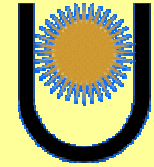


# **SEGURIDAD EN** **WINDOWS 2000 SERVER**

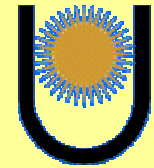


## **Alegre López, Anita**

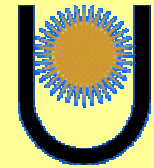
- DPTO. DE INFORMÁTICA
- FA.C.E.N.A.
- UNIVERSIDAD NACIONAL DEL NORDESTE
- (ARGENTINA)

## **Quintana, Miriam Carolina**

- DPTO. DE INFORMÁTICA
- FA.C.E.N.A.
- UNIVERSIDAD NACIONAL DEL NORDESTE
- (ARGENTINA)

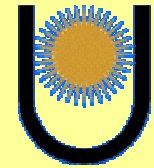


- **INTRODUCCIÓN.**
- **DEFINICION DE RIESGO DE SEGURIDAD.**
- **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000.**
- **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION.**
- **ADMINISTRAR REVISIONES.**
- **AUDITORÍA Y DETECCIÓN DE INTRUSIONES.**
- **RESPONDER A LAS INCIDENCIAS.**
- **CONCLUSIÓN.**



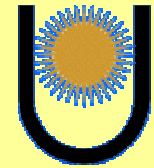
## INTRODUCCION

- A medida que aumenta la interconexión global del planeta:
  - Se dispone de información en cualquier lugar,
  - En cualquier momento y
  - En cualquier dispositivo.
- Encuesta sobre Delitos y Seguridad Informáticos del 2001 (*Computer Crime and Security Survey*) publicada por el CSI (*Computer Security Institute*) y el FBI (*Federal Bureau of Investigation*):
  - El 85 % de las grandes empresas y agencias del gobierno detectaron infracciones de seguridad.
- Independientemente de cuál sea el entorno, es muy recomendable tomarse en serio la seguridad.



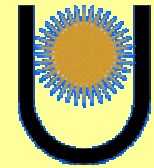
## INTRODUCCION

- Muchas organizaciones subestiman el valor del entorno de tecnología de la información (TI):
  - No tienen en cuenta costos indirectos importantes.
  - Las pérdidas podrían ascender al valor de la organización.
- Los sistemas informáticos más seguros del mundo son los que están completamente aislados de:
  - Los usuarios.
  - Otros sistemas.
- En el mundo real necesitamos sistemas informáticos que funcionen en red, a menudo en redes públicas.



## INTRODUCCION

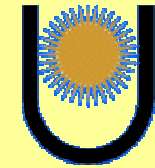
- Esta guía ayudará a:
  - Identificar los riesgos inherentes a un entorno de red.
  - Determinar el nivel de seguridad apropiado para el entorno.
  - Conocer los pasos necesarios para alcanzar ese nivel de seguridad.



## INTRODUCCION

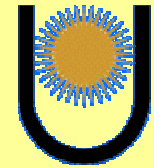
### Microsoft Operations Framework (MOF):

- Conjunto de prácticas recomendadas, principios y modelos que garantizan la capacidad de administración de los sistemas de producción fundamentales, brindando:
  - Seguridad
  - Confiabilidad
  - Disponibilidad
  - Soporte



# INTRODUCCION

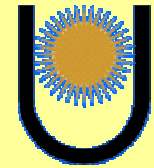




## INTRODUCCION

### Implementar y mantener la seguridad

- En octubre de 2001, Microsoft lanzó el Programa Estratégico de Protección de Tecnología (STPP, *Strategic Technology Protection Program*).
- Objetivo:
  - Integrar los productos, los servicios y el soporte del Microsoft dedicados a la seguridad.
- Microsoft divide el proceso de mantener un entorno seguro en dos fases relacionadas:
  - Implementar la seguridad.
  - Mantener la seguridad.



## **INTRODUCCION**

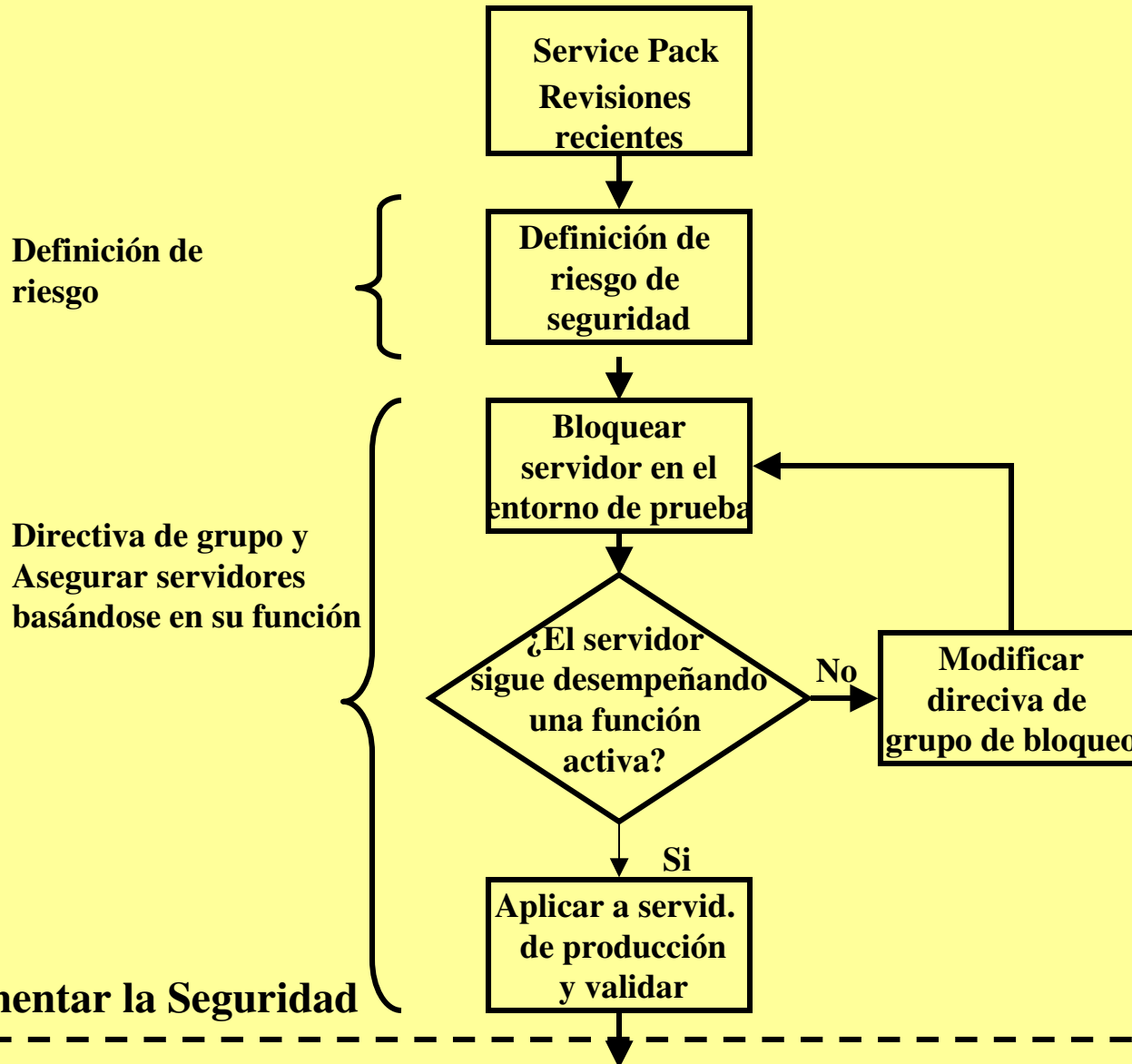
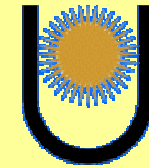
### **Implementar la seguridad**

- Se deben seguir las recomendaciones especificadas en el Microsoft Security Tool Kit.

