# GOB-PT-012 Política de Monitoreo de la Seguridad V2

# TABLA DE CONTENIDO



# ÍNDICE DE TABLAS

# 1. OBJETIVO

Establecer las directrices para la implementación de monitoreo en las actividades realizadas bajo los sistemas de información, aplicaciones y servicios de red de la Concesión RUNT 2.0 teniendo en cuenta las buenas prácticas de la NTC ISO/IEC 27002:2022.

# 2. ALCANCE

El alcance de la presente política abarca los controles de la NTC ISO/IEC 27002:2022 pertinentes para el proceso de Monitoreo de seguridad para los sistemas de información, aplicaciones y redes de la Concesión RUNT 2.0.

# 3. DIRECTRICES DE LA POLITICA DE MONITOREO

.

**3.1.** La Concesión RUNT 2.0 como parte de la gestión de Monitoreo de Seguridad debe producir, almacenar, proteger y analizar registros que lleven trazabilidad de actividades, excepciones, fallas y otros eventos relevantes para el análisis de causas en incidentes de seguridad, así como una contención bajo análisis previos frente a posibles amenazas que puedan llegar a afectar negativamente a la entidad.

El proceso de monitoreo debe tener en cuenta dentro de sus directrices los siguientes aspectos:

- Se debe establecer la información base para los registros de los eventos de seguridad.
- Se deben Identificar los eventos de seguridad considerados para la generación registros.
- Se deben establecer controles de aseguramiento para los registros generados por los eventos de seguridad.
- Se debe asegurar la información de lo registros de eventos aplicando medidas de protección de la privacidad.

**3.2.** Se debe realizar el monitoreo constante a Las redes, los sistemas y las aplicaciones en búsqueda de comportamientos anómalos que permitan prevenir posibles incidentes de seguridad de la información.

**3.3.** La Concesión RUNT 2.0 debe establecer desde las buenas prácticas los mecanismos que proporcionen conciencia del entorno de amenazas de seguridad de la información que permitan a la entidad tomar las debidas medidas de mitigación.

**3.4.** Desde el área de Monitoreo, la concesión RUNT 2.0 debe establecer las medidas de prevención de fuga de información que deben ser aplicadas a los sistemas de información aplicaciones, redes, y cualquier dispositivo que procese, almacene o transmita información confidencial.

**3.5.** Se debe realizar el monitoreo constante de los recursos informáticos como son los sistemas de información, aplicaciones y servicios de red de la entidad, garantizando que las capacidades de almacenamiento, procesamiento y transmisión de estos cumplan con

los requisitos actuales y esperados por la entidad.

## 4. CONTROLES DE SEGURIDAD PARA EL MONITOREO

**4.1.** Desde el SOC se deben determinar las reglas para la recopilación de registros para las actividades realizadas bajo los sistemas y servicios de la entidad, estos deben estar alineados a las políticas de seguridad de la información específica para los registros de eventos.

**4.2.** Los registros de eventos desde monitoreo deben incluir:

- Identificación del usuario.
- Actividades del sistema.
- Fechas, horas y detalles de eventos relevantes (por ejemplo, inicio y cierre de sesión);
- Entidad del dispositivo, identificador del sistema y ubicación;
- Direcciones de red y protocolos.

**4.3.** Los eventos mínimos que deben ser tenidos en cuenta por el monitoreo de la operación para los sistemas y servicios son:

- Intentos de acceso al sistema exitosos y rechazados.
- Datos exitosos y rechazados y otros intentos de acceso a recursos.
- Cambios en la configuración del sistema.
- Uso de privilegios de niveles altos.
- Uso de programas de utilidad y aplicaciones.
- Los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes;
- Alarmas emitidas por el sistema de control de acceso;
- Activación y desactivación de sistemas de seguridad, como sistemas antivirus.
- Creación, modificación o supresión de identidades;
- Transacciones ejecutadas por los usuarios en las aplicaciones.

**4.4.** Los sistemas y servicios dispondrán de fuentes de tiempo sincronizadas que permitan la correlación de registros entre sistemas para el análisis, alertas o investigación de incidentes.

**4.5.** Se debe restringir la eliminación o desactivación de registros de eventos, incluso para los derechos con accesos privilegiados.

