MODELO 18 - CONDICIONES MÍNIMAS DE SERVICIO PARA DATA CENTERS

DE LA ADMINISTRACIÓN PÚBLICA NACIONAL

Tabla de Contenidos

Consideraciones Preliminares

Un Data Center es una sala específica y exclusiva, que contiene de manera adecuada una cantidad determinada de equipamiento electrónico e informático y que permite proteger no sólo los equipos implicados, sino también la información contenida en sus servidores. Asimismo, permite tener rápido acceso a la información de cada organismo a fin de garantizar a los ciudadanos la continuidad de los servicios que el organismo presta.

En muchas ocasiones se denomina erróneamente Data Center a un espacio que no resulta ser específico ni exclusivo para llevar a cabo los objetivos descriptos precedentemente, y que tampoco proporciona al equipamiento informático o de comunicaciones las condiciones mínimas de seguridad física, seguridad lógica ni las condiciones de provisión de energía y aire acondicionado que éste requiere, lo cual impide una adecuada protección de la información contenida en las bases de datos y una adecuada provisión de servicio, lo cual resulta ser crítico para el organismo.

Es común denominar Data Center a una oficina o lugar cuyo ingreso es irrestricto, donde gracias al esfuerzo y la voluntad de un grupo de funcionarios y empleados se acumulan computadoras de escritorio que funcionan como servidores, las que no siempre son de última generación, donde las altas temperaturas reinan gran parte del año, en las que se guarda información crítica y sensible tanto para el organismo como para los ciudadanos, sin que se tengan las mínimas condiciones de seguridad física y lógica.

Ante esta situación, resulta relevante que cada organismo pueda determinar si el espacio destinado al equipamiento informático o de comunicaciones para el resguardo de su información crítica, cumple con la totalidad de las medidas de seguridad y de provisión de energía y aire acondicionado indispensables para la efectiva protección de dicha información.

En relación a ello, se pone de resalto que el resguardo de los datos o información sensible de los organismos garantiza la continuidad de los servicios que estos prestan a los ciudadanos. Por ello, es recomendable que a partir del conocimiento de las deficiencias de lugar físico y de los procedimientos de gestión de los Datacenters de cada organismo, se tomen las medidas necesarias para transformar dichos espacios en "verdaderos" Data Center.

Con la finalidad de colaborar con los organismos en la adaptación de estos espacios a las características precedentemente detalladas, la Oficina Nacional de Tecnologías de Información (ONTI), ha implementado lo que se denomina "**Emisión de Calificación**".

La "**Emisión de Calificación**" consiste en un procedimiento a partir del cual, la Oficina Nacional de Tecnologías de Información coopera con los organismos que así lo requieran a conocer el "**nivel**" en que se encuentra su Data Center. A ese fin, la ONTI realizará relevamientos in-situ y cuestionarios al personal técnico especializado.

A partir del análisis de la información obtenida, se orientará a los organismos en la implementación de aquellas acciones necesarias para madurar o crecer, en función del nivel en que se encuentren. Para ello, se han determinado cuatro grandes grupos o niveles, y la definición de las diferentes acciones que deberán tomarse en cada caso.

Descripción General del Proceso

El organismo deberá solicitar a la Oficina Nacional de Tecnologías de la Información, la emisión de "**Calificación**" de su Data Center. La solicitud se realizará a través de una nota formal.

Resulta importante aclarar que para solicitar este servicio, el organismo deberá encontrase, como mínimo, en el nivel que más adelante se denomina como "**VI) Nivel BASICO**".

La calificación será el resultado del procedimiento llevado a cabo en el organismo por el personal técnico especializado que a tal efecto designe la ONTI, y del posterior análisis y procesamiento de la información obtenida en base a parámetros preestablecidos.

En algunos casos, y a criterio de la ONTI, previo a la emisión de la "**Calificación**" que permita determinar el servicio que brinda el Data Center del organismo, la ONTI podrá solicitar aclaraciones o "evidencias" respecto a la información relevada.

La emisión de la "**Calificación**" permitirá al organismo conocer su grado de madurez, para que a partir su conocimiento, pueda desarrollar las "Tareas necesarias para mejorar la calificación", detalladas en el punto denominado ***"VII) Plan de Crecimiento para el ´DATA CENTER´ del Organismo".***

Calificación

Mínimamente, el organismo deberá indicar su voluntad de obtener la "**Calificación**" de su Data Center, debiendo consignar en la solicitud del pedido de emisión de calificación, lo siguiente:

- Organismo solicitante.
- Ubicación física del Data Center a calificar (Domicilio), donde deberá efectuarse la visita del personal calificado designado por la ONTI.
- Responsable del organismo a contactar para la realización del relevamiento (Nombre y Apellido, cargo, teléfono y dirección de correo electrónico).
- Horarios posibles para realizar el relevamiento.
- Funcionario que solicita y autoriza en nombre del organismo a que se lleve a cabo la tarea de relevamiento.