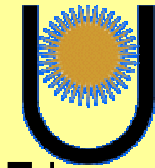
### **Mantener la seguridad**

- Cuando el sistema está configurado y en funcionamiento, es necesario:
  - Adoptar medidas preventivas contra las amenazas.
  - Responder con eficacia cuando se produzcan.

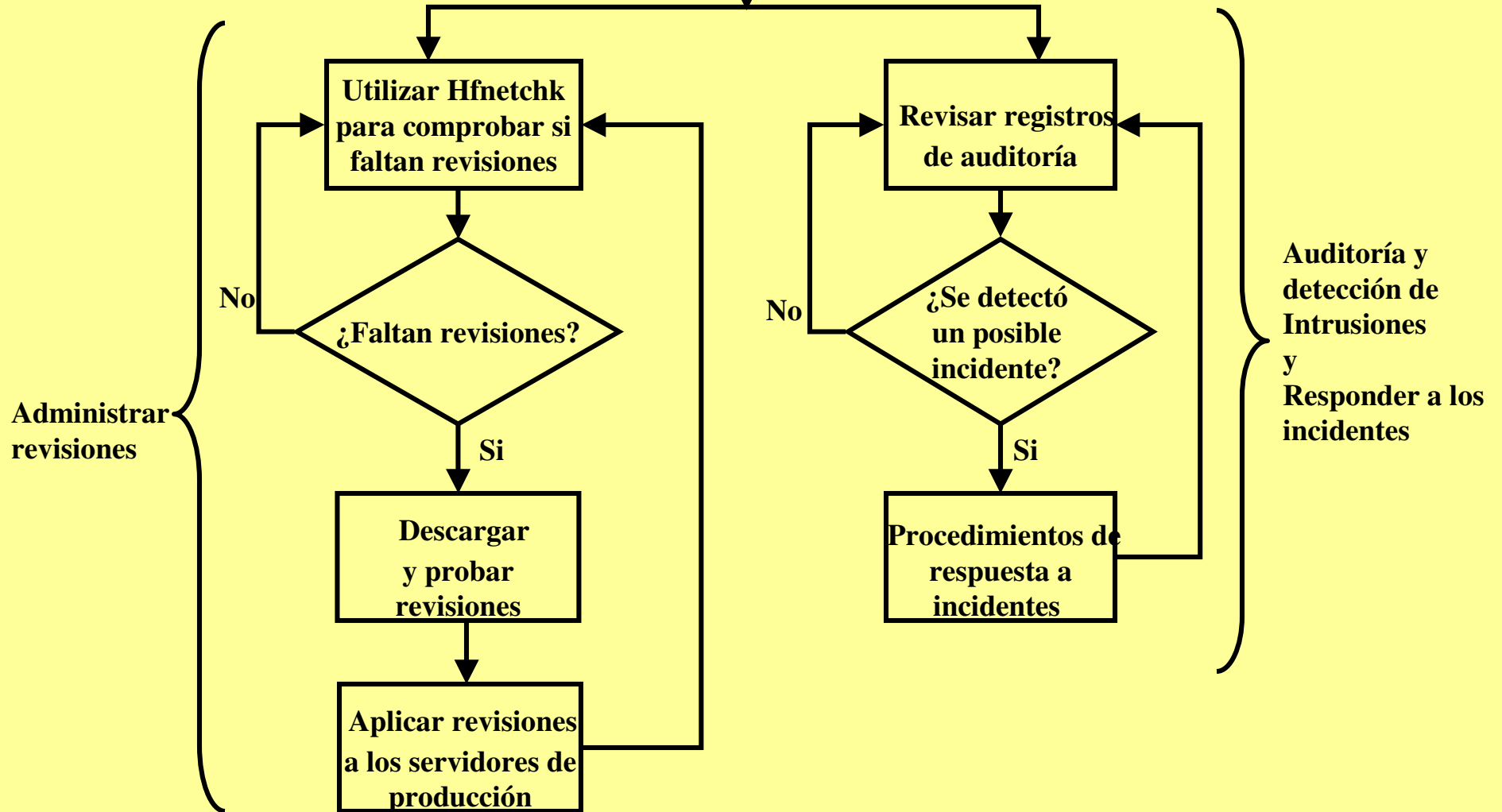
# Seguridad en Windows 2000 Server

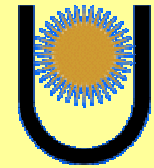


# Seguridad en Windows 2000 Server

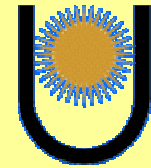


## Mantener la Seguridad





- **INTRODUCCIÓN.**
- **DEFINICION DE RIESGO DE SEGURIDAD.**
- **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000.**
- **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION.**
- **ADMINISTRAR REVISIONES.**
- **AUDITORÍA Y DETECCIÓN DE INTRUSIONES.**
- **RESPONDER A LAS INCIDENCIAS.**
- **CONCLUSIÓN.**

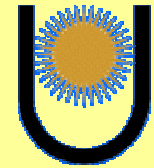


## **DEFINICION DE RIESGO DE SEGURIDAD**

- Al identificar las amenazas a la seguridad, se deben tener en cuenta dos factores principales:
  - Los tipos de ataques que seguramente se sufrirán.
  - Los lugares donde pueden ocurrir.

### **Administración de riesgos**

- A mayor nivel de seguridad en una organización:
  - Más costosa resultará su implementación.
  - Más posibilidades habrá de que se reduzca su funcionalidad.



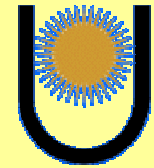
## DEFINICION DE RIESGO DE SEGURIDAD

### Administración de riesgos

- Luego de evaluar los posibles riesgos, para aumentar la funcionalidad quizá se deba:
  - Reducir el nivel de seguridad.
  - Reducir el costo.

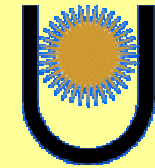
### Conceptos a considerar:

- **Recurso:** es cualquier elemento del entorno que se intente proteger:
  - Datos.
  - Aplicaciones.
  - Servidores.
  - Enrutadores.
  - Personas.



