

Desafío - Diseño de Políticas de GPO

Requerimientos








 Almacenar contraseñas con cifrado reversible	Deshabilitada
 Auditoría de longitud mínima de contraseña	No está definido
 Exigir historial de contraseñas	24 contraseñas recordadas
 La contraseña debe cumplir los requisitos de complejidad	Habilitada
 Longitud mínima de la contraseña	14 caracteres
 Vigencia máxima de la contraseña	60 días
 Vigencia mínima de la contraseña	2 días

Ilustración 1 En Configuración de Equipos -> Inforcap -> GPO -> en Editar -> Configuración de Equipo -> Directivas -> Configuración de Windows -> Configuración de Seguridad -> Directivas de Cuenta se encuentra: Contraseña y así esta Configurado





 Duración del bloqueo de cuenta	45 minutos
 Permitir bloqueo de cuenta de administrador	Habilitada
 Restablecer el bloqueo de cuenta después de	45 minutos
 Umbral de bloqueo de cuenta	3 intentos de inicio de sesión no...

Ilustración 2 En Configuración de Equipos -> Inforcap -> GPO -> en Editar -> Configuración de Equipo -> Directivas -> Configuración de Windows -> Configuración de Seguridad -> Directivas de Cuenta se encuentra: Bloqueo de Cuenta

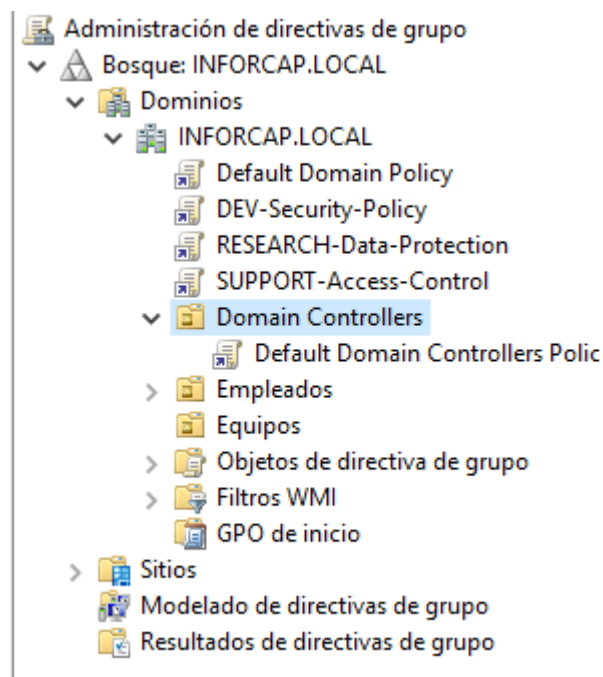


Ilustración 3 Creación de los GPOs

Acción	Usuario	Nombre	Condición
✓ Permitir	Todos	(Regla predeterminada) Todos los archi...	Ruta de a...
✓ Permitir	Todos	(Regla predeterminada) Todos los archi...	Ruta de a...
✓ Permitir	BUILTIN\Administradores	(Regla predeterminada) Todos los archi...	Ruta de a...
✓ Permitir	INFORCAP\Desarrollo Software Medico	Solo IDEs	Editor

Ilustración 4 En Directivas de Control de Aplicaciones -> Applocker -> Reglas Ejecutables -> Crear Regla -> Añadir Grupo -> Añadir la Ruta -> Ruta de Acceso -> Nombre y Crear

DEV-Security-Policy
Ámbito
Detalles
Configuración
Delegación

Detalles

Dominio
Propietario
Creado
Modificado
Revisiones de usuario
Revisiones de equipo
Id. único
Estado de GPO

INFORCAP.LOCAL
INFORCAP\Admins. del dominio
17/06/2025 17:37:44
17/06/2025 18:28:48
0 (AD), 0 (SYSVOL)
4 (AD), 4 (SYSVOL)
{9B01665A-E0F6-4985-A8B0-E2C11614654F}
Habilitado

Vínculos

Ubicación	Aplicado	Estado de vínculo	Ruta
INFORCAP	No	Habilitado	INFORCAP.LOCAL

Esta lista solo incluye vínculos en el dominio del GPO.

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
INFORCAP\Desarrollo Software Medico
NT AUTHORITY\Usuarios autenticados

Filtrado WMI

Nombre de filtro WMI	FILTRO DE RAM
Descripción	Aplica solo en equipos co mas de 8 gb de ram

Delegación

Ilustración 5 Configuración de GPO Desarrollo de Software Medico

DEV-Security-Policy

Ámbito

Detalles

Configuración

Delegación

Delegación

Estos grupos y usuarios tienen los permisos especificados para este GPO

Nombre	Permisos válidos	Heredado
INFORCAP\Administradores de empresas	Editar configuración, eliminar, modificar seguridad	No
INFORCAP\Admins. del dominio	Editar configuración, eliminar, modificar seguridad	No
INFORCAP\Desarrollo Software Medico	Lectura (de Filtrado de seguridad)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\Usuarios autenticados	Lectura (de Filtrado de seguridad)	No

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas de control de aplicaciones

Reglas Appx

No se definieron reglas del tipo 'Reglas Appx'.

