MARCO de CIBERSEGURIDAD

Uruguay Presidencia

agesic

SEGURIDAD DE LA INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

Guía Interpretación Decreto 92/014 ciberseguridad

Versión	1.0	**Categoría**	Guía
Última actualización	02/04/2014	**Estado**	Aprobado

Objetivos

El objetivo del presente documento es guiar en la interpretación del Decreto 92/014 en lo referente a: la gestión y uso de nombres de dominios de Internet, implementación y uso del servicio de correo electrónico y centro de datos seguros, así como sus correspondientes planes de acción.

Interpretación general del decreto

Dominios

El dominio es la "puerta de entrada", donde está alojada la información.
Los objetivos que se deben cumplir con el Decreto contribuyen a la mejora de la calidad de la Web del Estado, facilitando a los usuarios el acceso a la información y servicios publicados por los organismos y por ello se especifican medidas para,

- Fomentar el uso adecuado estandarizando los nombres de dominio de la Administración Central de forma tal de garantizar la transparencia y la seguridad.
- Garantizar la actualización de la información de contacto de sus responsables, de esta manera será posible contactarlos en caso de que ocurra un incidente de seguridad o se detecte algún inconveniente relacionado al sitio.
- Facilitar el acceso a la información a los usuarios racionalizando el uso de los dominios.

Correo electrónico

El objetivo detrás del decreto en lo que a Servicios de Correo Electrónico Seguro se refiere, es que la información (sea cual sea esta) sea transmitida de forma confiable, manteniendo su carácter de confidencialidad e integridad.

Para ello se pretende que los servicios de correo electrónico sean configurados de forma tal que contemplen la seguridad de los datos al momento de ser almacenados y transmitidos, utilizando para ello protocolos que permitan el cifrado de las comunicaciones.

Centro de datos

El objetivo detrás del decreto en lo que a Datacenter refiere, es que la información (sea cual sea esta) esté disponible, sea confiable e integra asegurada de acuerdo a la criticidad de la misma, en centros de datos acordes.

No se pretende que quien no cumpla con los requerimientos deba construir un datacenter, sino, consolidar sus centros de procesamiento de datos en alguno ya existente dentro del inciso. Es posible que algunos centros de datos puedan con pocos cambios acondicionarse y apegarse a las exigencias del decreto.

Lo anteriormente mencionado se alinea con la primera meta del Objetivo 10 de la Agenda Digital Uruguaya 2011-2015 que establece lo siguiente: “Consolidar las áreas de operación informática (Data Center) en la Administración Central, reduciendo a un tercio su número”

El alcance del decreto incluye todo lugar donde se procesan datos dentro de la Administración Central. Es decir, no solo abarca los centros de datos constituidos como tal, sino que también abarca todos aquellos sitios u oficinas en las cuales alojan servidores que publican servicios a internet o a la red interna.

Dominios

Portales Web Institucionales

Texto del decreto

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.”

Aclaración

Todos los servicios vinculados con Internet de los Organismos de la Administración Central deberán utilizar los nombres de dominio .gub.uy o mil.uy, este último para el Ministerio de Defensa. Es decir que no podrán existir servicios vinculados a internet de Organismos de la Administración Central con un nombre de dominio diferente a .gub.uy o .mil.uy, evitando el uso por ejemplo, de dominios com.uy o com.
Esto no implica que se registren dominios con otras extensiones con el fin de “reservar” el nombre de dominio por termas marcarios. Un ejemplo de esto son los dominios .uy, como ser, agesic.uy, pero estos no deben utilizarse, ni publicitarse.

Cada inciso deberá tener un único dominio identificado como gub.uy o mil.uy según corresponda, donde se publique el portal web institucional.

El nombre del dominio deberá seguir los lineamientos detallados en **Nombres de Dominio**.

Portales Web de contenido genérico

Texto del decreto

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.”

Aclaración
Con el objetivo de optimizar recursos y facilitar el acceso a la información a los ciudadanos, en general es deseable que se consoliden todos los dominios de las dependencias de un inciso (Unidades Ejecutoras, Áreas, Oficinas, etc.) en un solo dominio del inciso en un portal orientado al ciudadano.