Una vez emitida la "**Calificación**", la misma le será notificada al organismo.

El certificado de "**Calificación**" tendrá una validez de 1 (un) año a partir de la fecha de emisión del mismo, por parte de la ONTI.

Para solicitar la emisión de una nueva "**Calificación**", el organismo tendrá que haber cumplido con al menos el 50% de las tareas indicadas en el "**Plan de Crecimiento**" del nivel superior, de acuerdo a la última "**Calificación**" recibida.

Cuestionario

Se denomina "CUESTIONARIO" a las tareas que deberá realizar el personal técnico designado por la ONTI, las cuales consistirán en una o varias visitas al Data Center del organismo requirente. En dichas visitas la persona "Responsable" deberá responder a una serie de preguntas predeterminadas a los efectos de este estudio. Por lo tanto se requiere que la persona designada como "Responsable" por el organismo cuente con amplio conocimiento del Data Center y tenga facilidad de acceder a la información que le será requerida.

Modelo de Madurez ("NIVEL")

"Nivel BASICO"

Serán considerado como nivel básico, aquel Data Center que posea como mínimo los siguientes elementos y servicios:

- Una "Sala Específica" donde esté funcionando el Data Center del organismo.
- Provisión de energía.
- Aire Acondicionado.
- Estanterías o Racks.
- Equipamiento Básico (Servidores o Computadoras Personales que brinden el servicio).

Plan de Crecimiento para el ´DATA CENTER´ del Organismo.

A NIVEL 1 y 2

PROTECCIÓN CONTRA INCENDIO

A nivel 1	A nivel 2
• Crear un ambiente protegido del fuego para el CPD. • Implementar un sistema de detección de fuego automático. • Tener instalado detectores de humo dentro de los límites del CPD. • Identificar lugares estratégicos e instalar extintores portátiles. • Destinar un lugar seguro fuera del CPD para el almacenamiento de información de resguardo.	• Proteger contra incendio las áreas externas al CPD. • Definir revisiones periódicas para retirar materiales inflamables. • Crear un área externa al CPD para almacenamiento de papel y suministros. • Crear un panel de alarmas. • Adecuar energía de emergencia y aire acondicionado. • Definir un plan de ejercicios de control de incendios y evacuación.

PROTECCIÓN CONTRA DAÑOS POR AGUA

A nivel 1	A nivel 2
• Los equipos en el CPD deben estar elevados del nivel del piso. • Instalar los equipos de manera que queden protegidos de inundaciones y goteras. • Instalar una protección adecuada contra el efecto de los rayos.	• Construir un sistema de drenaje apropiado para el CPD. • Eliminar caños de agua o desagües en el área de CPD.

ELECTRICIDAD Y TELECOMUNICACIONES

A nivel 1	A nivel 2
• Debe haber alimentación de emergencia para alimentar al CPD. • Debe haber alimentación de emergencia para alimentar al Control de humedad y el Aire Acondicionado.	• Instalar un sistema de iluminación de emergencia. • Independizar las redes de datos y de voz.

• Debe haber UPS instaladas para la protección del equipamiento del CPD.	

AIRE ACONDICIONADO

A nivel 1	A nivel 2
• Instalar adecuada provisión de aire acondicionado para el CPD.	• Instalar la provisión de energía independiente para el CPD. • Incorporar elementos de control de humedad y temperatura.

CONTROL DE ACCESO

A nivel 1	A nivel 2
• Realizar control de acceso al CPD.	• Eliminar/proteger ventanas y aberturas existentes en el CPD. • Crear un área de separación del CPD respecto de otras áreas de la organización que tienen uso intensivo.

MANTENIMIENTO GENERAL

A nivel 1	A nivel 2
• Mantener el CPD limpio y ordenado. • Implementar control formal de inventario e identificación de los racks que contienen equipamiento.	• Crear e instaurar las normas para impedir el ingreso de comidas y bebidas en el CPD. • Instalar un sistema de iluminación adecuado y definir un proceso de revisión periódica.

CABLEADO Y REDUNDANCIA

A nivel 1	A nivel 2
• Utilizar un esquema estructurado en el cableado del CPD. • Asegurar la existencia de un plano del cableado de la red.	• Incorporar redundancia al backbone del CPD • Incorporar redundancia a la conectividad de los servidores

ORGANIZACIÓN Y PERSONAL

A nivel 1	A nivel 2
• Asegurar la asignación formal del personal asignado a la seguridad del CPD. • Implementar procedimientos formales para la gestión de los recursos humanos.	• Establecer convenios de confidencialidad y establecer un período de tiempo máximo para su adecuación. • Crear un registro de impacto de pérdidas sobre los servicios.