**4.6.** Los registros de eventos deben ser almacenados bajo espacios cifrados, bajo el control de accesos, permisos limitados (solo para creación y lectura) y bajo una responsabilidad

establecida desde la entidad bajo su Sistema de Gestión de Seguridad de la Información y/o regulaciones. Se recomienda que la entidad tenga en cuenta:

- Requisitos para la retención de información y/o requisitos para recopilación y conservación de evidencias de la entidad.
- Ante requerimientos de solicitudes de registros de actividades de los sistemas y servicios de la entidad, previo a su envió deben terne en cuenta las políticas y controles de enmascaramiento de datos.
- Deben tomarse las medidas adecuadas de protección de la privacidad de datos confidenciales o sensibles.

**4.7.** Los análisis de eventos deben realizarse teniendo en cuenta:

- Contar con un equipo de expertos con las habilidades necesarios para los análisis de eventos.
- Establecer un procedimiento de análisis de registros de eventos correlacionados de seguridad;
- Establecer atributos requeridos para cada evento de seguridad.
- Identificar las reglas de excepciones, por ejemplo, la gestión de eventos e información de seguridad (SIEM) o reglas de cortafuegos, IDS o firmas de malware.
- Comportamientos conocidos de trafico de red estándar en comparación con comportamientos anómalos.
- Resultados del análisis de tendencias o patrones como por ejemplo resultados de análisis de datos y herramientas de análisis especializadas.
- La inteligencia de amenazas como herramienta de prevención para ciberataques, así como detectar y responder ante incidentes en curso

**4.8.** Los análisis de registros deben estar respaldados por actividades de monitoreo y deben tener en cuenta para identificar y analizar comportamientos anómalos, los siguientes aspectos:

- Revisar los intentos exitosos y fallidos de acceso a los recursos protegidos como lo son: Servidores DNS, portales web y recursos compartidos.
- Verificar los registros DNS para identificar conexiones de red salientes a servidores maliciosos.
- Tener en cuenta los informes de los proveedores de servicios en busca de actividades inusuales dentro de los sistemas o redes de la entidad.
- correlación de registros para un análisis más eficiente y preciso.

**4.9.** El área de Monitoreo debe realizar constante seguimiento a:

- Trafico de red entrante y saliente de los sistemas de información y aplicaciones de la Concesión RUNT 2.0.
- Acceso a sistemas, servidores, equipos de red, sistemas de monitoreo, aplicaciones críticas y otras.
- Registros de herramientas de seguridad [por ejemplo, antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, cortafuegos, prevención de fuga de datos];
- Registros de eventos relacionados con la actividad del sistema y de la red;
- Comprobar que el código que se ejecuta está autorizado para ejecutarse en el sistema y que no ha sido alterado (p. ej., mediante recompilación para agregar código adicional no deseado);

- Uso de los recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su rendimiento.

**4.10.** Frente a las anomalías. Desde el área de Monitoreo se debe considerar lo siguiente:

- Monitorear la utilización de los sistemas de información, aplicaciones y redes en horarios normales y de alto volumen de trabajos.
- Establecer una línea de referencia de comportamiento de los accesos, sitio de acceso y otras características que permitan identificar comportamientos anómalos.

**4.11.** Con el fin de tener una línea base de comportamientos y de referencia para detección de variaciones de uso de los sistemas y servicios, se recomienda que el área de Monitoreo tenga en cuenta:

- Terminación no planificada de procesos o aplicaciones.
- Comportamientos asociados a Malware o tráfico que se origina en direcciones IP o dominios de red maliciosos (Botnet).
- Características de ataques conocidos como por ejemplo la denegación de servicios y otros.
- Sobrecargas en la red, cuellos de botellas de canales, y fluctuaciones en el tráfico de red.
- Escaneo de red con aplicaciones comerciales no autorizados.
- Comportamientos contrarios e inusuales de los usuarios frente a los comportamientos esperados.

**4.12.** Los procesos de monitoreo de la Concesión RUNT 2.0 deben ser realizados de manera continua, en tiempo real o en intervalos periódicos sujetos a las necesidades de la entidad y deben adaptarse a un panorama de amenazas en constante cambio y permitir notificaciones en tiempo real a través de consolas, mensajes de correo electrónico o sistemas de mensajería instantánea.