## DEFINICION DE RIESGO DE SEGURIDAD

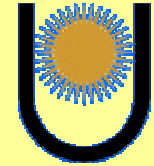
- **Amenaza:** es una persona, un lugar o un elemento que puede tener acceso a los recursos y dañarlos.
- **Vulnerabilidad:** es un punto en el que un recurso es susceptible de ser atacado. Se puede interpretar como un punto débil.
- **Explotación:** es una amenaza que se aprovecha de una vulnerabilidad del entorno para tener acceso a un recurso.
- **Contramedida:** se aplica para contrarrestar las amenazas y vulnerabilidades y de este modo reducir el riesgo del entorno.



# DEFINICION DE RIESGO DE SEGURIDAD

## Amenazas a entornos informáticos

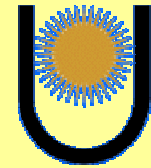
Tipo de amenaza	Ejemplo
Natural y física	Fuego, Agua, Viento Terremoto, Corte eléctrico.
No intencionada	Empleados no informados. Clientes no informados.
Intencionada	Atacantes. Terroristas. Espías industriales. Gobiernos. Código malicioso.



# DEFINICION DE RIESGO DE SEGURIDAD

## Vulnerabilidades en entornos informáticos

<b>Tipo de vulnerabilidad</b>	<b>Ejemplo</b>
<b>Física</b>	<b>Puertas sin cerrar.</b>
<b>Natural</b>	<b>Sistema antiincendios averiado.</b>
<b>De hardware y software</b>	<b>Software antivirus no actualizado.</b>
<b>De medios</b>	<b>Interferencia eléctrica.</b>
<b>De comunicación</b>	<b>Protocolos no cifrados.</b>
<b>Humana</b>	<b>Procedimientos no seguros de asistencia técnica.</b>



# DEFINICION DE RIESGO DE SEGURIDAD

## Explotaciones en entornos informáticos

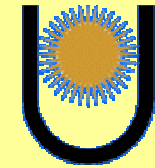
Tipo de explotación	Ejemplo
Explotación de vulnerabilidad técnica	Ataques a fuerza bruta. Desbordamiento del búfer. Problemas de configuración. Ataques repetidos. Secuestro de sesión.
Denegación de servicio	Daño físico. Eliminación de recursos. Modificación de recursos. Saturación de recursos.



# DEFINICION DE RIESGO DE SEGURIDAD

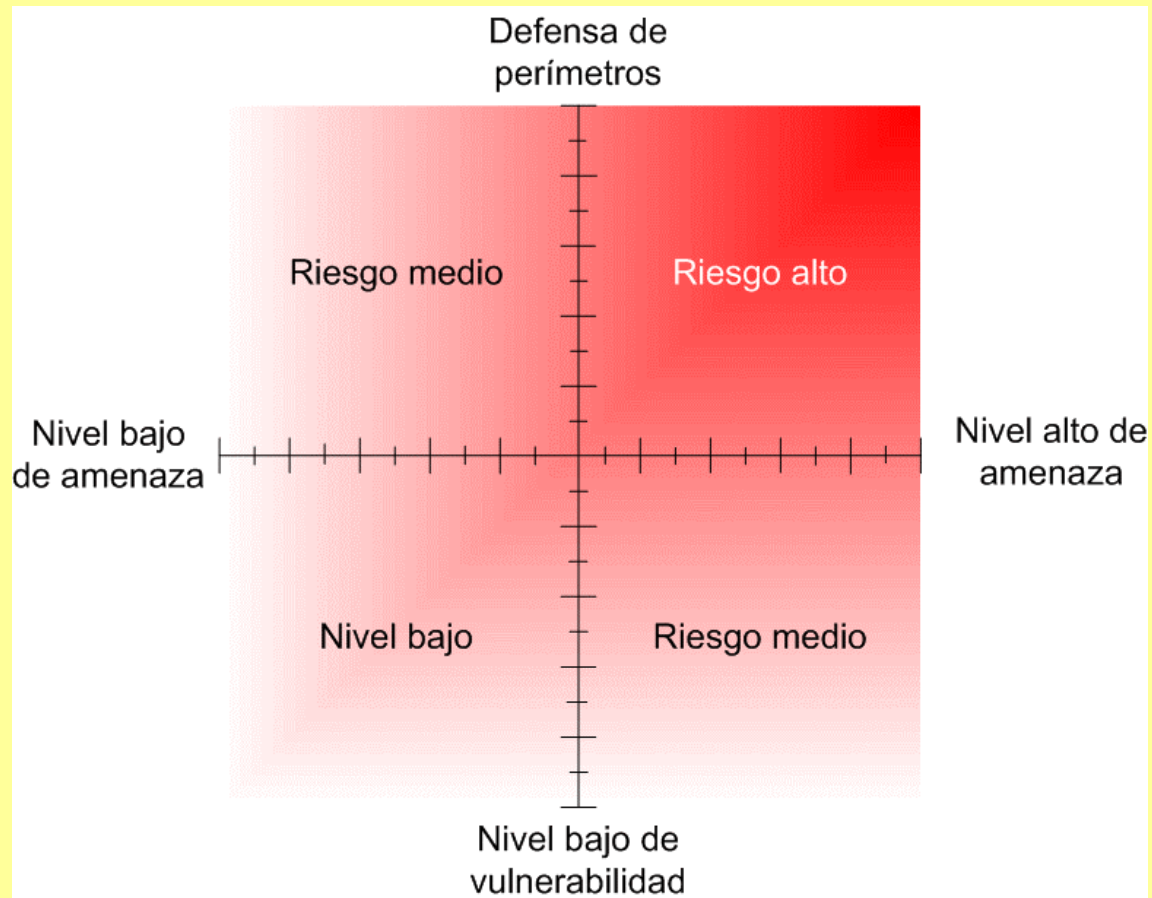
## Resultados de explotaciones

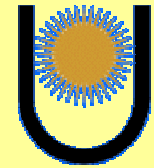
Resultados de una explotación	Ejemplo
Pérdida de confidencialidad	Acceso no autorizado Reasignación de privilegios Personificación o robo de identidad
Pérdida de integridad	Daños en datos Desinformación
Pérdida de disponibilidad	Denegación de servicio



