



OEA | CICTE



CSIRT Americas
Network

Manual Técnico de **MISP**

Facilitando el intercambio de información
en comunidades de ciberseguridad



UK Government

Índice

1. Modelo documental.....	10
1.1. Introducción	11
1.2. Organización de este documento.....	12
1.3. Consideraciones para el manual.....	12
1.4. Consideraciones para Entornos de Producción	13
2. Fundamentos y Usos de MISP.....	14
2.1. Introducción	15
2.1.1. Indicadores de compromiso (IOCs).....	15
2.1.2. Inteligencia de Amenazas	15
2.1.3. Plataforma de Inteligencia de Amenazas	15
2.2. ¿Qué es MISP?.....	16
2.3. ¿Por qué MISP?	16
2.4. ¿A quién va dirigido MISP?	18
2.5. Beneficios de Compartir Información de Inteligencia de Amenazas	19
2.6. Casos Prácticos de MISP.....	19
2.6.1. Red Nacional de SOC	20
2.6.2. MISP del CSIRT-CL	20
2.6.3. CSIRT Americas	21
3. Instalación Básica de MISP	22
3.1. Dimensionamiento y preparación del servidor para la instalación de MISP	23
3.2. Instalación de MISP	24
3.2.1. Instalación en Sistema Operativo Linux	24
3.3. Docker en MISP	25
3.4. Iniciar Sesión	26
3.5. Errores comunes en la instalación.....	27
3.5.1. Revisión de registros de errores con el instalador oficial de MISP	28

3.6.	Cambio de base de datos de MySQL a PostgreSQL	30
4.	Configuración Inicial, Personalización de la Instancia de MISP y Gestión de Taxonomías	31
4.1.	Configuración de la MISP.baseurl	32
4.1.1.	Pasos para configurar la BaseURL:	32
4.2.	Personalización de la Instancia MISP	33
4.3.	Taxonomías	37
4.3.1.	Taxonomías en MISP	39
4.3.2.	Agregar la taxonomía de CSIRT Americas a tu instancia MISP	39
4.3.3.	Agregar una Etiqueta a tu instancia MISP	41
5.	Creación de eventos en MISP	45
5.1.	Introducción	46
5.1.1.	Evento en MISP	46
5.1.2.	Atributos del Evento	46
5.1.3.	Organización	46
5.2.	Alcance de distribución de eventos	46
5.3.	Creación de eventos en MISP	47
5.3.1.	Añadir etiquetas al evento	49
5.3.2.	Agregar atributos al evento	50
5.3.3.	Publicar el evento	52
5.4.	Enriquecimiento de eventos	53
6.	Gestión de Usuarios y Organizaciones MISP	55
6.1.	Introducción	56
6.1.1.	Usuario	56
6.1.2.	Instancia de MISP	56
6.1.3.	Sincronización	56
6.1.4.	Administrador en MISP	56
6.2.	Gestión de usuarios	56
6.2.1.	Cómo añadir un nuevo usuario	57
6.2.2.	Cómo añadir un nuevo usuario	60

6.2.3.	Contactar a un usuario.....	62
6.3.	Gestión de usuarios	64
6.3.1.	Contactar a un usuario.....	64
6.3.2.	Cómo listar roles.....	67
6.4.	Gestión de organizaciones	69
6.4.1.	Cómo añadir una nueva organización	69
6.4.2.	Cómo listar organizaciones	71
7.	Sincronización de instancias.....	74
7.1.	Introducción	75
7.1.1.	Servidor de Sincronización	75
7.1.2.	Grupos de intercambio (Sharing Groups)	75
7.1.3.	Authkey (Clave de autenticación)	75
7.2.	Sincronización entre dos instancias de MISP.....	75
7.2.1.	Crear una organización local.....	76
7.2.2.	Crear un usuario de sincronización (Sync User)	78
7.2.3.	Crear la llave de autenticación	81
7.2.4.	Recopilar y enviar la información.....	87
7.2.5.	Configurar el servidor de sincronización en la Instancia País A	89
7.2.6.	Verificación de la Sincronización	93
7.3.	Modelos de Intercambio de información	94
7.3.1.	Solo tu organización (Your organisation only).....	94
7.3.2.	Solo tu comunidad (This community only)	95
7.3.3.	Comunidades conectadas (Connected communities).....	95
7.3.4.	Todas las comunidades (All communities).....	96
8.	Anexo 1 – Hardening Básico.....	98
8.1.	Introducción	99
8.1.1.	Hardening	99
8.1.2.	Backup (Respaldo)	99
8.2.	Actualización del sistema operativo	99
8.3.	Copias de seguridad y actualizaciones en MISP	100