Sin embargo, es posible asignar un subdominio del dominio del inciso sin perjuicio de ello estas dependencias podrán tener un subdominio del dominio del inciso siguiendo las mismas recomendaciones de nomenclatura realizadas para el caso de Portales Web Institucionales del Inciso.
Lo mismo aplica a las aplicaciones, proyectos, programas, portales promocionales y temáticos que serán subdominios del dominio del inciso.
Ejemplo de los subdominio, para la Unidad Centralizada de Adquisiciones, dependiente del MEF, el subdominio sería: uca.mef.gub.uy

Excepciones que requieran dominio autónomo:
En caso de ser necesario necesario contar con un dominio autónomo se deberá solicitar a AGESIC la excepción del cumplimiento para dicho dominio, con la justificación correspondiente.
Para justificar la excepción AGESIC se considerara:

- **Funciones y competencias**. Si las acciones o tipo de información que brinda el portal es muy específico, o por cuestiones relacionadas a la identidad o del plan de comunicaciones.
- **Nivel de aprehensión ciudadana**: Para el caso de los dominios ya existentes, si los ciudadanos ya conocen y usan ampliamente un dominio en particular, se podrá solicitar una excepción, contando con un registro de acceso al sitio que lo justifique.
- **Justificación de la necesidad**: Pueden darse situaciones diferentes a las descriptas que se analizarán debidamente.
- **Capacidad de mantenimiento del sitio y disponibilidad de recursos**: Para todas las excepciones se solicitará un plan de negocio del sitio que garantice el mantenimiento del sitio.

Excepciones de otros canales
Se exceptúan los canales de comunicación que por su vínculo con la ciudadanía y su carácter público no puedan adaptarse al cumplimiento de este decreto, como por ejemplo Facebook, Twitter, Youtube, etc.

Referenciamiento de dominios y subdominios

Texto del decreto
Referenciamiento de dominios y subdominios
"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."

Aclaración
En todos los casos en que un Inciso o sus unidades ejecutoras dependientes cuenten con varios dominios y/o subdominios, éstos deben estar referenciados en el Portal Web del Inciso, de una manera que resulte claro y fácil de encontrar para el ciudadano.

Nombres de Dominio

Texto del decreto

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."

Aclaración

Ejemplos:

a) **Sus iniciales:** para el Ministerio de Salud Pública: www.msp.gub.uy
b) **Su acrónimo:** para el Ministerio de Desarrollo Social: www.mides.gub.uy
c) **Nombre con el cual se conoce públicamente** y se justifique que sea más representativo que su nombre, acrónimo o iniciales: para Presidencia: http://www.presidencia.gub.uy/
d) Ejemplo de los subdominio, para la Unidad Centralizada de Adquisiciones, dependiente del MEF, el subdominio sería: uca.mef.gub.uy

Información de contacto

Texto del decreto

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."

Aclaración

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

La primera actualización se realizará con la entrega del plan de acción y para las siguientes actualizaciones se establecerá un mecanismo el cual será comunicado oportunamente.

Es necesario tener en cuenta la caducidad de los sitios para comunicar su baja cuando su contenido ya no sea necesario, de manera de evitar portales huérfanos.

Servicios de correo

Seguridad del servidor de correo

Texto del decreto

"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."

Aclaración

En este punto se pretende que los servidores de correo electrónico o Mail Transfer Agent (MTA) por sus siglas en inglés pertenecientes al gobierno o sea todo aquel que procese correos con dominios gub.uy se encuentren físicamente implementados dentro del territorio nacional. Esto significa que las interfaces de red que estén conectadas a

internet cuenten con direcciones IP públicas pertenecientes a los rangos asignados a Uruguay.

Con esto se busca que los correos electrónicos procesados y almacenados por dichos servidores se encuentren alojados dentro de la jurisdicción de la Republica Oriental de Uruguay.

Considerando que este punto también hace referencia al almacenamiento de los correos electrónicos, se debe considerar que cualquier repositorio o medio de almacenamiento en donde existan correos (servidores, respaldos, etc.) se encuentra dentro del alcance de este punto, no permitiéndose por ejemplo realizar ni trasladar respaldos de los mismos fuera del territorio nacional.

Este punto también hace referencias a aquellas tecnologías que no permitan cumplir con este requerimiento, como por ejemplo aquellos servicios de correo que estén soportado por infraestructuras Cloud las cuales estén distribuidas por el globo o proveedores que brinden dichos servicios también de forma distribuida dificultando la asociación de una dirección IP a un país en particular.