# DEFINICION DE RIESGO DE SEGURIDAD

## Relación entre amenazas, vulnerabilidades y riesgo

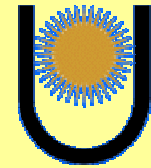




## **DEFINICION DE RIESGO DE SEGURIDAD**

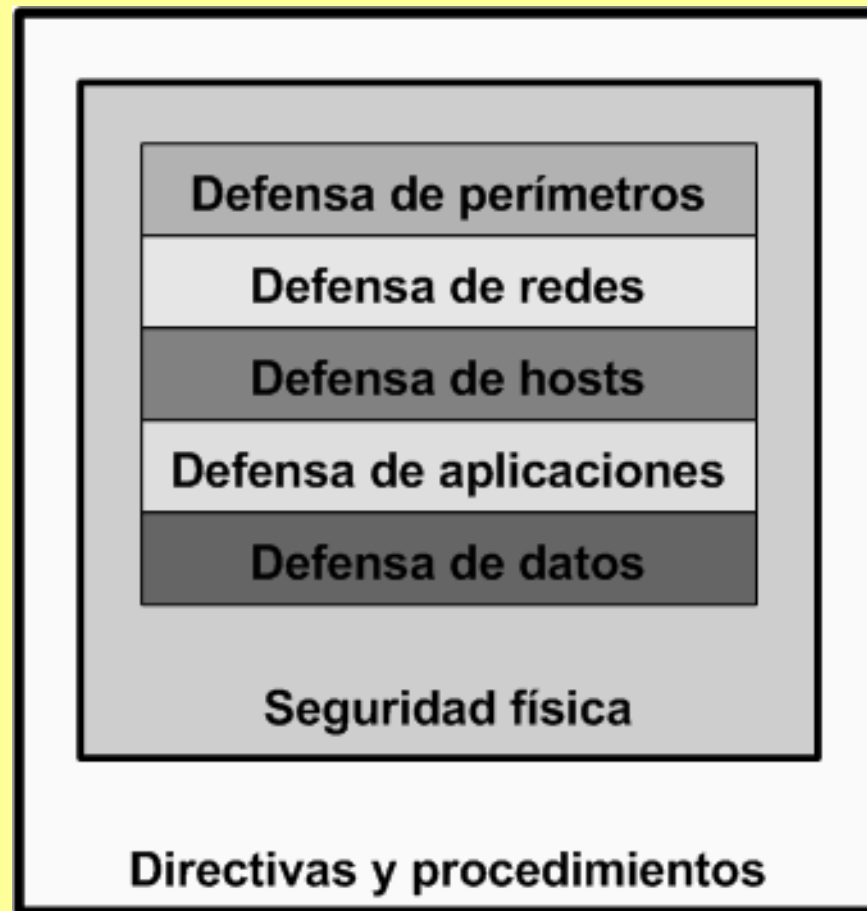
### **Defensa en profundidad o Seguridad multicapa**

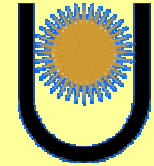
- Describe la aplicación de contramedidas de seguridad con el fin de formar un entorno de seguridad cohesivo sin un solo punto de error.
- El despliegue de varias capas de seguridad, garantiza que, si se pone en peligro una capa, las otras ofrecerán la seguridad necesaria para proteger los recursos.



# DEFINICION DE RIESGO DE SEGURIDAD

Estrategia de seguridad eficaz

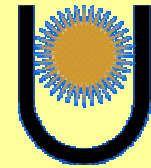




## **DEFINICION DE RIESGO DE SEGURIDAD**

### **Ejemplos de ataques:**

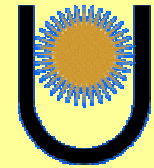
- El robo de datos:
  - Robar un equipo portátil.
  - Detectar paquetes en la red interna.
- La ejecución de código malicioso:
  - Activar un gusano desde el interior de la organización.
- El robo de información de seguridad crítica:
  - Cintas de copia de seguridad.
  - Manuales de funcionamiento.
  - Diagramas de red.



## **DEFINICION DE RIESGO DE SEGURIDAD**

### **Posibles medidas de seguridad física:**

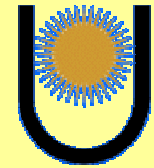
- Establecer seguridad física para todas las áreas del edificio:
  - Tarjetas de acceso.
  - Dispositivos biométricos.
  - Guardias de seguridad.
- Requerir a los visitantes que vayan acompañados en todo momento.
- Requerir a los visitantes que firmen un registro de entrada de todos los dispositivos informáticos.



## **DEFINICION DE RIESGO DE SEGURIDAD**

### **Posibles medidas de seguridad física:**

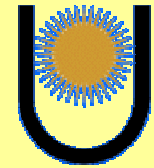
- Requerir a todos los empleados que registren cualquier dispositivo portátil de su propiedad.
- Fijar físicamente todos los equipos de sobremesa y portátiles a las mesas.
- Ubicar los servidores en salas separadas a las que sólo tengan acceso los administradores.



# DEFINICION DE RIESGO DE SEGURIDAD

## Directivas y procedimientos

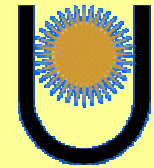
- Habrá personas del entorno que necesiten acceso de alto nivel a los sistemas.
- La estrategia de seguridad será perfecta si se puede garantizar que estas personas no van a hacer uso indebido de los derechos que se les han concedido.
- Los empleados deben someterse a un proceso de investigación de seguridad.
- Deberá hacerse una investigación más rigurosa para aquellos que vayan a tener un mayor acceso a los sistemas.



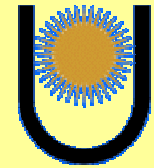
## **DEFINICION DE RIESGO DE SEGURIDAD**

### **Métodos de ataques comunes y medidas preventivas**

- Los empleados tienen que ser conscientes de las directivas de seguridad y de lo que está permitido y prohibido.
- Asegurarse de que sólo dispositivos específicos e identificados de la red permiten la conectividad mediante acceso remoto.
- Deshabilitar NetBIOS sobre TCP/IP, en los equipos directamente conectados a Internet a través del servidor de seguridad externo.

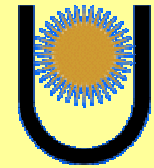


- **INTRODUCCIÓN.**
- **DEFINICION DE RIESGO DE SEGURIDAD.**
- **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000.**
- **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION.**
- **ADMINISTRAR REVISIONES.**
- **AUDITORÍA Y DETECCIÓN DE INTRUSIONES.**
- **RESPONDER A LAS INCIDENCIAS.**
- **CONCLUSIÓN.**



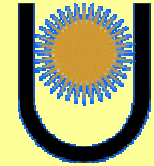
## **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000**

- Asegurar el entorno usando la Directiva de grupo.
- Directiva de grupo:
  - Método para definir los procedimientos de configuración y administración de la seguridad del entorno.
  - Un objeto de usuario o de equipo puede estar sujeto a varios Objetos de directiva de grupo (GPO).
  - Los GPO se aplican de forma secuencial y la configuración se acumula.



## **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000**

- Los controladores de dominio deben replicar los cambios de la Directiva de grupo en otros controladores de dominio.
- Este proceso puede tardar hasta 15 minutos en un sitio.
- Una vez replicados los cambios debe transcurrir otro período de tiempo:
  - se actualizan los cambios de la directiva en el equipo de destino.



## **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000**

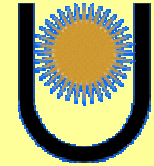
### **Estructura de la Directiva de grupo**

Las opciones de configuración de la Directiva de grupo se almacenan en dos ubicaciones:

- GPO en Active Directory.
- Archivos de plantillas de seguridad en el sistema de archivos local.

### **Plantillas de Windows 2000**

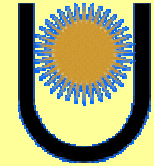
- Predeterminadas: para un entorno de seguridad baja.
- Incrementales: proporcionan opciones de configuración de seguridad adicionales con respecto a las plantillas básicas.



