

PROCEDIMIENTO PARA EL TRABAJO CON LA RED DE DATOS DEL SISTEMA DE LA ONE

OBJETIVO: Perfeccionar el trabajo con la red de datos del Sistema de la ONE, perfeccionar su seguridad y operatividad.

ALCANCE: Deben ser cumplido por todas las Oficinas Nacionales de Estadísticas (ONE) de los niveles central, provincial y municipal que integran la red de la ONE

RESPONSABILIDADES: Es responsabilidad del Director de Informática, delegados, jefes de informática y administradores de red hacer cumplir lo establecido.

DESARROLLO: La red es la columna del soporte fundamental del trabajo estadístico- La Informática- y como tal debe ser configurada y administrada, garantizando lo máximo posible su seguridad y operatividad. Para esto se deben tener en cuenta todas las regulaciones establecidas en la Resolución 127 del 2007 del MIC y las Políticas y medidas asociadas a ella para normar el trabajo de la informática en los diferentes niveles de la ONE.

Para garantizar este propósito la red debe contar con una serie de controles y registros:

1. Modelo Acta de Responsabilidad del Administrador de Red. (Anexo 1)
2. Modelo Diagrama estructural de conectividad de los servidores de red. (Anexo 2)
3. Modelo definición de la estructura de la red y los servicios implementados. (Anexo 3)
4. Procedimiento de salvaguarda de la configuración de Aplicaciones activas en los servidores y su correspondiente registro. (Anexo 4)
5. Documento del control y actualización de las políticas definidas en la red. (Anexo 5)
6. Procedimiento de salvaguarda de las trazas de mensajería y navegación y su correspondiente registro. (Anexo 6)
7. Registro de Sistemas Informáticos instalados en la red y su correspondiente procedimiento de salvaguarda. (Anexo 7)
8. Documento de la programación de los router y los switch. (Anexo 8)
9. Registro de control de diagnóstico a la red de datos.
10. Registro de Usuarios de la red y servicios que le presta la red.
11. Mapa de la red
12. Bitácora sobre como solucionar los errores más frecuentes de la red.
13. Modelo de acta de entrega de contraseñas de servidores y routers entregadas en sobre sellado al jefe de informática, que se modifican anualmente o después de la baja de un administrador de red.

MODELO ACTA DE RESPONSABILIDAD DEL ADMINISTRADOR DE RED

Oficina Nacional de Estadísticas de: _____

Nombre y apellidos del Administrador: _____

ACTA DE RESPONSABILIDAD

Declaro que conozco y asumo la responsabilidad en cuanto a la Seguridad Informática en el uso de las tecnologías de la información para el desempeño de mis funciones laborales como se expresa en la Resolución 127/2007 del Ministerio de la Informática y las Comunicaciones.

Como Administrador de Red en esta entidad, asumo las siguientes obligaciones:

1. Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red.
2. Realizar el análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red.
3. Garantizar que los servicios implementados sean utilizados para los fines que fueron creados.
4. Comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.
5. Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de incidentes y acciones nocivas que se identifiquen, preservando toda la información requerida para su esclarecimiento.
6. Participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas.
7. Informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento.
8. Otorgar a los usuarios sólo los derechos que le han sido otorgados.
9. Participar en la confección y actualización del Plan de Seguridad Informática.

PROHIBICIONES

1. La administración remota de las redes mediante conexiones conmutadas a través de las redes públicas de transmisión de datos.
2. La adición de algún equipo o la introducción de cualquier tipo de software en una red, ya sea a través de soportes removibles o mediante acceso a redes externas, sin la autorización de la dirección de la entidad.

Por lo que estoy dispuesto a cumplir y aceptar la Responsabilidad Administrativa y Material que se deriva de su incumplimiento.

Fecha de Realización: _____ Firma del Administrador de Red: _____

Para el trabajo con el Modelo Acta de Responsabilidad del Administrador de Red. (Anexo 1), se debe tener en cuenta que en los campos siguientes:

- Oficina Nacional de Estadísticas de: Nivel Central o provincia a la que pertenece
- Nombre y Apellidos: Nombre y Apellidos del Administrador de Red.
- Fecha de Realización: Fecha en que se llenó el modelo.
- Firma del Administrador de Red: Firma del Administrador de la Red como constancia de la aprobación de sus responsabilidades.
- Aprobado por, cargo, firma y cuño: Nombre y apellidos del director, su cargo, firma y cuño del mismo.

