

ÍNDICE

[1. Gestión de *logs* 3](#_Toc480469297)

[1.1. Antecedentes 3](#_Toc480469298)

[1.2. Objetivos 3](#_Toc480469299)

[1.3. Checklist 4](#_Toc480469300)

[1.4. Puntos clave 5](#_Toc480469301)

[2. Referencias 7](#_Toc480469302)

# Gestión de *logs*

## Antecedentes

Los sistemas registran la actividad de los usuarios y de sus procesos internos (*login/logout*, origen, tiempo de actividad, acciones, conexiones,…) en registros de eventos o *logs* [[1]](#referencias). La información de estos registros es esencial para elaborar **informes de gestión y para monitorización**.

Entre los eventos que los distintos sistemas registran están por ejemplo: el inicio/fin de sesión, el acceso y modificación de ficheros y directorios, cambios en las configuraciones principales, lanzamientos de programas, etc.

Los registros de actividad de los distintos sistemas y equipos son los datos a partir de los cuales es posible no sólo detectar fallos de rendimiento o mal funcionamiento, sino también **detectar errores e intrusiones.** Con ellos se alimentan sistemas de **monitorización** que convenientemente configurados pueden generar **alertas** en tiempo real. Por otra parte, facilitan el **análisis forense** para el diagnóstico de las causas que originan los incidentes. Por último, son necesarios para verificar el cumplimiento de ciertos requisitos **legales o contractuales** durante las auditorías.

## Objetivos

Determinar los **eventos más significativos** dentro de nuestros sistemas de información que han de ser **registrados**, y en qué modo ha de efectuarse dicho registro.

Establecer mecanismos de **monitorización** que permitan la detección de **intrusiones**, **errores** y **situaciones anómalas** o potencialmente peligrosas [[2]](#referencias).

## Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a la **gestión de *logs***.

Los controles se clasificarán en dos niveles de **complejidad**:

* Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
* Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

* Procesos (**PRO**): aplica a la dirección o al personal de gestión.
* Tecnología (**TEC**): aplica al personal técnico especializado.
* Personas (**PER**): aplica a todo el personal.

|  |  |  |  |
| --- | --- | --- | --- |
| **NIVEL** | **ALCANCE** | **CONTROL** | |
| B | PRO | **Qué actividad debe ser registrada**  Analizas qué eventos producidos en tus sistemas de información necesitas registrar. |  |
| B | PRO | **Información relevante incluida en el registro**  Determinas para cada tipo de suceso la información más significativa que se debe almacenar. |  |
| B | PRO | **Formato de la información registrada**  Detallas el formato de tus *logs* para facilitar su posterior análisis. |  |
| A | TEC | **Elección del mecanismo de registro**  Seleccionas el sistema de registro más apropiado para tu empresa. |  |
| B | TEC | **Protección y almacenamiento**  Proteges convenientemente la información registrada en los *logs*. |  |
| B | TEC | **Sincronización del reloj**  Revisas la correcta sincronización temporal de todos los dispositivos. |  |
| B | TEC | **Sistemas de monitorización y alerta**  Configuras los sistemas de monitorización de eventos para generar en tiempo real alertas ante posibles errores y comportamientos anómalos. |  |

**Revisado por**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Fecha:** \_\_\_\_\_\_\_\_\_\_

## Puntos clave

Los puntos clave de esta política son:

* **Qué actividad debe ser registrada.** Para obtener la información crítica sobre el funcionamiento de nuestros activos de información, analizaremos la actividad relevante que nos interesa registrar. Podríamos considerar registrar, entre otros, los siguientes eventos:
  + acceso, creación, borrado y actualización de información confidencial;
  + inicio y fin de conexión en la red corporativa;
  + inicio y fin de ejecución de aplicaciones y sistemas;
  + inicio y fin de sesión de usuario en aplicaciones y sistemas; intentos de inicio de sesión fallidos;
  + cambios en las configuraciones de los sistemas y aplicativos más importantes;
  + modificaciones en los permisos de acceso;
  + funcionamiento o finalización anómalos de aplicativos;
  + aproximación a los límites de uso de ciertos recursos físicos:
    - capacidad de disco;
    - memoria;
    - ancho de banda de red;
    - uso de CPU;
  + indicios de actividad sospechosa detectada por antivirus, Sistemas de Detección de Intrusos (IDS), etc.;
  + transacciones relevantes dentro de los aplicativos.
* **Información relevante incluida en el registro.** Detallaremos los elementos de información más útiles que deben ser incluidos en los distintos registros. Los más habituales son:
  + identificador del usuario que realiza la acción;
  + identificación del elemento sobre el que se realiza la acción (ficheros, bases de datos, equipos, etc.);
  + identificación de dispositivos, ya sea a través de sus direcciones IP, direcciones MAC, etc.;
  + identificación de protocolos;
  + fecha y hora de ocurrencia del evento;
  + tipología del evento.
* **Formato de la información registrada.** Conviene tener un formato de registro que ayude en la medida de lo posible a posteriores lecturas y análisis.
* **Elección del mecanismo de registro.** Tendremos que elegir un sistema de gestión de *logs* apropiado a nuestra política. Posteriormente será necesario disponer y configurar las herramientas de monitorización y registro adecuadas para implantarlo.
* **Protección y almacenamiento.** Nos aseguraremos de que la información de registro esta convenientemente almacenada para protegerla de accesos indebidos. Es conveniente incorporar esta información a nuestros sistemas de copia de seguridad [[3]](#referencias) para poderla recuperar en caso de pérdida.
* **Sincronización del reloj.** Debemos asegurarnos de que todos nuestros sistemas están sincronizados correctamente, de este modo garantizaremos el correcto registro temporal de los eventos más relevantes.
* **Sistemas de monitorización y alerta.** Paralelamente al registro de los eventos más significativos, utilizaremos los sistemas de monitorización para que nos alerten en tiempo real de posibles errores y comportamientos anómalos, tales como:
  + proximidad de alcanzar los límites en la utilización de los recursos físicos hardware;
  + finalización o comportamientos anómalos de programas;
  + comportamientos anómalos en la red;
  + cambios en configuraciones críticas;
  + picos de rendimiento anómalos en los sistemas y redes.

# Referencias

1. Incibe – Protege tu empresa – Blog – La gestión de eventos de seguridad: un diamante por pulir <https://www.incibe.es/protege-tu-empresa/blog/post-gestion-eventos>
2. Incibe – Protege tu empresa – Blog – Diez señales de compromiso en los sistemas informáticos de su empresa <https://www.incibe.es/protege-tu-empresa/blog/diez-senales-de-compromiso-en-los-sistemas-informaticos-de-su-empresa>
3. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Copias de seguridad <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
4. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Antimalware [https://www.incibe.es/protege-tu-empresa/herramientas/politicas](https://www.incibe.es/protege-tu-empresa/que-te-interesa)
5. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Respuesta a incidentes <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
6. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Protección de la página web <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
7. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Auditoría de sistemas <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>