Seguridad de los canales de comunicaciones

Texto del decreto

"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."

Aclaración

En este punto se enuncia genéricamente la voluntad de proteger la seguridad de los correos electrónicos, preservando la propiedad de la confidencialidad en los mensajes transmitidos desde y hacia el servidor de correos electrónico, tanto para aquellas transferencias realizadas entre servidores de correo como así también las realizadas clientes de correo y servidores.

Para poder cumplir con este requerimiento es necesario implementar protocolos de transferencia seguros que hagan uso de algoritmos robustos de cifrado de datos, como lo pueden ser STARTTLS, S/MIME, POP3S, IMAPS.

En los siguientes enunciados se realizan especificaciones al respecto de si la comunicación es entre servidores de gobierno o no.

Entre MTAs de dominios gubernamentales

Texto del decreto

"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."

Aclaración
En este punto lo que se pretende es que todo correo electrónico intercambiado entre servidores gub.uy se realice únicamente utilizando protocolos seguros como SSLv3, TLS 1.0, STARTTLS los cuales hacen uso de cifrado robusto de datos.

Para ello se deberá configurar reglas de distribución de correos (dentro del software de plataforma utilizado) las cuales establezcan este requerimiento. La forma de realizar esta configuración puede variar entre las diferentes plataformas de correo existentes, AGESIC cuenta con guías de configuración para los servidores de correo más utilizados.

El requerimiento de la interrupción de intento de entrega no se deberá implementar hasta que AGESIC indique, debido a que para habilitar esto es necesario que todos los servidores de correo gubernamentales estén configurados correctamente. Mientras tanto, deberá configurarse el canal cifrado como método preferido (no mandatorio).

AGESIC comunicara de manera oportuna cuando la mandatoriedad de esto deba implementarse.

Entre MTAs gubernamentales y MTAs de terceros

Texto del decreto
"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."

Aclaración
Tal cual como lo establece este punto, siempre que se realice una transferencia de correos con un servidor de correo que no sea gubernamental o sea no pertenezca al dominio .gub.uy, siempre se deberá preferir el uso de protocolos seguros para realizar la misma. Esto se realiza con el objetivo de que todo correo intercambiado con servidores externos al ámbito gubernamental sea transmitido tratando de conservar la confidencialidad de los datos. Pero debido a que no todos los servidores implementados en internet soportan esta característica es necesario que el servidor pueda en su defecto realizar la transferencia del mensaje, para ello y como última opción se podrá realizar el envió del correo sin utilizar cifrado alguno.

Entre MUA y MTA de dominios gubernamentales

Texto del decreto

"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."

Aclaración
Aquí se pretende que siempre que un cliente de correo se conecte a un servidor para realizar la descarga o envió de mail lo pueda hacer únicamente a través de protocolos seguros.

Para ello es necesario que los servidores únicamente ofrezcan la posibilidad de conexión a través de protocolos seguros y además se debe adecuar la configuración de los clientes de correo para que utilicen los protocolos ofrecidos.
El intento de entrega o consulta de correos electrónicos entre clientes de correo y servidores de correo mediante protocolos inseguros deberá ser impedido.

Seguridad de los MUA

Texto del decreto
"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."

Aclaración
Un servicio de WebMail no deja de ser un MUA implementado en la Web y como todo MUA establece conexiones con el servidor de correo y realiza envió y recepción de mensajes. Además de esto también realiza la transmite información hacia el browser del usuario, transmisión que incluye los correos que el usuario recibe y envía. Es por esto último que es necesario proteger la confidencialidad de este tramo de la comunicación, entre el browser del cliente y el servicio Web y para esto se requiere el uso de SSL y la implementación de certificados digitales válidos y emitidos por una Autoridad Certificadora de confianza.

Hay que tener en cuenta que el servicio de WebMail podría estar implementado en un servidor diferente al servidor de correo y en consecuencia podría llegar a almacenar la información de los correos. Si tenemos en cuenta esto y que en el primer punto del decreto se requiere que los mails no sean almacenados fuera del territorio de la República Oriental del Uruguay, vemos que también aplica para los WebMail y es por esto que no se debe implementar ningún servicio de WebMail fuera de territorio nacional.