## **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000**

### **Se debería considerar:**

- Las plantillas se pueden modificar utilizando un editor de texto.
- Los cambios realizados en la seguridad de los sistemas de TI se deben evaluar en un entorno de prueba antes de realizar cambios en el entorno de producción.
- Las pruebas son necesarias para:
  - Determinar si el entorno es funcional después de realizar los cambios.
  - Verificar si se ha aumentado el nivel de seguridad.



## **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000**

### **Diseño e implementación de directivas**

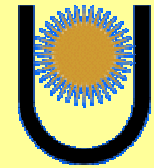
Para simplificar el proceso de aplicación y comprobación de la configuración, se recomienda aplicarla en dos niveles:

- *Nivel de dominios:* cumplir los requisitos de seguridad comunes.
- *Nivel de unidad organizativa:* cumplir los requisitos de seguridad específicos.

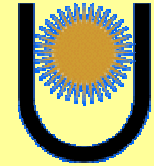
### **Herramientas del kit de recursos**

\* GpoTool

\* GPRresult



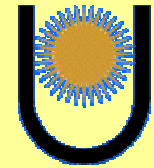
- **INTRODUCCIÓN.**
- **DEFINICION DE RIESGO DE SEGURIDAD.**
- **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000.**
- **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION.**
- **ADMINISTRAR REVISIONES.**
- **AUDITORÍA Y DETECCIÓN DE INTRUSIONES.**
- **RESPONDER A LAS INCIDENCIAS.**
- **CONCLUSIÓN.**



## **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION**

### **Directivas de línea de base:**

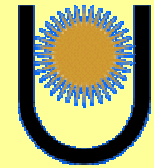
- Pueden definirse para todos los servidores miembros y controladores de dominio de la organización.
- Su funcionalidad es mínima.
- Permiten que los servidores se comuniquen con otros equipos en el mismo dominio.
- Permiten la autenticación a través de los controladores de dominio.
- A partir de ellas se pueden implementar otras directivas incrementales.



## **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION**

### **Tipos de Directivas:**

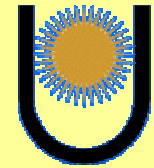
- **Directiva para todo el dominio:** requisitos de seguridad comunes:
  - Directivas de cuentas que se deben aplicar para todos los servidores y estaciones de trabajo.
  
- **Directivas para el controlador de dominio:** se aplican a la OU de los controladores de dominio:
  - Directivas de auditoría.
  - Opciones de seguridad.



## **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION**

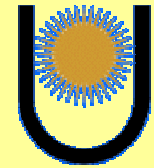
### **Tipos de Directivas:**

- **Directivas para los servidores miembros:** la configuración común para todos los servidores miembros:
  - Directivas de auditoría.
  - Configuración de servicios.
  - Directivas que restringen el acceso al registro, el sistema de archivos, etc.
- **Directivas para la función del servidor:**
  - De aplicaciones.
  - De archivos y de impresión.
  - De infraestructura.
  - IIS.

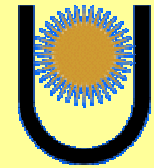


## **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION**

- Los servidores basados en Windows 2000:
  - Proporcionan un gran número de funciones desde el momento en que se instalan.
  - No todos los servidores necesitan todas estas funciones.
- Al definir las tareas que realizarán los servidores se puede:
  - Deshabilitar los elementos innecesarios.
  - Aumentar de esta forma la seguridad en el entorno.

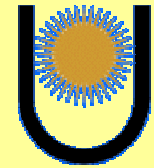


- **INTRODUCCIÓN.**
- **DEFINICION DE RIESGO DE SEGURIDAD.**
- **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000.**
- **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION.**
- **ADMINISTRAR REVISIONES.**
- **AUDITORÍA Y DETECCIÓN DE INTRUSIONES.**
- **RESPONDER A LAS INCIDENCIAS.**
- **CONCLUSIÓN.**



## ADMINISTRAR REVISIONES

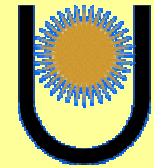
- Es fundamental que el software funcione de manera confiable y no peligre la seguridad ni la estabilidad del entorno de TI (tecnología de la información).
- Para reducir al mínimo los problemas, los programas se comprueban exhaustivamente antes de salir al mercado.
- Es imposible prever todos los ataques que pueden ocurrir en el futuro.
- Hasta que no se implemente la revisión, la seguridad que espera tener y de la que depende puede verse reducida notablemente.



## ADMINISTRAR REVISIONES

### Service Packs

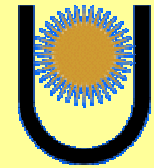
- Mantienen el producto actualizado, corrigen los problemas conocidos y amplían la funcionalidad del equipo.
- Incluyen:
  - Herramientas.
  - Controladores y actualizaciones.
  - Mejoras desarrolladas después de la comercialización del producto.
- Son específicos para cada producto.



## **ADMINISTRAR REVISIONES**

### **Service Packs**

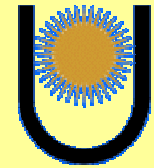
- Se utiliza el mismo Service Pack para actualizar Windows 2000 Server y Windows 2000 Professional.
- Son acumulativos.
- No se necesita instalar el Service Pack anterior antes de instalar el más reciente.



## **ADMINISTRAR REVISIONES**

### **Revisiones o QFE (Ingeniería de corrección rápida)**

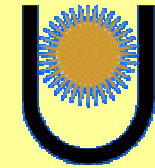
- Es un grupo interno de Microsoft que crea revisiones (hotfix), es decir, revisiones de código para los productos.
- Se envían a clientes con problemas críticos para los que no existe una solución preexistente.
- Son específicas para cada problema.
- Periódicamente, se incorporan grupos de revisiones a los Service Packs, se someten a comprobaciones más rigurosas y se ponen a disposición de todos los clientes.