8.3.1.	Backup (Respaldo)	100
8.3.2.	Actualizaciones de MISP	101
8.4.	Configurar el firewall.....	103
8.5.	Cifrado de Datos	104
8.5.1.	Uso de HTTPS	104
8.6.	Políticas de Seguridad	105
8.6.1.	Autenticación multifactor (MFA)	105
8.6.2.	Política de contraseñas.....	109
8.6.3.	Restringir el acceso SSH	109
8.7.	Hardening del Sistema Operativo.....	110
8.7.1.	Utilizar CIS Benchmarks	110

Índice de Figuras

Figura 1. Intercambio de Información en MISP	16
Figura 2. Visualización de Atributos Compartidos en MISP.....	17
Figura 3. Proceso de Instalación de MISP en Linux.	24
Figura 4. Pantalla de inicio de sesión en MISP.	27
Figura 5. Configuración de Permisos en MariaDB para MISP.....	29
Figura 6. Configuración del Archivo database.php en MISP.	30
Figura 7. Acceso a Server Settings & Maintenance en MISP.....	32
Figura 8. Configuración de MISP.baseurl y MISP.external_baseurl.	33
Figura 9. Acceso a Manage Files en MISP.	34
Figura 10. Carga de Imágenes en Additional Image Files de MISP.	34
Figura 11. Logotipos en Pantallas de Inicio y Bienvenida en MISP.	35
Figura 12. Textos de Bienvenida en la Pantalla de Inicio de MISP.	36
Figura 13. Ejemplo de Personalización Final en MISP.....	36
Figura 14. Elementos Visuales en la Interfaz de MISP.....	37
Figura 15. Taxonomía CSIRT Americas.....	38
Figura 16. Acceso a la Lista de Taxonomías en MISP.	40
Figura 17. Habilitación de Taxonomías en MISP.....	40
Figura 18. Confirmación de Etiquetas Habilitadas.	41
Figura 19. Confirmación de Etiquetas Habilitadas.	41
Figura 20. Acceso a la Opción Add Tag en MISP.....	42
Figura 21. Formulario de Configuración de Etiquetas en MISP.....	43
Figura 22. Selección de Color para Etiquetas en MISP.	44
Figura 23. Creación de eventos en MISP.....	47
Figura 24. Formulario de creación de eventos en MISP.	48
Figura 25. Detalles del evento en MISP.....	48

Figura 26. Añadir etiquetas al evento en MISP.	49
Figura 27. Detalles del evento con etiquetas en MISP.	50
Figura 28. Agregar atributos al evento en MISP.	50
Figura 29. Menú para agregar atributos al evento en MISP.	51
Figura 30. Formulario para agregar atributos al evento en MISP.	51
Figura 31. Opciones para publicar eventos en MISP.	52
Figura 32. Confirmación para publicar evento en MISP.	52
Figura 33. Enriquecimiento de eventos en MISP.	53
Figura 34. Importación de atributos con texto libre en MISP.	53
Figura 35. Herramienta de importación de texto libre en MISP.	54
Figura 36. Resultados de importación de texto libre en MISP.	54
Figura 37. Menú para añadir un nuevo usuario en MISP.	57
Figura 38. Formulario de administración para añadir usuarios en MISP.	59
Figura 39. Listado de usuarios existentes en MISP.	60
Figura 40. Opciones de acción para usuarios en MISP.	61
Figura 41. Función para contactar usuarios en MISP.	62
Figura 42. Formulario para contactar usuarios en MISP.	63
Figura 43. Formulario para añadir roles en MISP.	65
Figura 44. Listado de roles en MISP.	68
Figura 45. Menú para añadir una nueva organización en MISP.	69
Figura 46. Formulario para añadir una nueva organización en MISP.	70
Figura 47. Menú para listar organizaciones en MISP.	71
Figura 48. Opciones para filtrar organizaciones en MISP.	72
Figura 49. Opciones de acciones para organizaciones en MISP.	73
Figura 50. Sincronización entre dos instancias de MISP.	76
Figura 51. Menú para añadir una nueva organización en MISP.	76
Figura 52. Formulario para crear una organización local en MISP.	77
Figura 53. Proceso de creación de una organización local en MISP.	78
Figura 54. Menú para crear un usuario de sincronización en MISP.	79
Figura 55. Usuario de sincronización entre nodos en MISP.	79