EQUIPAMIENTO

A nivel 1	A nivel 2
• Asegurar la existencia de un inventario formal del equipamiento. • Asegurar la existencia de un inventario formal de los servicios soportados por cada equipo. • Asegurar la identificación en forma clara de todo el equipamiento.	• Crear los mecanismos para asegurar la provisión de repuestos críticos. • Asegurar la vigencia de contratos de mantenimiento técnico.

RESGUARDO Y RECUPERACIÓN

A nivel 1	A nivel 2
• Asegurar la existencia de un inventario detallado y actualizado de los archivos críticos. • Asegurar la existencia de un procedimiento formal de respaldo periódico calendarizado.	• Crear un procedimiento de respaldo de datos y aplicaciones. • Crear un área externa para el archivo de datos y programas. • Almacenar copias de los archivos de datos en otra ubicación diferente al CPD.

MEDIOS MAGNÉTICOS

A nivel 1	A nivel 2
• Asegurar la existencia de un inventario de medios magnéticos.	• Crear un procedimiento para controlar los medios de almacenamiento. • Formalizar procedimientos para controlar el almacenamiento en discos.

OPERACIÓN DEL CPD

A nivel 1	A nivel 2
• Implementar procedimientos formales y detallados para guiar la operación del CPD. • Asegurar que las funciones de la operación de los servidores estén segregadas.	• Crear un procedimiento de control de acceso a la operación. • Crear un procedimiento de control de acceso a los servidores. • Crear una biblioteca protegida para el resguardo de programas fuentes y archivos de configuración y procedimientos de acceso. • Crear un procedimiento de control de acceso a los sistemas de auditoría.

• Implementar procedimientos formales para la asignación de cuentas y claves de acceso.	• Establecer medidas suficientes para asegurar la protección de las bibliotecas. • Proteger adecuadamente el acceso a los sistemas de auditoría.

REDES Y CONECTIVIDAD

A nivel 1	A nivel 2
• Crear un diagrama formal de la topología de la red de datos.	• Formalizar un inventario de los enlaces de datos involucrados en la red.

ADMINISTRACIÓN DE EQUIPOS

A nivel 1	A nivel 2
• Formalizar procedimientos para el alta y asignación de equipos.	• Formalizar procedimientos para la discontinuidad y destrucción de equipos.

A NIVEL 3 y 4

PROTECCIÓN CONTRA INCENDIO

A nivel 3	A nivel 4
• Modificar piso y techo utilizando material no combustible. • Utilizar materiales de construcción ignífugos en las paredes en el CPD. • Utilizar materiales de construcción ignífugos en las puertas en el CPD. • Utilizar materiales de construcción ignífugos en las ventanas en el CPD. • Utilizar materiales de construcción ignífugos en los pisos en el CPD. • Utilizar mobiliario ignífugo. • Utilizar materiales de construcción ignífugos. • Almacenar los materiales de mantenimiento de los equipos en contenedores ignífugos. • Establecer un procedimiento con instrucciones claras y precisas a ejecutar en caso de incendio.	• Crear un proceso para la revisión periódica de los extintores • Incorporar un interruptor manual para la alarma de incendio • Conexión de alarma en puesto de Guardia y bomberos • Establecer un procedimiento de evacuación de las instalaciones • Actualizar los medios de apagado de incendios • Crear un procedimiento de prueba y revisión periódica de los detectores de humo.

• Instalar interruptores de alarma contra incendios • Determinar la posibilidad de construir una salida de emergencia. • Crear las facilidades de acceso para los casos de emergencia	

PROTECCIÓN CONTRA DAÑOS POR AGUA

A nivel 3	A nivel 4
• Crear procedimientos de revisión periódica de azoteas y torres de ventilación para detectar fugas y filtraciones • Proteger los conectores y cajas eléctricas del piso	• Definir la estructura de protección adecuada. • Definir la estructura de protección adecuada • Definir la estructura de protección adecuada.