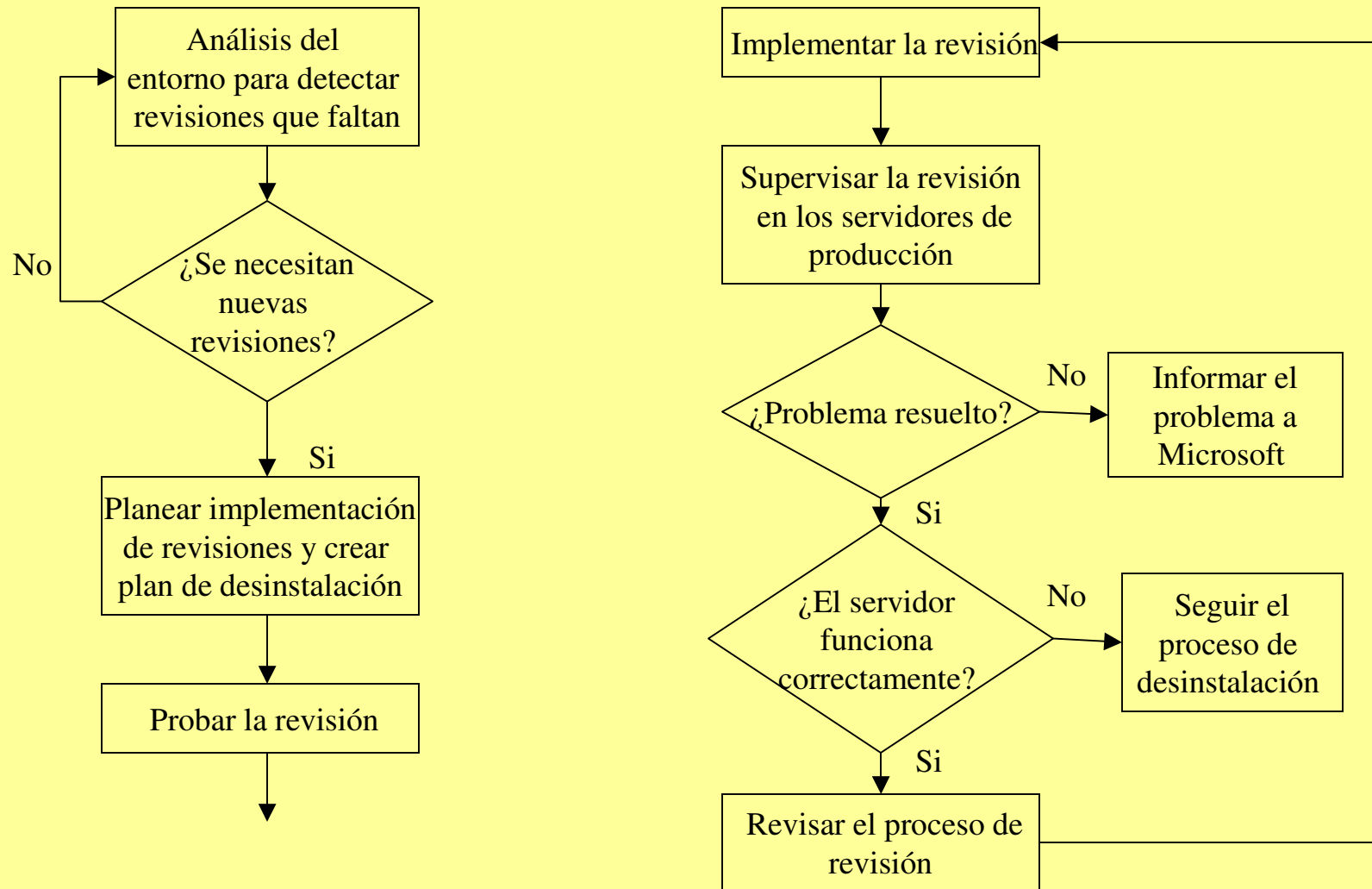
# ADMINISTRAR REVISIONES

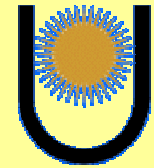
## Revisiones de seguridad

- Diseñadas para eliminar los riesgos de la seguridad.
- Son análogas a las revisiones (hotfix), pero se consideran:
  - Obligatorias, si las circunstancias lo justifican.
  - Deben implementarse rápidamente.



# ADMINISTRAR REVISIONES

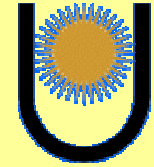




## ADMINISTRAR REVISIONES

### Análisis del entorno para detectar revisiones que faltan

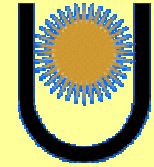
- Se debe analizar de manera continua todos los servidores para asegurarse de que están totalmente actualizados con las revisiones más recientes necesarias.
- Puede utilizar la herramienta: **Microsoft Network Security Hotfix Checker (Hfnetchk)**



## ADMINISTRAR REVISIONES

### Plan

- Cuando se leen avisos de posibles nuevos riesgos de un sistema operativo o una aplicación, se debe evaluar si éstas afectan al entorno.
- Se debe leer toda la información de apoyo correspondiente.
- Esto permitirá:
  - Tomar una decisión inteligente sobre si existe un riesgo significativo para el entorno.
  - Determinar la respuesta apropiada.

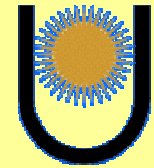


# ADMINISTRAR REVISIONES

## Clasificación de las revisiones

Determinar:

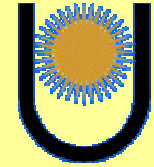
- La importancia para el entorno.
- Si es urgente que la instale.
- La cantidad de pruebas que se debe realizar.



## **ADMINISTRAR REVISIONES**

### **Realizar pruebas de las revisiones**

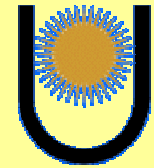
- Comprobar exhaustivamente todas las revisiones que se instalarán en el entorno.
- La cantidad de pruebas necesarias dependerá de cómo haya clasificado la revisión.
- Todas las pruebas deben realizarse en servidores que se parezcan lo más posible a los servidores de producción.



# ADMINISTRAR REVISIONES

## Evaluación de la revisión

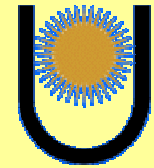
- Se debe incluir los pasos siguientes:
  - Identificación del propietario de la revisión.
  - Revisión de toda la documentación.
  - Verificación de la categoría de la revisión.



## **ADMINISTRAR REVISIONES**

### **Creación de un plan de contingencias**

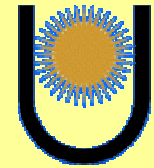
- Se debe contar con un plan de acción para restaurar el sistema al estado en el que estaba antes de instalar la revisión.
- En algunos casos, esto se hace realizando una copia de seguridad instantánea de un servidor antes de la instalación.
- Sea cual sea el plan de contingencias, se debe realizar pruebas exhaustivas.



# ADMINISTRAR REVISIONES

## Instalación de las revisiones

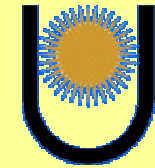
- Luego de realizar las pruebas, se estará listo para instalar la revisión.
- Esto puede hacerse por distintos métodos:
  - Manual.
  - Directivas de grupo.
  - Archivos de comandos.