Figura 56. Formulario para crear un usuario de sincronización en MISP.	80
Figura 57. Acceso al listado de usuarios en MISP.....	81
Figura 58. Usuario de sincronización en el listado de usuarios en MISP.	81
Figura 59. Opciones de acciones para usuarios en MISP.....	81
Figura 60. Perfil del usuario de sincronización en MISP.	82
Figura 61. Gestión de claves de autenticación en MISP.....	83
Figura 62. Configuración de claves de autenticación en MISP.	83
Figura 63. Confirmación de clave de autenticación en MISP.	84
Figura 64. Perfil de usuario Sync User en MISP.	84
Figura 65. Acceso a My Profile en MISP.	84
Figura 66. Perfil de usuario en MISP.	85
Figura 67. Gestión de claves de autenticación en MISP.....	86
Figura 68. Ventana para agregar clave de autenticación en MISP.....	86
Figura 69. Clave de autenticación creada en MISP.....	87
Figura 70. Vista general de la organización local	88
Figura 71. Vista general del JSON Sync User	88
Figura 72. Configuración del servidor de sincronización en MISP.	89
Figura 73. Acceso a Remote Servers en MISP.	89
Figura 74. Selección de New Server en MISP.	90
Figura 75. Configuración de servidor en MISP.....	91
Figura 76. Lista de servidores en MISP	92
Figura 77. Resultados de prueba de conexión en MISP.	93
Figura 78. Modelo de intercambio "Solo tu organización" en MISP.....	94
Figura 79. Modelo de intercambio "Solo tu comunidad" en MISP.....	95
Figura 80. Modelo de intercambio "Comunidades conectadas" en MISP.	96
Figura 81. Modelo de intercambio "Todas las comunidades" en MISP.....	97
Figura 82. Acceso a Server Settings & Maintenance.	102
Figura 83. Sección Diagnostic en Server Settings & Maintenance.....	102
Figura 84. Opciones de Actualización en Diagnostic.	102
Figura 85. Confirmación para Actualizar MISP.....	103

Figura 86. Acceso a la Configuración de Usuario en MISP.	105
Figura 87. Habilitación de TOTP en el Perfil de Usuario.	105
Figura 88. Generación de Código QR para TOTP.	106
Figura 89. Validación del Código TOTP.	107
Figura 90. Códigos de Respaldo de TOTP.	108
Figura 91. Solicitud de TOTP al Iniciar Sesión.	108
Figura 92. Guía de CIS Benchmarks para Ubuntu 24.04 LTS.	111

**MODELO
DOCUMENTAL
MISP**

1.1. Introducción

[CSIRTAmericas](#)¹ es la red de Equipos de Respuesta ante Incidentes Cibernéticos (CSIRT²) gubernamentales de los Estados Miembros de la Organización de los Estados Americanos (OEA). Actúa como el impulsor principal de la Sección de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE³) de la OEA en el fortalecimiento de las capacidades de respuestas ante incidentes cibernéticos de la región, promoviendo la cooperación y el intercambio efectivo de información entre los CSIRTs de la región, facilitando respuestas más rápidas y coordinadas frente a los incidentes cibernéticos.

La Red CSIRTAmericas destaca la necesidad de implementar acciones coordinadas en la respuesta a incidentes de ciberseguridad en la región de las Américas, con el objetivo de mejorar la capacidad de reacción de los CSIRTs y minimizar el impacto de las amenazas que trascienden fronteras y sectores. En este sentido, los CSIRTs desempeñan un rol fundamental en la gestión e intercambio de información sobre de amenazas cibernéticas, encargándose de recibir, analizar y recopilar información clave.

Sin embargo, los CSIRTs enfrentan importantes desafíos para el intercambio de información sobre ciberseguridad, tales como: la falta de homogenización en la categorización y formatos de incidentes; la duplicidad de información recibida de diversas fuentes de datos; el manejo de grandes volúmenes de información; así como la ausencia de procedimientos efectivos en el intercambio de conocimiento. Frente a estos retos, fortalecer la cooperación y fomentar el intercambio de información sobre amenazas cibernéticas se ha convertido en una prioridad estratégica. Para lograrlo, es fundamental la implementación de sistemas que faciliten la comunicación, particularmente para los equipos de seguridad que enfrentan recursos humanos limitados y restricciones financieras.

