# POLÍTICAS DE SEGURIDAD INFORMÁTICA

*Oficina de Seguridad para las Redes Informáticas*

## Índice

## Sobre el documento:

Este documento es emitido por la Oficina de Seguridad para las Redes Informáticas (OSRI) y contiene los principales aspectos y medidas a cumplir por las entidades del país, así como la explicación paso a paso para llevar a cabo la aplicación de cada una de ellas; de igual forma se hace alusión a algunas medidas de seguridad informática que propone la Oficina de forma opcional para su aplicación.

Comenzaremos por establecer que el administrador de la red de la entidad es el informático en caso que no exista el especialista que realice esa función, por lo que es el que administra y monitorea todo el funcionamiento de la entidad desde el punto de vista de redes, sistemas y subsistemas con los que se trabaja, aunque esto no le da autorización de violar ninguna de las medidas que están establecidas.

## Unidades Organizativas

Deben crearse **Unidades Organizativas**, las cuales contienen a los usuarios y estaciones de trabajo. Estas unidades se deben crear de acuerdo a las características de cada máquina o usuario respectivamente.

En el servidor que tiene el controlador de Dominio (Directorio Activo) realizar la siguiente configuración.

- **Cómo se hace una unidad organizativa:**

Se abre el Directorio Activo, clic derecho arriba del *Nombre del dominio->Nuevo->Unidad Organizacional*, se le pone el nombre y se da OK. Así se crea cada una de las unidades organizativas que se requieran, pueden existir varias Unidades Organizativas anidadas de acuerdo a los requerimientos.

- **Cómo se configura las políticas de seguridad para una unidad organizativa:**

Clic derecho encima de la unidad organizativa que se creó, *Propiedades->Políticas de Grupo->Nuevo* y le ponen un nombre para identificarla, luego clic encima y le dan (Editar) para configurarla, también se utiliza el botón (Agregar) para el caso de una política que se quiera utilizar y ya haya sido creada anteriormente.

### 1. Aplicación de políticas de seguridad a las Estaciones de Trabajo

#### 1.1. Registros de Auditorías

Se habilitaran los registros de auditoría, quiere decir que cada acción que realice en la máquina quedará registrada.

Habilitar la auditoría para Sistema, Seguridad y Aplicación, asignándole a cada Registro el tamaño máximo (307 200) y activar la opción de borrar si es necesario. Cuando el Registro se llene el Sistema Operativo reemplaza las entradas más antiguas del registro por las nuevas entradas que se van a almacenar, de esta forma se cumple con lo que plantea la Resolución 127/2007 del Ministerio de Comunicaciones, donde plantea que deben recolectarse y guardarse las auditorias del sistema por un periodo no menos de 1 año.

Trazar la siguiente política por (Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Directivas Locales\ **Directiva de Auditoría**):

- Activar todo (Correcto, Error).

Es opcional no activar “Auditar el acceso a objetos”, por la gran cantidad de información que genera.

Trazar la siguiente política por (Conf. Equipo\ Conf. Windows\ Conf. Seguridad\Registros de Sucesos):

**Para Aplicación:**
Doble clic en Tamaño máximo del registro de aplicación:

- Se **habilita**: Definir esta configuración de directiva.
- Se escribe: 307 200 como tamaño máximo del registro.

Doble clic en Método de retención del registro de la aplicación.

- Se **habilita**: Definir esta configuración de directiva.
- Se marca: Sobrescribir sucesos cuando sea necesario.

**Para Seguridad**
Doble clic en Tamaño máximo del registro de seguridad:

- Se **habilita**: Definir esta configuración de directiva.
- Se escribe: 307 200 como tamaño máximo del registro.

Doble clic en Método de retención del registro de seguridad.

- Se **habilita**: Definir esta configuración de directiva.
- Se marca: Sobrescribir sucesos cuando sea necesario.

**Para Sistema**
Doble clic en Tamaño máximo del registro del sistema:

- Se **habilita**: Definir esta configuración de directiva.
- Se escribe: 307 200 como tamaño máximo del registro.

Doble clic en Método de retención del registro del sistema:

- Se **habilita**: Definir esta configuración de directiva.
- Se marca: Sobrescribir sucesos cuando sea necesario.