ELECTRICIDAD Y TELECOMUNICACIONES

A nivel 3	A nivel 4
• Proteger las líneas de alimentación del CPD contra sobrecargas • Actualizar UPS. • Definir un mecanismo de protección adecuado del sistema de telecomunicaciones • Establecer un procedimiento de apagado de equipos en caso de emergencia. Se deben identificar particularidades en caso de existir.	• Definir un procedimiento de revisión de los generadores eléctricos • Definir un procedimiento de revisión de las UPS • Instaurar los procedimientos de capacitación para el personal

AIRE ACONDICIONADO

A nivel 3	A nivel 4
• Evaluar las posibilidades de instalar aire acondicionado de respaldo. • Instalar entradas de aire fresco por encima del nivel del suelo • Modificar la entrada de aire.	• Instalar interruptores de aire acondicionado y de emergencia conectados entre si. • Instalar los interruptores en lugar accesible.

CONTROL DE ACCESO

A nivel 3	A nivel 4
• Crear un procedimiento para prevenir el acceso no autorizado al CPD, así como prevenir actos de vandalismo o sabotaje. • Formalizar procedimientos para prevenir los sabotajes y el vandalismo • Establecer un mecanismo específico para manejo de amenazas de bomba, intrusos y su notificación.	• Establecer un procedimiento de revisión periódica de los dispositivos de seguridad. • Identificar las áreas sensibles a controlar.

MANTENIMIENTO GENERAL

A nivel 3	A nivel 4
• Establecer la prohibición de fumar en el área del CPD, definir las sanciones y notificar al personal. • Rediseñar el plano del CPD manteniendo las distancias mínimas requeridas.	• Establecer un cronograma de limpieza y rotación de medios. • Revisar el plano del CPD manteniendo las distancias mínimas requeridas.

CABLEADO Y REDUNDANCIA

A nivel 3	A nivel 4
• Se debe adoptar un modelo de cableado estructurado. • Se debe crear un inventario del cables y patcheras.	• Identificar servicios críticos y los niveles de redundancia requeridos.

ORGANIZACIÓN Y PERSONAL

A nivel 3	A nivel 4
• Crear un procedimiento para la gestión de los riesgos del CPD. • Se deben establecer los planes de recuperación. • Establecer un plan de Continuidad de Negocios por parte de TI. • Establecer una política de seguridad en la organización.	• Establecer un procedimiento de revisión periódica de los planes de recuperación. • Asignar las responsabilidades al personal para actuar en caso de desastres. • Formalizar una matriz de asignación de responsabilidades para los activos críticos • Formalizar el Plan de Continuidad de Negocios. • Formalizar procedimientos de revisiones periódicas del Plan de Continuidad de Negocios.

	• Documentar y Formalizar la Política de seguridad en la organización. • Establecer una matriz de riesgo de los activos críticos. • Formalizar procedimientos de revisiones y mantenimiento periódicos de la matriz de riesgo.

EQUIPAMIENTO	
A nivel 3	**A nivel 4**
• Crear un flujo de escalado de incidentes críticos. • Crear un proceso de evaluación de la capacidad y disponibilidad de la infraestructura.	• Crear un proceso de evaluación de la capacidad y disponibilidad de la infraestructura. • Establecer un procedimiento de revisión periódica de los equipos críticos.

RESGUARDO Y RECUPERACIÓN	
A nivel 3	**A nivel 4**
• El procedimiento de respaldo debe contener los roles y responsabilidades formalmente establecidos. • Formalizar un procedimiento para el resguardo de eventos de seguridad. • Formalizar un procedimiento de resguardo de logs de auditoría.	• Definir los requerimientos de equipos de back up. • Establecer un proceso de revisión de los equipos críticos.

MEDIOS MAGNÉTICOS	
A nivel 3	**A nivel 4**
• Construir un área protegida para el almacenamiento de medios magnéticos. • Construir un área de almacenamiento de medios magnéticos protegido contra vandalismo y robos.	• Establecer un proceso de control de acceso al área de almacenamiento de medios magnéticos.

OPERACIÓN DEL CPD	
A nivel 3	**A nivel 4**
• Crear procedimientos para el almacenamiento y resguardo de claves. • Definir los pasos formales para la administración de las	• Separar los ámbitos de administración de servidores y usuarios. • Establecer un procedimiento de cambio periódico de

claves.	claves de usuarios.
• Definir reglas precisas para la creación de password. • Crear los procesos que aseguren la confidencialidad de los datos.	• Crear un procedimiento para identificar y gestionar vulnerabilidades. • Crear un procedimiento para aplicar parches y controles de seguridad.

REDES Y CONECTIVIDAD	
A nivel 3	**A nivel 4**
• Formalizar un inventario de los dispositivos involucrados en la red de datos.	• Formalizar procedimientos de seguridad de la red de datos.

ADMINISTRACIÓN DE EQUIPOS	
A nivel 3	**A nivel 4**
• Instalar una Base de Datos con el registro de movimiento (altas, bajas y modificaciones) de equipos	• Asegurar la trazabilidad del movimiento de equipos dentro de la organización.