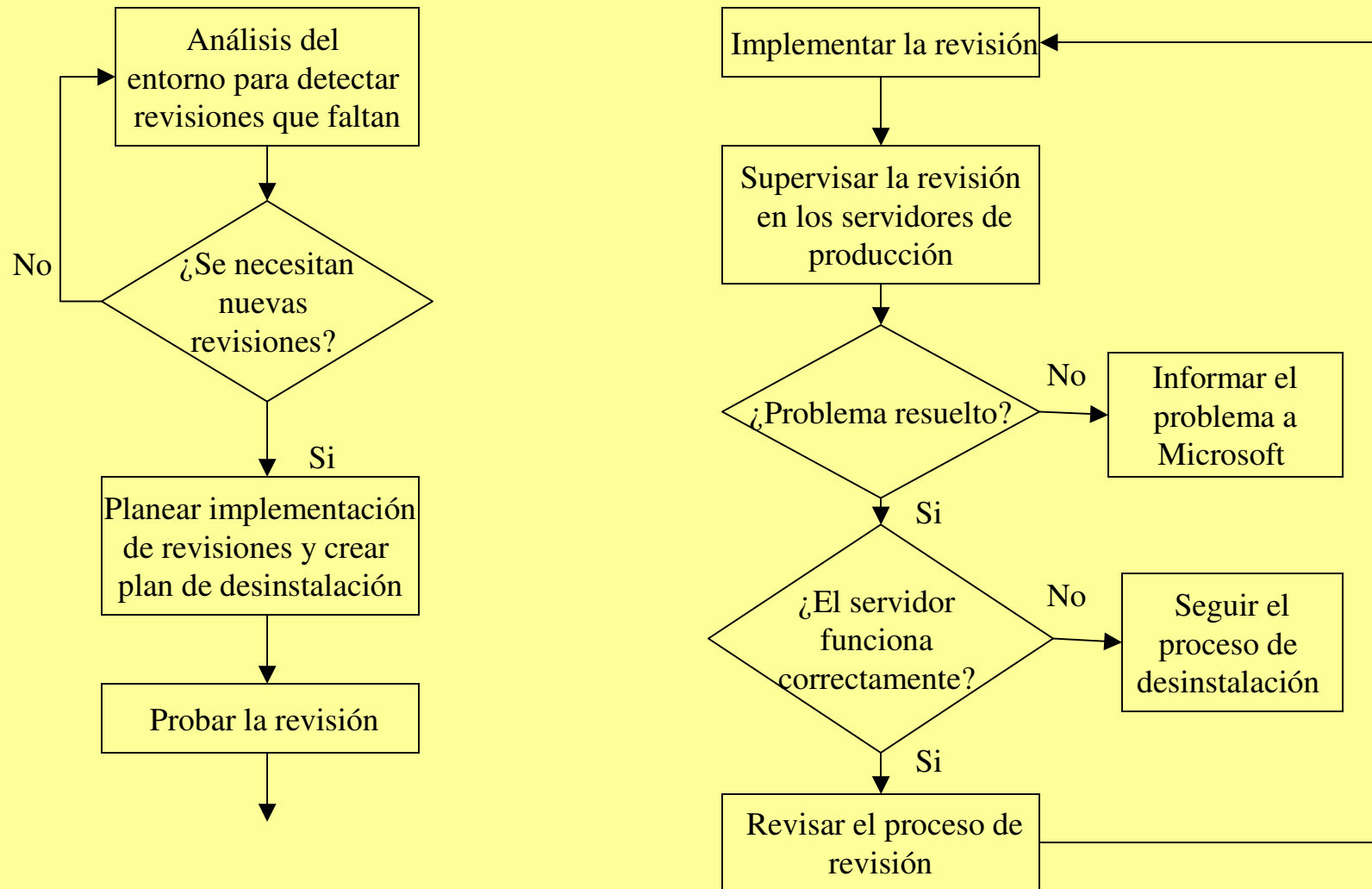
# ADMINISTRAR REVISIONES

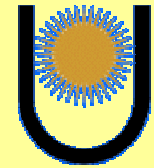
## Supervisión

- Después de instalar las revisiones en el entorno de producción, es necesario:
  - Seguir supervisando los servidores.
  - Revisar los contadores del Registro de Sucesos.
- Si se observa algún error en el equipo, se debe:
  - Realizar pruebas para asegurarse de que no está relacionado con la revisión implementada.

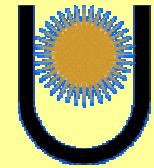


# ADMINISTRAR REVISIONES



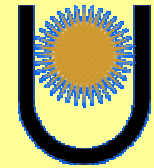


- **INTRODUCCIÓN.**
- **DEFINICION DE RIESGO DE SEGURIDAD.**
- **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000.**
- **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION.**
- **ADMINISTRAR REVISIONES.**
- **AUDITORÍA Y DETECCIÓN DE INTRUSIONES.**
- **RESPONDER A LAS INCIDENCIAS.**
- **CONCLUSIÓN.**



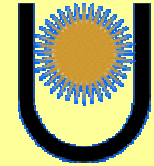
# AUDITORÍA Y DETECCIÓN DE INTRUSIONES

- Cualquier entorno informático funcional está sujeto a ataques.
- Los ataques verdaderos suelen producirse a menudo tras varios ataques infructuosos.
- Cuanto antes se detecte el ataque, más fácil resultará contener los daños.
- Para recuperarse de un ataque, se necesita conocer los daños que se han producido.



# AUDITORÍA Y DETECCIÓN DE INTRUSIONES

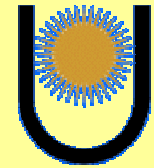
- La auditoría y la detección de intrusiones ayudan a determinar el origen del ataque.
- Los sucesos de auditoría pueden dividirse en dos categorías:
  - *De acierto*: indican que un usuario ha conseguido obtener acceso a un recurso.
  - *De error*: indican que se produjo un intento fallido.



# AUDITORÍA Y DETECCIÓN DE INTRUSIONES

## Sucesos para auditar

- Windows 2000 incluye varias categorías de auditoría para los sucesos de seguridad:
  - De inicio de sesión.
  - De inicio de sesión de cuentas.
  - Acceso a objetos.
  - Acceso del servicio de directorio.
  - Uso de privilegios.
  - Seguimiento de procesos.
  - Del sistema.
  - Cambio de directivas.



## AUDITORÍA Y DETECCIÓN DE INTRUSIONES

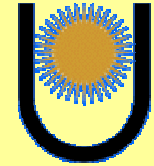
*Sucesos de inicio de sesión que aparecen en el Registro de Sucesos*

528. Un usuario inició la sesión correctamente en un equipo.

529. El intento de inicio de sesión se realizó con:

- un nombre de usuario desconocido o
- un nombre de usuario conocido y una contraseña incorrecta.

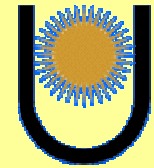
530. La cuenta de usuario intentó iniciar la sesión fuera del período de tiempo permitido.



## AUDITORÍA Y DETECCIÓN DE INTRUSIONES

*Para proteger la seguridad de los Registros de Sucesos, debería:*

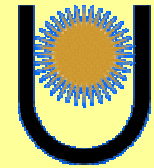
- Definir una directiva para el almacenamiento, la sobrescritura y el mantenimiento de todos los registros de sucesos.
- Evitar el acceso de invitados a los registros de sucesos.
- El plan de seguridad debe incluir también la seguridad física de todos los servidores.
- Poner en práctica un método de eliminación o almacenamiento de los registros de sucesos en una ubicación independiente del servidor físico.



# AUDITORÍA Y DETECCIÓN DE INTRUSIONES

## Supervisar las intrusiones y los sucesos de seguridad

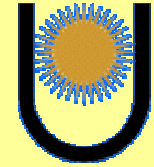
- Cuando las intrusiones se detectan una vez que se ha producido el ataque por medio de la inspección de los archivos de registro, se denomina, detección de intrusiones *pasiva*.
- Cuando las intrusiones se detectan mientras se produce el ataque, se denomina, detección de intrusiones *activa*.