### 1.2. Directivas de contraseñas

Las contraseñas de los usuarios deberán cumplir los requisitos siguientes:

- Longitud mínima (6 caracteres).
- Forzar cambio (60 días)

- El usuario puede cambiar la contraseña desde su propia máquina.
- En el cambio se solicitará la anterior.
- No se permitirá utilizar las últimas 5 contraseñas usadas.
- Se bloqueará la cuenta a los tres intentos fallidos.
- Duración del bloqueo (30 min).

Trazar las siguientes políticas por (Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Directivas de Cuentas\ Directivas de Contraseñas):

- Longitud mínima de la contraseña (**7 caracteres**).
- Vigencia máxima de la contraseña (**60 días**).
- Vigencia mínima de la contraseña (**3 días**)
- Forzar el historial de contraseñas (**10 contraseñas recordadas**).
- Las contraseñas deben cumplir los requerimientos de complejidad (**Habilitada**).

Trazar las siguientes políticas por (Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Directivas de Cuentas\ Directiva de bloqueo de cuentas):

- Duración del bloqueo (**30 minutos**).
- Restablecer la cuenta de bloqueos después de (**30 minutos**)
- Umbral de bloqueo (**5 intentos de inicio de sesión**).

### 1.3. Asignación de derechos de usuarios

Se requiere habilitar las siguientes políticas para evitar posible apropiación del usuario de carpetas que no le pertenecen, así como evitar el cambio de hora en la computadora, entre otras cosas.

#### 1.3.1. Cambio de la hora del sistema

No permitir a ningún usuario de la red ni a ningún administrador local de las estaciones de trabajo cambiar la hora del sistema, esta operación solo debe ser realizada por el Administrador de la red, para asegurarnos de esto trazaremos la siguiente política.

(Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Opciones de Seguridad\Asignación de Derechos de Usuarios)

Doble clic sobre Cambiar la hora del sistema, quitamos todos los usuarios que aparecen allí, seguidamente clic en Agregar Usuario o Grupo y ponemos allí el usuario del administrador de red que debe ser el usuario del dominio.

#### 1.3.2. Tomar posesión de archivos y objetos

No permitir a ningún usuario de la red ni a ningún administrador local de las estaciones de trabajo tomar posesión de archivos que no le pertenecen, esto se ve muy evidenciado cuando trabajan más de dos usuarios en una misma computadora y por algún motivo administrativo tienen privilegios administrativos, para evitar esto trazaremos la siguiente política.

(Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Opciones de Seguridad\Asignación de Derechos de Usuarios)

Doble clic sobre Tomar posesión de archivos y otros objetos, quitamos todos los usuarios que aparecen allí, seguidamente clic en Agregar Usuario o Grupo y ponemos allí el usuario del administrador de red que debe ser el usuario del dominio.

### 1.3.3. Administrar los registros de auditorias

Los registros de auditorías son un elemento fundamental para un trabajo pericial en caso de suceder cualquier incidente, se debe tener en cuenta que ningún usuario puede modificar estos registros, para evitar esto se debe tener en cuenta que solo el administrador de la red con su usuario del dominio tiene derecho a administrar estas auditorías, para ello aplicaremos la siguiente política.

(Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Opciones de Seguridad\Asignación de Derechos de Usuarios)

Doble clic sobre Administrar los Registros de auditorías, quitamos todos los usuarios que aparecen allí, seguidamente clic en Agregar Usuario o Grupo y ponemos allí el usuario del administrador de red que debe ser el usuario del dominio.

## 1.4. Políticas Opcionales

Un sistema informático no siempre está seguro un 100% pues cada día se hacen más presente las brechas de seguridad, en este apartado se le presenta a los administradores de red o al informático de la entidad algunas políticas de seguridad que se pueden aplicar en su sistema pero que son solo para mejorar más aun la seguridad.

### 1.4.1. Inicio de Sesión

Al iniciar la sesión se les mostrará un mensaje que le recuerda que debe cumplir con lo comprometido en la declaración jurada que firma cada usuario de la red.

Trazar las siguientes políticas por (Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Directivas Locales\ **Opciones de Seguridad**):

- Inicio de sesión interactivo: Titulo del mensaje para los usuarios que intentan iniciar una sesión.

Esta configuración de seguridad permite que el titulo especificado aparezca en la barra de título de la ventana que contiene el inicio de sesión interactivo. (Cuando se habilite esta opción debe escribirse el texto)

Ejemplo (Sin las comillas): “**ESTIMADO USUARIO:”**

Trazar las siguientes políticas por (Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Directivas Locales\ **Opciones de Seguridad**):

- Inicio de sesión interactivo: Texto del mensaje para los usuarios que intentan iniciar una sesión.