MODELO DIAGRAMA ESTRUCTURAL DE CONECTIVIDAD DE LOS SERVIDORES DE LA RED

Oficina Nacional de Estadísticas de _____

No. Consecutivo: _____ **de** _____

MODELO DEFINICIÓN DE LA ESTRUCTURA DE LA RED Y LOS SERVICIOS IMPLEMENTADOS

Oficina Nacional de Estadísticas de _____

Nombre y Apellidos Administrador de la Red: _____

ESTRUCTURA DE LA RED

No. de Licencia de Red de Datos: _____

Alcance de Red:

Red Local: _____ Red Corporativa: _____ Wan: _____ Lan: _____

Nombre de Dominio: _____ No. de Inscripción: _____

Subdominio: Sí: _____ Nombre de Subdominio: _____

 No: _____

SERVICIOS IMPLEMENTADOS

Cantidad de Servidores: _____

Para cada servidor especificar

Servicio que presta: _____

Descripción: _____

IP Fija: _____

Fecha de Realización: _____

Firma del Administrador de Red: _____

Para llenar el Modelo Definición de la estructura de la red y los servicios implementados. (Anexo 3), se debe conocer que:

- No. Consecutivo: especificar para ese modelo la página de las que tiene
- Oficina Nacional de Estadísticas de: Nivel Central o provincia a la que pertenece
- No. de Licencia de Red de Datos: Número de la licencia de red de datos, conociendo según la Resolución 195/2007 del MIC sobre las Redes, que toda red que brinde servicios de Internet nacional o internacional debe estar inscrita en el Registro de Proveedores de Servicios en el Entorno de Internet existente y anexar la fotocopia.
- Alcance de Red: Marcar con una (X) el tipo de red que sea, teniendo en cuenta según la Resolución 195/2007 del MIC, que una Red Local suele limitarse al interior de un edificio o complejo hospitalario, docente, etc; una Red Sectorial proporciona conectividad a PCs para un determinado grupo, así como a Organizaciones Políticas y de Masas u otras y fuera de estos no suministra conectividad a terceros; una Red Corporativa proporcionan conectividad a PCs de Empresas, Grupos Empresariales, Institutos, Centros o Asociaciones, entre otras y fuera de estos no suministran a terceros.
- Nombre de Dominio: Nombre del dominio de red.
- No. de Inscripción: Número de la inscripción de la red.
- Subdominio (Si-No): Marcar con una (X) en caso que haya o no subdominio. De existir subdominio especificar el Nombre de Subdominio.
- Cantidad de Servidores: La cantidad de servidores existentes

Para cada servidor especificar:

- Servicio o servicios que presta es decir: de correo de DHCP, de Domino, de Ficheros, etc
- Descripción del servicio, o característica para esa red, en caso del servidor de ficheros, FTP o de Sitios especificar la estructura, para el DHCP, cuantas IP son fijas y forma de asignación.
- IP Fija: indicar la dirección IP que tiene eses servidor y su alias.
- Fecha de realización: Fecha en que se llenó el modelo.
- Firma del Administrador de Red: Firma del Administrador de Red como aprobación del Modelo.