Centros de datos

Telecomunicaciones

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

Aclaración
Lo que se pretende en este punto es que la infraestructura de redes del centro de datos no tenga puntos únicos de falla, es decir, que la operativa del centro de datos pueda continuar aun ante la caída de un activo de red. La implementación de esto es muy variada, habiendo soluciones a nivel de capa 2 (del modelo OSI) como ser Spanning Tree, soluciones de Capa 3 como ser HSRP, soluciones mixtas e incluso soluciones propietarias del proveedor tecnológico de infraestructura de redes. Hay soluciones de implementación automática y otras de implementación manual.

No se pretende que ante la caída de un activo de red la operativa del centro de datos se mantenga la performance de la red ni que el 100% de las soluciones se mantengan disponibles, lo que si se pretende es que en caso de falla, las aplicaciones críticas del negocio puedan continuar funcionando y que estén documentados todos los procedimientos necesarios para continuar operando.

Arquitectura y Estructura

Texto del decreto
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.

Aclaración
Los activos críticos de información deben estar alojados en centros de datos cuya estructura y la del edificio que la contiene debe ser suficientemente robusta para soportar los eventos climáticos habituales en Uruguay, como ser lluvias, tormentas eléctricas, vientos fuertes. Los materiales de dicha estructura no pueden ser de materiales inflamables ni livianos. Los materiales de pisos, puertas y mamposterías tampoco podrán ser inflamables. Se recomienda además el uso de piso técnico elevado. Se deberá contar con un mantenimiento adecuado de la estructura que impida la filtración de humedades hacia el interior de la misma.

El centro de datos no podrá estar localizado en un sitio expuesto a inundaciones. Tampoco puede estar ubicado en zona donde el acceso se pueda ver afectado ya sea por condiciones naturales como humanas.

El acceso al Centro de Datos deberá estar asegurado y ser restringido. Para ello es requisito que los muros exteriores al recinto no tenga ventanas y se cuente con seguridad perimetral. Además debe contar con sistemas cerrados de TV y protección contra incendios (detección y extinción.)

En caso de incendio ya sea dentro del centro de Datos como fuera del mismo, el fuego no debe traspasar la barrera física del centro de Datos por el mayor tiempo posible.

Electricidad

Texto del decreto

"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."

Aclaración

Los cortes de energía en un centro de datos no solo impiden la continuidad de los servicios, sino que el apagado no programado del equipamiento puede ocasionar daños irreversibles en los mismos. Es por esto que es necesario tener esquemas redundantes de energía eléctrica para el centro de Datos. En Uruguay contamos únicamente con un único proveedor de energía eléctrica (UTE) por lo que contar con un respaldo de energía implica tener un generador de energía propio (o arrendado de uso exclusivo). Este generador debe ser dimensionado para poder abastecer la totalidad de carga eléctrica del centro de datos, pues de lo contrario fallará y no podrá cumplir con su cometido.

Contar con un generador no es suficiente, pues en caso de requerir su uso se producen interrupción de energía eléctrica entre que se detecta el corte en el suministro de la red y se enciende el generador. Es por esto que es necesario contar además con sistemas de UPS (sistema de energía ininterrumpido) a Baterías que puedan soportar la carga de todo el centro de datos durante estos cortes.

Al día de hoy casi todos los activos de un centro de datos, como ser servidores, switches, routers, firewalls, cuentan con alimentación redundante de energía eléctrica. Esto es porque es común que falle una línea de energía y los equipos están pensados para no interrumpir su funcionamiento en caso de una falla de estas. Para poder cumplir con este fin, es necesario que a este equipamiento le lleguen 2 líneas eléctricas independientes. Para proteger además los sistemas criticos del datacenter que no tengan doble fuente de energía, existen en el mercado dispositivos que se conectan a las 2 líneas eléctricas y que entregan una sola fase.

Finalmente, para minimizar el impacto de fallas eléctricas es que se solicita que las acometidas eléctricas desde el tablero general a cada rack sean exclusivas para dicho rack.

Mecánica

Texto del decreto

"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."

