



IT-OPE-004 Resguardo de bitácoras

Responsables

Elaboró:	Analista de Monitoreo
Revisó:	Control de Documentos
Aprobó:	Gerente de Operaciones

Control de versiones

Versión	Fecha	Descripción del cambio
1	06/05/2021	Emisión inicial
2	06/05/2022	Revisión Anual
3	15/10/2022	Actualización y revisión general del documento.

Clave del formato de instructivo: F-SGI-003 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Objetivo.....	3
2. Alcance	3
3. Definiciones.....	3
4. Descripción del instructivo.....	3
4.1 Nombre y tipos de logs	3
4.2 Ubicación.....	5
4.3 Respaldo.....	6
4.4. Depuración	6
4.5. Seguridad	6
5. Anexos.....	7

1. Objetivo

Este documento tiene como objetivo describir las actividades a llevar a cabo para el resguardo de bitácoras, para asegurar su adecuada recolección y la protección de la información almacenada.

2. Alcance

El presente documento se limita a las actividades requeridas para realizar el resguardo de bitácoras, logs o eventos de los sistemas de correlación a través de equipos de almacenamiento de información de uso específico con los que cuenta Silent4Business.

3. Definiciones

- **Logs:** En informática, se usa el término registro, log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).
- **SCP:** Es un protocolo para sistemas informáticos, que garantiza la transferencia segura de datos entre un equipo local (host local) y un equipo remoto (host remoto) o, alternativamente, entre dos equipos remotos.
- **Bitacora:** Es un cuaderno en el cual estudiantes, diseñadores y artistas plásticos, entre otros, desarrollan sus bocetos, toman nota de recuerdos y cualquier información que consideren que puede resultar útil para su trabajo.

4. Descripción del instructivo

4.1 Nombre y tipos de logs











Todos los dispositivos que reporten bitácoras hacia los sistemas de correlación contendrán los siguientes datos por default:

Basic Information
Normal Date:
Last Normal Date:
Log Count:
Log Source Entity:
Log Source Host:
Log Source:
Log Source Type:





















Dependiendo del tipo de información que contengan las bitácoras podrán contener datos en forma de campos para la mejor interpretación y correcto análisis, algunos de los campos disponibles son:

Entity (Origin)
Entity (Impacted)
Location (Origin)
Network (Origin)
Network (Impacted)
Known Host (Origin)
IP Address (Origin)
Hostname (Origin)
Known Host (Impacted)
IP Address (Impacted)
Hostname (Impacted)
Known Application
TCP/UDP Port (Origin)
TCP/UDP Port (Impacted)
Protocol
Process Name
Process ID
Severity

Todas las bitácoras se almacenan en el formato del sistema de correlación, el nombre de los archivos a resguardar son del tipo LCA, identificado por fecha y ID asignado por el sistema de correlación.

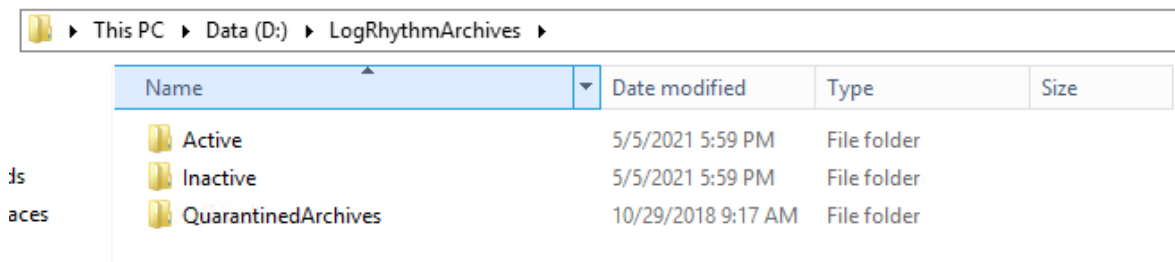
Name	Date modified	Type	Size
 20200506_115_33_1_637455475873008523.lca	1/13/2021 11:27 AM	LCA File	8 KB
 20200506_118_34_1_637455474698294768.lca	1/13/2021 11:27 AM	LCA File	6 KB
 20200506_130_38_1_637455494472543573.lca	1/13/2021 11:27 AM	LCA File	9 KB
 20200506_168_2_1_637455618732438371.lca	1/13/2021 3:27 PM	LCA File	78 KB
 20200506_169_2_1_637455486050551237.lca	1/13/2021 11:27 AM	LCA File	7 KB
 20200506_172_42_1_637455487427068434.lca	1/13/2021 11:27 AM	LCA File	4 KB
 20200506_188_45_1_637455481456673313.lca	1/13/2021 11:27 AM	LCA File	7 KB
 20200506_190_45_1_637455509933759288.lca	1/13/2021 12:27 PM	LCA File	8 KB
 20200506_191_46_1_637455483042330035.lca	1/13/2021 11:27 AM	LCA File	6 KB
 20200506_193_46_1_637455487631972764.lca	1/13/2021 11:27 AM	LCA File	8 KB

Estos archivos se encuentran organizados en carpetas por día, con la nomenclatura fecha+ID