Reglas Dll

No se definieron reglas del tipo 'Reglas Dll'.

Reglas ejecutables

DEV-Security-Policy

Ámbito

Detalles

Configuración

Delegación

Reglas ejecutables

Directiva

Configuración

Aplicar reglas de este tipo

Verdadero

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	INFORCAP\Desarrollo Software Medico	Solo IDEs	Editor	No
Permitir	Todos	(Regla predeterminada) Todos los archivos de la carpeta Archivos de programa	Ruta de acceso	No
Permitir	Todos	(Regla predeterminada) Todos los archivos de la carpeta Windows	Ruta de acceso	No
Permitir	BUILTIN\Administradores	(Regla predeterminada) Todos los archivos	Ruta de acceso	No

Reglas de Windows Installer

Directiva

Configuración

Aplicar reglas de este tipo

Verdadero

No se definieron reglas del tipo 'Reglas de Windows Installer'.

Reglas de scripts

No se definieron reglas del tipo 'Reglas de scripts'.

Configuración del usuario (habilitada)

Configuración no definida.

RESEARCH-Data-Protection

Datos recopilados el: 18/06/2025 1:37:19

General

Detalles

Dominio	INFORCAP.LOCAL
Propietario	INFORCAP\Admins. del dominio
Creado	17/06/2025 17:39:56
Modificado	17/06/2025 18:38:30
Revisiones de usuario	0 (AD), 0 (SYSVOL)
Revisiones de equipo	0 (AD), 0 (SYSVOL)
Id. único	{3C2128FB-84BA-4C9D-98EB-8A7640F34D0B}
Estado de GPO	Habilitado

Vínculos

Ubicación	Aplicado	Estado de vínculo	Ruta
INFORCAP	No	Habilitado	INFORCAP.LOCAL

Esta lista solo incluye vínculos en el dominio del GPO.

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
INFORCAP\Investigacion Clinica
NT AUTHORITY\Usuarios autenticados

Filtrado WMI

Ilustración 6 Configuración de GPO Investigación Clínica

RESEARCH-Data-Protection

Ámbito

Detalles

Configuración

Delegación

Nombre

INFORCAP\Investigacion Clinica

NT AUTHORITY\Usuarios autenticados

Filtrado WMI

Nombre de filtro WMI	FILTRO WIN10
Descripción	Filtro para equipos con win 10

Delegación

Estos grupos y usuarios tienen los permisos especificados para este GPO

Nombre	Permisos válidos	Heredado
INFORCAP\Administradores de empresas	Editar configuración, eliminar, modificar seguridad	No
INFORCAP\Admins. del dominio	Editar configuración, eliminar, modificar seguridad	No
INFORCAP\Investigacion Clinica	Lectura (de Filtrado de seguridad)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\Usuarios autenticados	Lectura (de Filtrado de seguridad)	No

Configuración del equipo (habilitada)

Configuración no definida.

Configuración del usuario (habilitada)

Configuración no definida.

SUPPORT-Access-Control

Ámbito

Detalles

Configuración

Delegación

SUPPORT-Access-Control

Datos recopilados el: 18/06/2025 1:38:59

General

Detalles

Dominio	INFORCAP.LOCAL
Propietario	INFORCAP\Admins. del dominio
Creado	17/06/2025 17:40:46
Modificado	17/06/2025 18:19:58
Revisiones de usuario	0 (AD), 0 (SYSVOL)
Revisiones de equipo	0 (AD), 0 (SYSVOL)
Id. único	{A28C38B2-6DE2-4951-9610-85ED2484B9FA}
Estado de GPO	Habilitado

Vínculos

Ubicación	Aplicado	Estado de vínculo	Ruta
INFORCAP	No	Habilitado	INFORCAP.LOCAL

Esta lista solo incluye vínculos en el dominio del GPO.

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
INFORCAP\Soporte Técnico
NT AUTHORITY\Usuarios autenticados

Filtrado WMI

Ilustración 7 Configuración de GPO Soporte Técnico

SUPPORT-Access-Control

Ámbito

Detalles

Configuración

Delegación

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
INFORCAP\Soporte Técnico
NT AUTHORITY\Usuarios autenticados

Filtrado WMI

Nombre de filtro WMI	FILTRO WIN10
Descripción	Filtro para equipos con win 10

Delegación

Estos grupos y usuarios tienen los permisos especificados para este GPO

Nombre	Permisos válidos	Heredado
INFORCAP\Administradores de empresas	Editar configuración, eliminar, modificar seguridad	No
INFORCAP\Admins. del dominio	Editar configuración, eliminar, modificar seguridad	No
INFORCAP\Soporte Técnico	Lectura (de Filtrado de seguridad)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\Usuarios autenticados	Lectura (de Filtrado de seguridad)	No

Configuración del equipo (habilitada)

Configuración no definida.