En este contexto, MISP⁴ (Malware Information Sharing Platform & Threat Sharing) puede ser considerada como una herramienta clave para la región, por ser un proyecto que facilita el intercambio estructurado, seguro y automatizado de indicadores de ciberseguridad y de información sobre amenazas. Este proyecto cofinanciado por CSIRT.lu y la Unión Europea es de código abierto, lo que asegura su uso a lo largo del tiempo sin necesidad de grandes inversiones de recursos, además de ser una herramienta empleada a nivel global, que ha

¹ Iniciativa de la OEA que fortalece la cooperación entre CSIRTs gubernamentales en América, promoviendo el intercambio de información sobre ciberseguridad. Más información: <https://csirtamericas.org/>

² Equipo encargado de gestionar y responder a incidentes de seguridad cibernética en una organización, sector o país.

³ Órgano de la OEA que coordina esfuerzos contra el terrorismo, incluyendo la ciberseguridad, a través de iniciativas y cooperación entre Estados Miembros.

⁴ Malware Information Sharing Platform, una plataforma de código abierto para compartir información sobre amenazas de ciberseguridad. Más información: <https://www.misp-project.org>

demostrado su efectividad al ser utilizadas por diversas comunidades operativas multisectoriales, como las comunidades MISP de CSIRTAmericas, FIRST⁵, OTAN, CIRCL⁶ y múltiples X-ISACs.

A pesar de que esta herramienta es altamente conocida en la región, existen limitaciones para su implementación, como la dificultad para comprender la documentación oficial, el desconocimiento de sus capacidades y características clave, la incertidumbre sobre cómo configurarla de manera adecuada y la complejidad en su instalación. Ante estos desafíos, el equipo de CSIRTAmericas del CICTE de la OEA han desarrollado y puesto a disposición del público una serie de manuales prácticos, que se describen en las secciones posteriores.

1.2. Organización de este documento

Este documento está estructurado en varios apartados técnicos que cubren desde la instalación y configuración inicial de **MISP** hasta su mantenimiento, endurecimiento de seguridad y gestión de usuarios y eventos. Además, se incluyen secciones dedicadas a la personalización de la instancia y la conexión con otras instancias de **MISP**.

1. Instalación Básica de MISP.
2. Configuración Inicial, Personalización de la Instancia MISP y Gestión de Taxonomías.
3. Creación de Eventos en MISP.
4. Gestión de Usuarios y Organizaciones.
5. Conexión a Instancias de MISP.
6. Hardening Básico del Servidor MISP.

1.3. Consideraciones para el manual

Este manual se desarrolló utilizando un entorno específico con las siguientes configuraciones técnicas:

- **Sistema Operativo:** Ubuntu 24.04 LTS.
- **Versión de MISP:** 2.5
- **Entorno de instalación:** Incluye configuraciones locales y de Docker, con conexión a internet habilitada para la descarga de dependencias y la comunicación interorganizacional.

Es importante tener en cuenta que las capturas de pantalla, comandos y procedimientos descritos corresponden a las versiones y configuraciones disponibles al momento de la

⁵ Foro internacional que agrupa a equipos de respuesta a incidentes de seguridad (CSIRTs) para fomentar la cooperación y el intercambio de mejores prácticas. Más información: <https://www.first.org>.

⁶ Centro nacional de respuesta a incidentes de Luxemburgo, reconocido por su desarrollo y soporte a herramientas de seguridad como MISP. Más información: <https://www.circl.lu>.

elaboración de este manual. En caso de utilizar una versión más reciente o antigua, algunos detalles podrían variar.

1.4. Consideraciones para Entornos de Producción

Antes de implementar estas guías en un entorno de producción, es imprescindible validar los requisitos técnicos con el área de TI de su organización. Esto incluye:

- **Compatibilidad:** Verificar que el sistema operativo, las dependencias y las versiones de software sean compatibles con los sistemas existentes.
- **Espacio y Recursos:** Confirmar que los recursos de hardware (CPU, RAM, almacenamiento) sean adecuados para el uso planificado.
- **Versiones Actuales:** Consultar la [documentación oficial de MISP](#) para asegurarse de que las configuraciones sean compatibles con las versiones actuales.

Nota:

El manual está disponible para consulta y descarga a través del sitio web oficial de CSIRT Americas <https://csirtamericas.org/es/resources>.

FUNDAMENTOS
Y USOS DE
MISP

2.1. Introducción

En esta sección, presentamos conceptos clave que ayudarán a los usuarios a comprender los fundamentos y beneficios de MISP, así como los términos que se utilizarán a lo largo de este manual. Familiarizarse con estos términos facilitará la navegación y el entendimiento del contenido presentado.