	20210422_1_637546284383812857	4/30/2021 10:41 AM	File folder
	20210421_1_637545420446440351	4/29/2021 2:20 PM	File folder
	20210420_1_637544557436980188	4/29/2021 11:38 AM	File folder
	20210419_1_637544292099584663	4/27/2021 3:23 AM	File folder
	20210418_1_637542828763590968	4/26/2021 6:22 PM	File folder
	20210417_1_637541964436651767	4/25/2021 12:21 AM	File folder
	20210416_1_637541121382159058	4/23/2021 11:20 PM	File folder
	20210415_1_637540236413166867	4/22/2021 11:18 PM	File folder
	20210414_1_637539382972451203	4/21/2021 10:38 PM	File folder
	20210413_1_637538519370377615	4/20/2021 8:36 PM	File folder
	20210412_1_637537652908089157	4/19/2021 9:43 PM	File folder
	20210411_1_637536791581135732	4/18/2021 9:14 PM	File folder
	20210410_1_637535926519913277	4/17/2021 9:13 PM	File folder
	20210409_1_637535673371660724	4/16/2021 11:11 PM	File folder
	20210408_1_637534507765548157	4/16/2021 4:11 PM	File folder
	20210407_1_637534035444649241	4/16/2021 2:11 PM	File folder
	20210406_1_637532607483091463	4/16/2021 1:10 PM	File folder
	20210405_1_637531627326131693	4/13/2021 5:43 PM	File folder
	20210404_1_637530772728154069	4/12/2021 3:43 AM	File folder
	20210403_1_637529878084537847	4/11/2021 8:42 PM	File folder

4.2 Ubicación

Las bitácoras del sistema de correlación se mantienen con los parametros por default y se encuentran ubicadas en la ruta:



La ubicación física de los sistemas de correlación y almacenamiento se encuentran en un Site con las siguientes

sgi@silent4business.com



Insurgentes Sur #2453, Piso 4, Col, Tizapán San Ángel, Álvaro Obregón, 01090 Ciudad de México, CDMX

"La información contenida en este documento es propiedad intelectual de SILENT4BUSINESS SA DE CV, por lo que queda estrictamente prohibida su reproducción, modificación, divulgación, uso o aprovechamiento por cualquier medio impreso, mecánico o electrónico sin la autorización previa por escrito de Silent4Business."

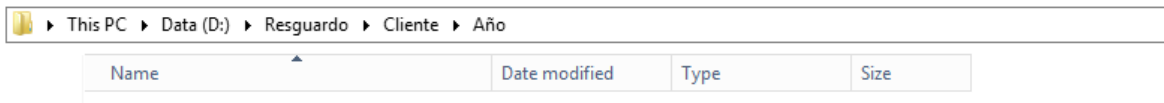


características:

- Site de comunicaciones dedicado
- Sistema de aire acondicionado
- Sistema contra incendios
- Acceso biométrico
- UPS
- Planta de emergencia
- Sistema de videovigilancia

4.3 Respaldo

Las bitácoras se respaldan en los equipos de almacenamiento de bitácoras de uso específico con los que cuenta Silent4Business en la siguiente ruta:



Los respaldos se realizan de manera manual de forma semanal y se realizan mediante protocolo SCP (Secure Copy Protocol) por el puerto 22.

4.4. Depuración

Las bitácoras en los sistemas de correlación se mantienen durante 12 meses, así como su resguardo en los sistemas de almacenamiento, esto garantiza su consulta y posterior análisis.

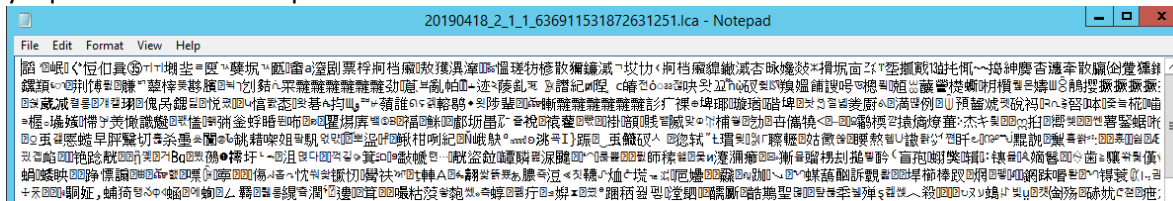
El tiempo de retención puede variar en casos específicos donde esta información se requiera retener por un periodo mayor y este considerado en el alcance del servicio con nuestros clientes.

4.5. Seguridad

Las bitácoras presentan las siguientes características:

- Formato nativo
- Compresión de archivos
- Validación de integridad

Las anteriores características garantizan que la información contenida no pueda ser visualizada en texto plano ya que el formato no lo permite



Los sistemas de correlación y almacenamiento cuentan con los siguientes controles de seguridad:

- Control de accesos de usuarios por Directorio Activo
- Acceso por roles
- Segregación de redes
- Protección por sistemas de Firewall de red

sgi@silent4business.com



Insurgentes Sur #2453, Piso 4, Col, Tizapán San Ángel, Álvaro Obregón, 01090 Ciudad de México, CDMX

"La información contenida en este documento es propiedad intelectual de SILENT4BUSINESS SA DE CV, por lo que queda estrictamente prohibida su reproducción, modificación, divulgación, uso o aprovechamiento por cualquier medio impreso, mecánico o electrónico sin la autorización previa por escrito de Silent4Business."



- Sistema de prevención de intrusos
- Sistema de archivos de sistema operativo Cifrado
- Arreglos de discos de almacenamiento con tolerancia a fallos (Raid1,Raid5)
- Sin exposición a internet ni a redes no autorizadas

5. Anexos

No aplica.