseñados para un funcionamiento continuo 7 días/24 horas/365 días/año.

El sistema de climatización debe ser alimentado por el generador de energía eléctrica.

Control de Acceso y Protección del Centro de Datos

Se deberá contar con los mecanismos de gestión que aseguren la protección y salvaguarda de los componentes físicos y lógicos, incluyendo entre otros la seguridad física, de la red de datos, de la infraestructura, así como protección contra incendios, desastres naturales o riesgos por fallas humanas.

Requerimientos de Gestión y Operación

Gestión de Monitoreo

Se recomienda contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos.

Disponibilidad y Niveles de servicio

Se deben definir acuerdos de niveles de servicio con los proveedores que den soporte a los componentes críticos del centro de datos y deben ofrecer cobertura en un régimen de 7 días/24 horas/365 días/año.