2.1.1. Indicadores de compromiso (IOCs)

Los indicadores de compromiso son datos técnicos que evidencian actividades maliciosas o anomalías dentro de un sistema. Estos pueden incluir direcciones IP sospechosas, hashes de archivos maliciosos, dominios utilizados para ataques, o cualquier artefacto digital relacionado con una amenaza. En MISP, los IOCs se estructuran de manera uniforme y se comparten entre las organizaciones, facilitando su análisis, correlación y uso para fortalecer las estrategias de defensa contra ataques dirigidos.

Ejemplos:

- Direcciones IP maliciosas.
- Hashes de archivos infectados.
- URLs de phishing.

2.1.2. Inteligencia de Amenazas

La inteligencia de amenazas es información procesada que permite identificar, analizar y responder a las amenazas cibernéticas de manera efectiva. Incluye datos específicos sobre los actores maliciosos, sus tácticas, técnicas y procedimientos (TTPs⁷), así como los objetivos de los ataques. Este conocimiento ayuda a anticiparse a posibles riesgos, mejorar sus defensas y tomar decisiones informadas para prevenir o mitigar incidentes de seguridad.

2.1.3. Plataforma de Inteligencia de Amenazas

Una plataforma de inteligencia de amenazas es una herramienta diseñada para recopilar, organizar y compartir información sobre amenazas cibernéticas. MISP actúa como un repositorio centralizado que permite almacenar datos relacionados con amenazas de manera estructurada, lo que facilita la colaboración y el intercambio de información entre organizaciones. Esta plataforma no solo optimiza la detección y respuesta ante incidentes, sino que también fomenta la construcción de una red de conocimiento

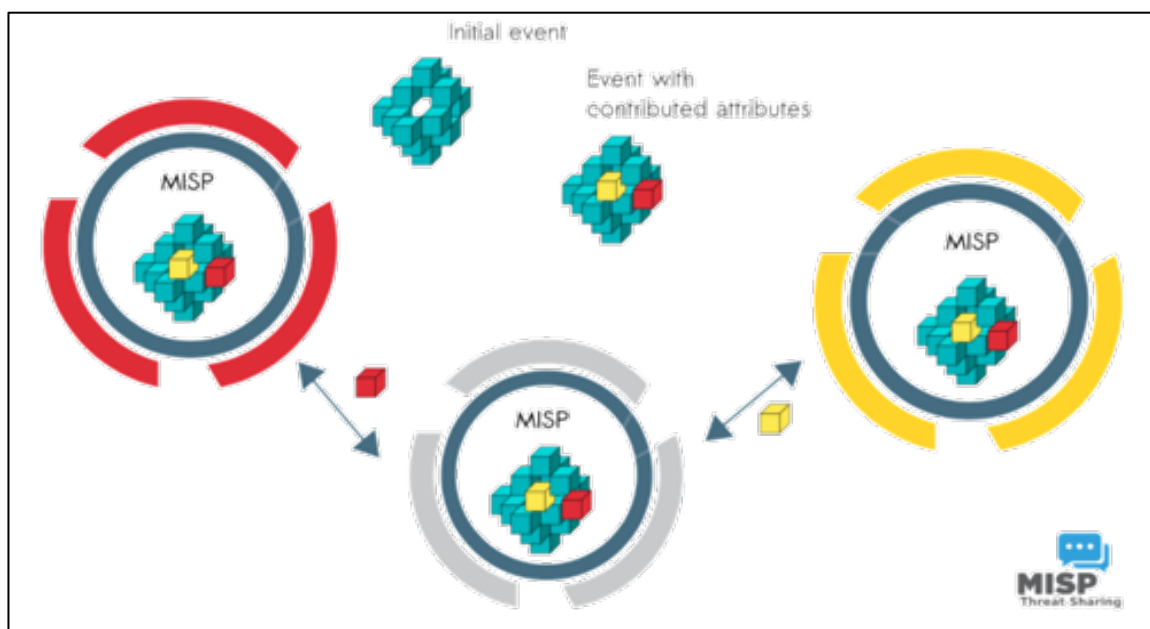
⁷ Tácticas, Técnicas y Procedimientos (TTPs) son los métodos utilizados por actores maliciosos para llevar a cabo ataques cibernéticos

colectivo, mejorando la capacidad de las organizaciones para enfrentar desafíos de seguridad comunes.