# AUDITORÍA Y DETECCIÓN DE INTRUSIONES

## Métodos de detección pasivos

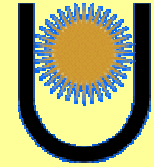
- Los sistemas de detección de intrusiones pasivos implican la revisión manual de los registros de sucesos y aplicaciones.
- La inspección requiere:
  - El análisis y la detección de pautas de ataque en los datos de los registros de sucesos.



# AUDITORÍA Y DETECCIÓN DE INTRUSIONES

## Métodos de detección pasivos

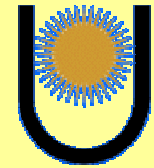
- Existen varias herramientas que pueden facilitar la revisión de los registros de sucesos:
  - *Visor de sucesos*: Permite ver los registros de aplicaciones, de seguridad y del sistema.
  - *Dump Event Log (Dumpele.exe)*: Guarda un registro de sucesos de un sistema local o remoto en un archivo de texto separado por tabulaciones.
  - *EventCombMT*: Tiene varios subprocesos que analizan registros de sucesos de varios servidores.



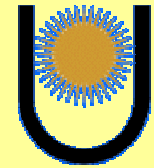
# AUDITORÍA Y DETECCIÓN DE INTRUSIONES

## Métodos de detección activos

- Los sistemas de detección de intrusiones activos analizan:
  - El tráfico de red entrante en el nivel de aplicaciones.
  - Buscan métodos conocidos de ataques.
- Si se recibe un paquete sospechoso, el sistema de detección de intrusiones:
  - Normalmente lo rechaza.
  - Guarda una entrada en un archivo de registro.
- También se puede alertar a un administrador si se detecta un ataque serio.

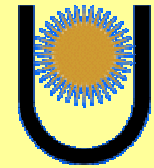


- **INTRODUCCIÓN.**
- **DEFINICION DE RIESGO DE SEGURIDAD.**
- **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000.**
- **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION.**
- **ADMINISTRAR REVISIONES.**
- **AUDITORÍA Y DETECCIÓN DE INTRUSIONES.**
- **RESPONDER A LAS INCIDENCIAS.**
- **CONCLUSIÓN.**



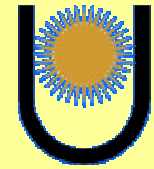
## RESPONDER A LAS INCIDENCIAS

- Muchas organizaciones no aprenden cómo responder a una incidencia de seguridad hasta que sufren un ataque.
- *Existen medidas de prudencia para minimizar el número y la gravedad de las incidencias de seguridad:*
  - Establecer claramente todas las directivas y procedimientos y exigir su cumplimiento.
  - Supervisar y analizar de forma rutinaria el tráfico de la red y el rendimiento del sistema.
  - Evaluar de forma rutinaria la vulnerabilidad del entorno.



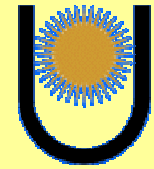
## RESPONDER A LAS INCIDENCIAS

- *Existen medidas de prudencia para minimizar el número y la gravedad de las incidencias de seguridad:*
  - Comprobar los servidores de forma rutinaria para garantizar que tienen instaladas las revisiones más recientes.
  - Establecer programas de formación en seguridad para el personal del departamento de TI y para los usuarios finales.
  - Publicar avisos de seguridad que recuerden a los usuarios sus responsabilidades y restricciones, también advertencias de posibles acciones legales en caso de infracción.
  - Desarrollar, implementar y exigir una directiva sobre la necesidad de contraseñas complejas.



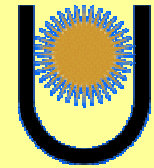
## RESPONDER A LAS INCIDENCIAS

- *Existen medidas de prudencia para minimizar el número y la gravedad de las incidencias de seguridad:*
  - Verificar los procedimientos de copia de seguridad y restauración.
  - Crear un equipo de respuesta a incidencias de seguridad informática (CSIRT).
  - Anotar toda la información del sistema de emergencia en una ubicación central sin conexión, por ejemplo, un bloc de notas o un equipo sin conexión.



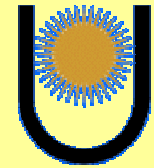
## RESPONDER A LAS INCIDENCIAS

- *El equipo básico de respuesta a incidencias de seguridad informática (CSIRT) es responsable de:*
  - Supervisar los sistemas para detectar infracciones de seguridad.
  - Documentar y catalogar las incidencias de seguridad.
  - Promover la conciencia sobre la seguridad en la empresa.
  - Mantenerse actualizado sobre las nuevas vulnerabilidades y estrategias que emplean los atacantes.



## RESPONDER A LAS INCIDENCIAS

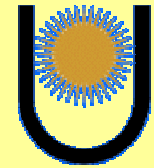
- *El equipo básico de respuesta a incidencias de seguridad informática (CSIRT) es responsable de:*
  - Mantenerse actualizado sobre las nuevas revisiones de software.
  - Analizar y desarrollar nuevas tecnologías para minimizar las vulnerabilidades y los riesgos de seguridad.
  - Proporcionar servicios de consultoría sobre seguridad.
  - Perfeccionar y actualizar de forma continua los sistemas y procedimientos actuales.



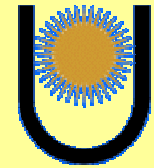
## **RESPONDER A LAS INCIDENCIAS**

### **Definir un plan de respuesta a incidencias**

- Si bien el CSIRT llevará a cabo la mayoría de las acciones, todos los niveles del personal de TI deberían saber como comunicar la incidencia internamente.
- Todos los miembros del equipo deberían revisar con detalle el plan de respuesta a incidencias, que debería ser fácilmente accesible para todo el personal de TI.
- Así, se podrá garantizar que se siguen los procedimientos adecuados cuando se produzca una incidencia.



- **INTRODUCCIÓN.**
- **DEFINICION DE RIESGO DE SEGURIDAD.**
- **ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000.**
- **ASEGURAR SERVIDORES BASANDOSE EN SU FUNCION.**
- **ADMINISTRAR REVISIONES.**
- **AUDITORÍA Y DETECCIÓN DE INTRUSIONES.**
- **RESPONDER A LAS INCIDENCIAS.**
- **CONCLUSIÓN.**

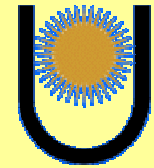


## CONCLUSIÓN

*En el presente estudio se logró:*

- Exponer los principios fundamentales para implementar un sistema de seguridad bajo el entorno Windows 2000 Server, por medio del STTP.
- Identificar los riesgos inherentes a un entorno de red.
- Determinar el nivel de seguridad apropiado para el entorno.
- Definir los pasos necesarios para alcanzar el nivel de seguridad adecuado al entorno.

## Seguridad en Windows 2000 Server



- **[aalegrelopez@yahoo.com.ar](mailto:aalegrelopez@yahoo.com.ar)**
- **[ckintana@hotmail.com](mailto:ckintana@hotmail.com)**
- **<http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SOF.htm>**