Aclaración
Los activos de Centros de Datos están diseñados para funcionar en un ambiente controlado de temperatura y humedad. Dadas las condiciones climáticas de Uruguay y sumado a que el equipamiento disipa importantes cantidades de Calor, es necesario contar con sistemas de aire acondicionado para mantener la temperatura controlada en las condiciones de diseño. Del mismo modo la humedad del ambiente también deberá mantenerse dentro de valores controlados.
Los sistemas de acondicionamiento térmico deben ser redundantes, pues en caso que fallen la temperatura del centro de datos puede alcanzar valores no deseados que provoque desde la falla en el equipamiento que cause la pérdida de su garantía, hasta un posible incendio.

Control de Acceso y Protección del Centro de Datos

Texto del decreto
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.

Aclaración
Este punto pretende reforzar algunos conceptos ya mencionados donde se mencionan los requerimientos de estructura y arquitectura.

Se debe contar con sistema autónomo de control de acceso, con lectores de tarjetas magnéticas, identificación por Radiofrecuencia (RFID) o sistemas biométricos. Estos sistemas deben ser administrados remotamente y deben mantener información histórica de accesos al centro de datos.

Los activos del centro de datos deberán estar protegidos con barreras físicas de forma de prevenir el daño de los mismos ya sea con o sin intención. Para esto se sugiere el uso de racks con puertas y cerraduras. Las instalaciones eléctricas deben estar protegidas de forma tal que evite el contacto no deseado con humanos. Es deseable que la sala de energía esté separada de la sala de cómputo. Todo esto se complementa con el sistema de Video Vigilancia que debe existir y debe poder registrar toda actividad dentro del recinto.

Se debe contar con sistema de detección y extinción de incendios. Estos deben contar con mantenimiento periódico que aseguren su correcto funcionamiento.

Desde el punto de vista lógico, toda la red de datos deberá estar protegida mínimamente con firewalls que permitan controlar los accesos ya sea desde redes públicas como de las redes privadas de la propia organización propietaria del centro de Datos.

Todos los activos deberán contar con contraseña de acceso, la cual es recomendable que sea personal e intransferible para los administradores de cada dispositivo.

Requerimientos de Gestión y Operación

Gestión de Monitoreo

Texto del decreto

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

Aclaración

Para administrar correctamente un Centro de Datos, es necesario que se realice un monitoreo permanente de todas las variables ambientales, del estado de salud de los activos e incluso de los servicios informáticos que se brindan desde el centro de datos. Existen varios tipos de monitoreo. Una posible clasificación es Informativo, Preventivo y Reactivo.

El monitoreo preventivo permite analizar en base a histórico y la situación actual el comportamiento futuro de la infraestructura y sistemas de información. El mantenimiento histórico de los valores monitoreados no solo permite realizar pronósticos de tendencia sino puede aportar información valiosa en análisis forenses de incidentes o eventos no esperados.

El monitoreo reactivo es el encargado de "disparar" alarmas en caso de fallas o umbrales definidos para prevenir eventos no deseados. Este tipo de monitoreo deberá realizarse y ser atendido en una modalidad 7x24 para los eventos críticos. Estas alarmas deberán clasificarse según su severidad desde informativas a críticas, siendo estas últimas las que deben atenderse de forma inmediata.

Las herramientas más comunes para consolidar monitoreo implementan protocolos como snmp, icmp, http, consulta de apertura de puertos tcp y permiten realizar scripts para obtener valores a graficar. Las mismas herramientas permiten definir umbrales y enviar alarmas por mail, en tiempo real en un cuadro de mando.

Disponibilidad y Niveles de servicio

Texto del decreto

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.

Aclaración

Como se aclaraba en el punto anterior, la administración de infraestructura de Datacenter requiere atención en modalidad 7x24. Muchas veces las organizaciones no tienen capacidad operativa para cubrir este servicio por lo que delegan la operación del centro de datos a proveedores. Es importante firmar con los proveedores acuerdos de servicios que exija el cumplimiento de tiempos de respuesta estipulados según las necesidades de negocio así como el aseguramiento de la disponibilidad comprometida de los servicios de Centro de Datos.

También es necesario tener acuerdos que aseguren los tiempos de respuesta para aquellos componentes que por su complejidad no puedan ser redundantes pero que por su criticidad la falla del mismo pueda provocar disrupción de servicios u otros daños. Es el caso de los generadores, chasis de equipamiento de gran porte como ser Routers, Storage, Servidores.

Básicamente todo el equipamiento crítico del datacenter debe contar con soporte de mantenimiento y recambio de partes o en su defecto con un plan acción en caso de falla.