**4.13.** La Concesión RUNT 2.0 tendrá en cuenta el panorama delictivo frente a la Seguridad de la Información y la Ciberseguridad, incluyendo aquellas amenazas conocidas que se encuentren en constante cambio. Con estas, se debe realizar una estrategia para anticipar de riesgos del entorno y minimizar los posibles incidentes que puedan impactar negativamente la prestación del servicio de la entidad.

**4.14.** Como estrategia de anticipación del riesgo se tendrá en cuenta el modelo de capas las cuales serán un apoyo para cada uno de los niveles organizacionales en la toma de decisión y prevención, estas son:

- inteligencia de amenazas estratégicas: intercambio de información de alto nivel sobre el cambiante panorama de amenazas (por ejemplo, tipos de atacantes o tipos de ataques);
- inteligencia de amenazas tácticas: información sobre las metodologías, herramientas y tecnologías involucradas del atacante;
- inteligencia de amenazas operativas: detalles sobre ataques específicos, incluidos indicadores técnicos.

**4.15.** Con el fin de evitar la fuga de información se debe:

- Tener en cuenta la clasificación de la información de la entidad.
- Establecer reglas de Monitoreo para los servicios de correo electrónico, transferencia de archivos, dispositivos móviles, dispositivos de almacenamiento portátiles, uso de servicios en línea de transferencia no autorizados.
- Establecer reglas de control para los niveles de confidencialidad de los correos de la entidad y limitantes de acciones para estos (por ej. Accesos sin restricciones, no permitir su reenvió, no responder a todos).

**4.16.** La organización establece herramientas para la prevención de la fuga de información que deben utilizarse para:

- Identificar y monitorear información sensible en riesgo de divulgación no autorizada.
- Detectar la divulgación de información confidencial sin autorización bajo servicios en la nube de terceros no autorizados o por envíos mediante correos electrónicos.
- Bloquear acciones de los usuarios o transmisiones de la red que expongan información confidencial.

**4.17.** La Concesión RUNT 2.0 debe establecer (en caso de requerirse) restricciones para las acciones copiar, pegar, cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la entidad.

**4.18.** La operación tecnológica debe realizar el aseguramiento de los recursos garantizando que las capacidades de estos cumplan con los requerimientos actuales y esperados por la entidad en aspectos como procesamiento, transmisión, canales WAN y otros; también se deben establecer proyecciones de crecimiento para los niveles de almacenamiento (BD, repositorios y otros) supliendo las necesidades actuales y posteriores de la entidad.

El aseguramiento de los recursos de la concesión RUNT 2.0 debe tener en cuenta:

- La supervisión de las capacidades actuales y ajustes necesarios de las capacidades de las tecnologías garantizando su disponibilidad y eficiencia dentro de la entidad.
- Realizar pruebas de estrés programas (planeación) y garantizando la no afectación de los servicios a los sistemas y servicios de la entidad.
- Establecer reglas de detección que permitan identificar futuras eventualidades negativas de la capacidad de los sistemas y servicios.
- Las proyecciones deben tener en cuenta los nuevos requisitos del negocio para la capacidad de procesamiento de información de la entidad.
- La información de capacidad de los sistemas y servicios debe ser tenido en cuenta por los Gerente, responsables de área, líderes y otros cargos estratégicos para evitar posibles limitaciones de recursos que puedan representar una amenaza para la seguridad de los sistemas o los servicios.

**4.19.** Como buenas prácticas, la operación tecnológica de la concesión RUNT 2.0 debe considera lo siguiente:

- Eliminación de datos obsoletos (Liberar espacio en disco).
- Optimizar los procesos por lotes y tareas programadas.

- Los desarrollos internos deben optimizar los códigos de las aplicaciones y consultas a bases de datos.
- Control de priorización de tráfico para el ancho de banda de la entidad para los servicios que no son críticos.
- Establecer y documentar un plan de gestión de capacidad para los sistemas o servicios críticos.

## 5. CONTROL DE CAMBIOS

| 1. Control de cambios | | | | | |
|---|---|---|---|---|---|
| **Versión** | **Elaboró** | **Revisó** | **Aprobó** | **Fecha** | **Descripción** |
| 1 | IT Managers | Jefe de seguridad de la Información | Líder dominio de seguridad | 11/04/2023 | Creación del documento |
| 2 | Analista de seguridad de la información | Jefe de seguridad de la Información | Jefe de seguridad de la Información | 19-04-2024 | Se ajusta clasificación de la informacion |

*Tabla 1. Control de cambios*