PROCEDIMIENTO DE SALVAS DE LA CONFIGURACIÓN DE APLICACIONES ACTIVAS EN LOS SERVIDORES

Se utilizará el formato establecido en el procedimiento del control de salvas

DOCUMENTO DEL CONTROL DE LAS POLÍTICAS DEFINIDAS EN LA RED

- Las características de la información que serán priorizadas son en orden de importancia: *INTEGRIDAD* (no modificación sin autorización), *DISPONIBILIDAD* (no retener información no autorizada) y *CONFIDENCIALIDAD* (no divulgar información no autorizada).
- Se instruirá a todos los trabajadores de la importancia del cumplimiento de las medidas relacionadas en este plan de seguridad informática.
- La información limitada, que procesa la oficina del Ministro, recibirá el tratamiento que establece el Decreto Ley 199/99; así como también la documentación relacionada con la defensa.
- Todas las microcomputadoras tendrán definido clave de encendido siempre que el sistema lo permita y protector de pantalla, el que no excederá de los diez minutos en activarse después de no estar utilizando la microcomputadora.
- Las contraseñas de los usuarios para acceder a la red tiene una duración máxima de 6 meses y tendrá una longitud mínima de 8 caracteres, como mínimo pertenecientes al grupo de las Mayúsculas, Minúsculas, Números y Caracteres Especiales. No se permiten contraseñas en blanco.
- El personal autorizado utilizará los servicios de la red con fines estrictamente de trabajo.
- La autorización a los servicios de Internet será otorgada por el Jefe de la ONE o cuadro del primer nivel en quien delegue.
- El personal autorizado a los servicios de Internet y correo electrónico deberá firmar un compromiso sobre su conocimiento y las reglamentaciones existentes para estos servicios.
- Monitorear sistemáticamente la navegación por Internet, analizando los horarios críticos. Se establecerá el traceado del tráfico por Internet.
- Se accederá a la red Internet por medio de un enlace arrendado con ENET, solo los usuarios de la red local autorizados a la navegación tendrán acceso a ella.
- Sólo el personal que posee buzones de correo electrónico internacional podrá hacer uso del mismo.
- Cuando un usuario de correo electrónico cause baja del centro se inhabilita su cuenta de correo, el nombre de la misma no volverá a utilizarse.
- La utilización de soportes magnéticos estará precedida de su chequeo contra virus o desperfectos, esto es responsabilidad del especialista que lo utilice, en caso de duda acudirá al activista de seguridad informática de su área.
- La salva y conservación de la información se realizará según lo establece la explotación de cada una de las aplicaciones autorizadas.

- El administrador de la red realizará las copias de respaldo correspondientes tanto del sistema operativo de la red como de la información de los servidores que garanticen su disponibilidad en caso de cualquier contingencia.
- La salvaguarda y cuidado de la información que se procese en las microcomputadoras es responsabilidad de la persona a la que se le haya asignado la misma.
- Se prohíbe la entrada de personal no autorizado al local en que se encuentran los servidores.
- La adquisición, mantenimiento, reparación, y traslado de las tecnologías informáticas será realizado por los especialistas de la Dirección o Departamento de Informática, siempre que cumpla con el debido movimiento de los medios básicos.
- El mantenimiento a las tecnologías informáticas se realizará como lo establece la Dirección de Informática, y se reflejará en el en el modelo de Control del Equipamiento de cada área.
- Se realizarán de manera sistemática supervisiones sobre el uso y explotación de las TIC.
- Cualquier violación que se detecte en materia de seguridad informática debe ser comunicada al activista de Seguridad Informática quien a su vez lo debe comunicar a la Dirección o Departamento de Informática.

REGISTRO DE SALVAS DE LAS TRAZAS DE MENSAJERÍA Y NAVEGACIÓN

Se utilizará el formato establecido en el procedimiento del control de salvas

**REGISTRO DE SISTEMAS INFORMÁTICOS INSTALADOS EN LA RED Y SU
CORRESPONDIENTE PROCEDIMIENTO DE SALVA**

**Se tendrá un registro de todos los sistemas informáticos de la Oficina y anexado el
procedimiento de salva que se emplea con los mismos**

DOCUMENTO DE LA PROGRAMACIÓN DE LOS ROUTER Y LOS SWITCH

En general en la configuración de los router se debe tener en cuenta:

- Cambiar la contraseña por defecto y que la nueva cumpla con los requerimientos y políticas de contraseñas vigentes. Configurar el “enable secret password” para garantizar que se proteja con algoritmos basados en MD5.
- Deshabilitar la administración desde la interface WAN.
- Configurar la administración del mismo por las interfaces LAN y desde una IP específica, gestionada y controlada por el administrador de la red.
- Aplicar Listas de Acceso desde la interface WAN hacia la LAN según los servicios autorizados a la entidad
- Aplicar Listas de Acceso desde la interface LAN hacia la WAN según los permisos plasmados en el plan de seguridad.
- Almacenar los Log de los routers y realizar un análisis periódico con las herramientas que colecten dicha información para posteriormente generar reportes de actividad.
- Tener actualizado el IOS del router.
- Verificar que las sub-interfaces correspondan con las contratadas.
- Configurar el router para que incluya en los logs la información relativa al tiempo para que le permita al administrador registrar ataques a su red de forma más segura.
- Mantener una copia externa de la configuración del router, mantenerla bien documentada y comentada.