POLÍTICA DE REGISTRO DE INICIO DE SESIÓN

Sistema de Gestión de Seguridad de la Información
Secretaría de Educación Del Distrito

Vigencia 2025
Versión: 1.0

Tabla de Contenido

GLOSARIO

Registro de inicio de sesión (Log): Conjunto de datos que evidencian los accesos a un activo de información.

SIEM: Sistema de gestión de eventos e información de seguridad, utilizado para la centralización, correlación y monitoreo de logs.

Criticidad del activo: Nivel de importancia de un activo tecnológico para la operación de la organización (Alto, Medio o Bajo).

1. OBJETIVO

La presente política tiene como finalidad establecer los lineamientos para el registro, almacenamiento y revisión de los inicios de sesión en los activos de información de la organización, garantizando la trazabilidad, detección temprana de incidentes de seguridad y cumplimiento de la **ISO/IEC 27001:2022, control 8.15 "Registro de eventos"**.

2. ALCANCE

Esta política aplica a todos los activos tecnológicos, sistemas de información, aplicaciones y servicios que requieran autenticación de usuarios, clasificados con criticidad **Alta, Media o Baja** en la **Matriz de Clasificación de Activos de Información** de la organización.

3. LINEAMIENTOS GENERALES

3.1. Registros de inicio y cierre de sesión.

Todos los activos tecnológicos que requieran autenticación deberán generar registros de inicio y cierre de sesión.

3.2. Requerimientos mínimos de los registros

Los registros deberán incluir, como mínimo, la siguiente información:

- Identidad del usuario (ID o credencial).
- Fecha y hora exacta del evento (sincronizada mediante NTP).
- Dirección IP o dispositivo origen.
- Resultado del intento de acceso (exitoso o fallido).
- Identificador del activo o sistema accedido.

3.3. Almacenamiento de registros.

Los registros deberán almacenarse en un repositorio seguro y con acceso restringido, preferiblemente centralizado en un SIEM.

3.4. Conservación

El tiempo de conservación de los registros se definirá en función del nivel de criticidad del activo, teniendo en cuenta las Tabla de Retención Documental (TRD) aprobada y definidas por la entidad[1].

3.5. Intentos de acceso fallidos

Todo intento de acceso fallido deberá registrarse y, dependiendo del nivel de criticidad, generar alertas automáticas al área de seguridad de la información, el tratamiento de dichas alertas será conforme a la política de atención a incidentes.

4. REQUERIMIENTOS SEGÚN NIVEL DE CRITICIDAD

4.1. Activos de Alta Criticidad

- Registrar todos los intentos de inicio de sesión (exitosos y fallidos).
- Registrar accesos fuera de horario laboral o desde ubicaciones no habituales.
- Generar alertas automáticas en tiempo real ante intentos fallidos consecutivos (≥3).
- Retención mínima de registros: **24 meses**.
- Integración obligatoria con el SIEM corporativo.

4.2. Activos de Media Criticidad

- Registrar intentos de inicio de sesión exitosos y fallidos.
- Generar alertas automáticas ante intentos fallidos consecutivos (≥5).
- Retención mínima de registros: **12 meses**.
- Se recomienda integración con el SIEM o repositorio seguro.

4.3. Activos de Baja Criticidad

- Registrar inicios de sesión exitosos y fallidos.

[1] https://www.educacionbogota.edu.co/portal_institucional/transparencia/tablas-de-retencion-documental

- No requiere generación automática de alertas, pero los registros deberán estar disponibles para revisión.

- Retención mínima de registros: **6 meses**.

5. RESPONSABILIDADES

- Usuarios:
  - Acceder únicamente con credenciales autorizadas.
  - Reportar accesos sospechosos o intentos de intrusión.
- Administradores de Sistemas:
  - Configurar los mecanismos de logging en cada activo conforme a esta política.
  - Garantizar la integridad y disponibilidad de los registros.
- Área de Seguridad de la Información / SOC:
  - Supervisar el cumplimiento de la política.
  - Analizar y dar respuesta a las alertas generadas.
  - Conservar y custodiar los registros en el tiempo definido.

6. MEJORA CONTINUA

6.1. Responsabilidades por Rol

Rol	Responsabilidades de mejora continua
Dueño del Activo	- Revisar periódicamente que las configuraciones de logging y control de accesos se mantengan vigentes. Asegurar que el activo esté clasificado y documentado en el inventario. - Aprobar excepciones y revisarlas al menos una vez al año.
Administrador del Activo	- Revisar que el envío de logs al SIEM sea continuo (monitoreo de “heartbeat” del agente). Probar periódicamente el registro de inicios de sesión exitosos y fallidos. Mantener las configuraciones documentadas (baselines).
Equipo de Seguridad / SOC	- Monitorear alertas y tendencias de accesos sospechosos. Ajustar reglas de correlación en SIEM según nuevos riesgos. Coordinar con administradores la investigación de incidentes. Realizar revisiones trimestrales de efectividad de controles.
Auditor Interno / Cumplimiento	- Verificar evidencias de logging y pruebas. Validar que se cumplen las retenciones de acuerdo con la política. Reportar hallazgos y oportunidades de mejora.

6.2. Ciclo de Mejora Continua (PDCA aplicado)

- Plan (Planear): definir métricas de cumplimiento (ej. % de activos con logging habilitado, % de cuentas con MFA).
- Do (Hacer): aplicar revisiones de roles, capacitaciones y actualizaciones de controles.
- Check (Verificar): ejecutar auditorías internas, pruebas de logging y revisión de alertas.
- Act (Actuar): implementar ajustes, mejorar reglas de SIEM, actualizar políticas de contraseñas.

7. BUENAS PRÁCTICAS DE CONSERVACIÓN Y CUIDADO DE CONTRASEÑAS

- Longitud y complejidad: mínimo 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos.
- Autenticación multifactor (MFA): habilitar en todos los sistemas de criticidad ALTA y recomendada en MEDIA.
- No reutilización: políticas de control que eviten reutilizar contraseñas anteriores.
- Gestores de contraseñas: uso corporativo de password managers aprobados.
- Prohibiciones: no compartir contraseñas por correo, chat, ni almacenarlas en texto plano.
- Rotación de credenciales privilegiadas: cada 90 días o tras cualquier evento sospechoso.
- Bloqueo de cuentas: tras 5 intentos fallidos consecutivos.
- Concienciación: capacitaciones semestrales sobre ciberseguridad y phishing.
- Revisión continua: aplicar recomendaciones actualizadas de NIST SP 800-63B y OWASP Authentication Cheat Sheet.

8. CUMPLIMIENTO Y AUDITORÍA

El incumplimiento de esta política se considerará una falta grave a la seguridad de la información y podrá derivar en sanciones disciplinarias y/o legales.

Esta política será objeto de revisión anual, o en caso de cambios significativos en los activos tecnológicos, en los requisitos legales o en la normativa ISO/IEC 27001 aplicable.

MILENA DEL PILAR SANDOVAL GOMEZ
Jefe Oficina de las Tecnologías de la Información y Las Comunicaciones

Elaboró: Juan Carlos Parra Moreno – Oficial Seguridad Informática

Reviso: Henry Alexander Moyan Montenegro – Oficial Seguridad de la Información

Reviso: Jasson Smit Castro León – Profesional Especializado OTIC

Reviso: Luz Dary Vargas Suarez – Profesional OTIC

Reviso: Álvaro Echeverry Salcedo – Contratista Especializado