Configuración del usuario (habilitada)

FILTRO WIN10

General
Delegación

Filtro WMI

Descripción: Filtro para equipos con win 10
Editar filtro...

Consultas:

Espacio de nombres	Consulta
root\CIMv2	SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.%"

Objetos de directiva de grupo que usan este filtro WMI

Los siguientes GPO están vinculados a este filtro WMI:

GPO

DEV-Security-Policy
RESEARCH-Data-Protection
SUPPORT-Access-Control

Ilustración 8 Filtro para Equipos con Windows 10

FILTRO DE RAM

General
Delegación

Filtro WMI

Descripción: Aplica solo en equipos co mas de 8 gb de ram
Editar filtro...

Consultas:

Espacio de nombres	Consulta
root\CIMv2	SELECT * FROM Win32_ComputerSystem WHERE TotalPhysicalMemory > 8589934592

Objetos de directiva de grupo que usan este filtro WMI

Los siguientes GPO están vinculados a este filtro WMI:

GPO

DEV-Security-Policy

Ilustración 9 Filtro para Equipos con RAM de 8 GB

RESEARCH-Data-Protection

Ámbito
Detalles
Configuración
Delegación

Vínculos

Mostrar vínculos en esta ubicación:
INFORCAP.LOCAL

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vínculo habilitado	Ruta
INFORCAP.LOCAL	No	Sí	INFORCAP.LOCAL

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
Investigacion Clinica (INFORCAP\Investigacion Clinica)
Usuarios autenticados

Agregar...
Quitar
Propiedades

Filtrado WMI

Este GPO está vinculado al siguiente filtro WMI:

FILTRO WIN10
Abrir

Ilustración 10 Filtro de Seguridad

DEV-Security-Policy

Ámbito
Detalles
Configuración
Delegación

Vínculos

Mostrar vínculos en esta ubicación:
INFORCAP.LOCAL

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vínculo habilitado	Ruta
INFORCAP.LOCAL	No	Sí	INFORCAP.LOCAL

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
Desarrollo Software Medico (INFORCAP\Desarrollo Software Medico)
Usuarios autenticados

Agregar...
Quitar
Propiedades

Filtrado WMI

Este GPO está vinculado al siguiente filtro WMI:

FILTRO DE RAM
Abrir

SUPPORT-Access-Control

Ámbito

Detalles

Configuración

Delegación

Vinculos

Mostrar vinculos en esta ubicación: INFORCAP.LOCAL

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vínculo habilitado	Ruta
INFORCAP.LOCAL	No	Si	INFORCAP.LOCAL

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre

Soporte Tecnico (INFORCAP\Soporte Tecnico)

Usuarios autenticados

Agregar...

Quitar

Propiedades

Filtrado WMI

Este GPO está vinculado al siguiente filtro WMI:

FILTRO WIN10

Abrir

```
Microsoft Windows [Versión 10.0.17763.7434]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador.WIN-OG13JNQ38J3>gpresult /r

Herramienta de resultados para la Directiva de grupos del
sistema operativo Microsoft (R) Windows (R) v2.0
© 2018 Microsoft Corporation. Todos los derechos reservados.

Creado el 17/06/2025 a las 18:27:28

RSOP datos para INFORCAP\Administrador en WIN-OG13JNQ38J3 : modo de inicio de sesión
-----
Configuración del sistema operativo: Controlador de dominio principal
Versión del sistema operativo: 10.0.17763
Nombre de sitio: Default-First-Site-Name
Perfil móvil: n/a
Perfil local: C:\Users\Administrador.WIN-OG13JNQ38J3
¿Conectado a un vínculo de baja velocidad?: No

CONFIGURACIÓN DE EQUIPO
-----
CN=WIN-OG13JNQ38J3,OU=Domain Controllers,DC=INFORCAP,DC=LOCAL
Última vez que se aplicó la Directiva de grupo: 17/06/2025 a las 18:27:01
Directivas de grupo aplicadas desdeWIN-OG13JNQ38J3.INFORCAP.LOCAL
Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kbps
Nombre de dominio: INFORCAP
Tipo de dominio: Windows 2008 o posterior

Objetos de directiva de grupo aplicados
-----
Default Domain Controllers Policy
Directiva de grupo local

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
DEV-Security-Policy
Filtrar: Denegado (Filtro WMI)
Filtro WMI: FILTRO DE RAM
```

Ilustración 11 Validación por gpresult