Esta configuración de seguridad especifica un mensaje de texto que se muestra a los usuarios cuando inician sesión. (Cuando se habilite esta opción debe escribirse texto)
Ejemplo (Sin las comillas): **"Se le advierte que todas sus acciones quedarán registradas para poder auditarse y si tiene cuenta de correo sus mensajes serán monitoreados, por favor cumpla lo convenido en su DECLARACION JURADA."**

### 1.4.2. Otras acciones de seguridad que se deben tener en cuenta

Trazar las siguientes políticas por (Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ Directivas Locales\ Opciones de Seguridad):

- Inicio de sesión Interactivo: no requiere Ctrl+Alt+Supr: **Deshabilitada**.

Esta configuración de seguridad determina si es necesario presionar Ctrl+Alt+Supr para que el usuario pueda iniciar sesión, si esta directiva está habilitada no es necesario que el usuario presione Ctrl+Alt+Supr para iniciar sesión.

- Cuentas: Estado de la cuenta Invitado: **Deshabilitada**.
- Cambiar el nombre del usuario Administrador. (**Especificar otro nombre de usuario**)
- Inicio de sesión Interactivo: pedir al usuario que cambie la contraseña antes que caduque: **7 días.**

### 1.4.3. Reproducción de archivos de videos

Para evitar la reproducción de archivos de videos en las estaciones de trabajo de los usuarios podemos trazar la siguiente política en todas las PC, opcional en la del Administrador de Red e Informáticos, tiene que ser por políticas de cada Unidad Organizativa, en el caso de algún video en específico de capacitación que se envíe, la dirección determinará en que estación de trabajo será transmitido y el administrador de la red es el encargado de habilitar la misma.

**a)** Por el editor de políticas de grupo en la unidad organizativa (Conf. Equipo\ Conf. Windows\ Conf. Seguridad\ **Directiva de Restricción de Software**).

• **Obligatoriedad**: Deben dejar todo como está, solamente marcar dentro de "Aplicar directiva de restricción de software a los siguientes usuarios:"
Marcar: "Todos los usuarios excepto los administradores locales".

• **Niveles de seguridad:** Deben marcar por defecto "No Permitido".

• **Tipos de ficheros designados:**

Se desmarcan del listado de las extensiones no permitidas a ejecutar las siguientes:
- **.lnk**
- **.mdb**
- **.mde**
- **.url**

Se agregan las extensiones siguientes, para evitar que se reproduzcan videos en las estaciones de trabajos.
- **. avi**
- **.mpg**

- **.vob**
- **.flv**
- **.mov**
- **.divx**
- **.mp4**
- **.mkv**

**b)** Deshabilitamos los reproductores conocidos para no permitir que el usuario pueda acceder a ellos, así nos aseguramos que no se pueda ver ningún video, esta política sirve de complemento para la política anterior.

Trazar la siguiente política por (Conf. Usuario\ Plantillas Administrativas\ **Sistema**):

No ejecutar aplicaciones de Windows especificadas: **Habilitado**

Lista de aplicaciones no permitidas: Clic en (**Mostrar**) y en (**Agregar**) y adicionar las siguientes aplicaciones:

- mplayer.exe
- Crystal.exe
- mpc-hc.exe
- Kmplayer.exe
- mplayerc.exe
- winamp.exe
- wmplayer.exe
- splayer.exe
- MPUI.exe
- Bsplayer.exe
- QQplayer.exe
- QuickTimePlayer.exe
- vlc.exe

En el caso de algún otro reproductor de video agregarlo a la lista para que se bloquee su uso, se debe tener en cuenta por parte del administrador de red cual es o serán los reproductores permitidos para el uso del mismo para escuchar música si está permitido en la entidad.

### 1.4.4. Prohibir el acceso al Panel de Control

Esta configuración impide que el proceso control.exe, el archivo de programa de Panel de Control, se inicie. Como resultado, los usuarios no pueden iniciar Panel de control o ejecutar elementos del Panel de Control. Esta configuración también quita el Panel de Control del menú Inicio, así como también lo quita del explorador de Windows.

Trazar la siguiente política: (Conf. De Usuario\ Plantillas Administrativas\ Panel de Control)

Doble clic sobre “Prohibir el acceso al Panel de control”: **Habilitado**