2.2. ¿Qué es MISP?

Malware Information Sharing Platform (MISP, por sus siglas en inglés) es un software de código abierto y gratuito diseñado para facilitar el intercambio, almacenamiento y análisis de información sobre inteligencia de amenazas. Esta plataforma permite a las organizaciones compartir datos estructurados relacionados con amenazas cibernéticas, incluidos los indicadores de compromiso (IoCs), información sobre actores maliciosos, vulnerabilidades y eventos de seguridad.

Figura 1. Intercambio de Información en MISP



Nota: Diagrama que ilustra el proceso de intercambio de información en MISP. Tomado de MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing (<https://www.misp-project.org>).

2.3. ¿Por qué MISP?

MISP es una plataforma fundamental para gestionar y compartir inteligencia sobre amenazas cibernéticas. Su estructura organizada y su enfoque colaborativo ofrecen múltiples beneficios, convirtiéndolo en una herramienta clave en la defensa contra las ciberamenazas. Es especialmente útil para equipos de Respuesta a Incidentes de Seguridad Informática (CSIRTs), Centros de Operaciones de Seguridad (SOC), unidades de ciberseguridad de

Fundamentos y Usos de MISP

organizaciones públicas y privadas, y otras entidades que necesiten recolectar, analizar y compartir información de amenazas. Más adelante, se detallarán los tipos específicos de usuarios que pueden aprovechar MISP.

Figura 2. Visualización de Atributos Compartidos en MISP.

2020-12-05	Object name: covid19-csse-daily-report ⓘ References: 0		
2020-12-05	Other	country-region: Mexico	text
2020-12-05	2020-12-05 Object name: covid19-csse-daily-report ⓘ References: 0		
2020-12-05	2020-12-05	Other	country-region: Bolivia text
2020-12-05	2020-12-05	2020-12-05 Object name: covid19-csse-daily-report ⓘ References: 0	
2020-12-05	2020-12-05	2020-12-05	Other country-region: China text
2020-12-05	2020-12-05	2020-12-05	Other update: 2020-12-05T05:27:36.000000 datetime
	2020-12-05	2020-12-05	Other confirmed: 93348 counter
	2020-12-05	2020-12-05	Other death: 4746 counter
		2020-12-05	Other recovered: 87204 counter
		2020-12-05	Other active: 1398 counter

Nota: Captura de pantalla realizada en la plataforma de MISP, mostrando un ejemplo de atributos y eventos compartidos.

Algunas de sus características más relevantes incluyen:

- **Código abierto y gratuito:** Al ser un software de código abierto, MISP no implica costos de licencia, lo que lo hace accesible para organizaciones de cualquier tamaño. Este modelo también fomenta la innovación, ya que una comunidad activa contribuye continuamente al desarrollo y mejora de la plataforma.
- **Colaboración comunitaria:** La comunidad de usuarios de MISP facilita el acceso a IoCs generados por otros. Estos indicadores ayudan a detectar, prevenir y mitigar incidentes de seguridad antes de que ocurran, mejorando la preparación y la respuesta ante amenazas.
- **Flexibilidad en su aplicación:** MISP puede ser utilizado para estructurar y compartir cualquier tipo de datos relevantes, como información sobre fraude financiero,

campañas de desinformación, etc., adaptándose a las necesidades específicas de cada organización.

- **Estructura consistente y eficiente:** Su modelo de datos organizado permite buscar, analizar y correlacionar eventos de manera eficiente. Esto mejora la capacidad de las organizaciones para identificar patrones de ataque y conectar eventos aparentemente aislados, fortaleciendo su postura de ciberseguridad.
- **Interoperabilidad entre organizaciones:** MISP promueve el intercambio seguro de información entre diferentes sectores, como gobiernos, instituciones financieras, empresas de telecomunicaciones y servicios públicos. Esto fortalece la colaboración interorganizacional frente a amenazas comunes.
- **Reducción del tiempo de respuesta:** Al contar con datos procesables y contextualizados, las organizaciones pueden reaccionar más rápidamente ante incidentes, minimizando su impacto y mejorando la eficiencia de sus equipos de seguridad.
- **Adaptación al panorama de amenazas:** En un entorno cibernético en constante evolución, MISP permite que las organizaciones se mantengan actualizadas sobre nuevas tácticas, técnicas y procedimientos (TTPs) de los atacantes, lo que refuerza su capacidad para anticiparse y adaptarse a las amenazas emergentes.

2.4. ¿A quién va dirigido MISP?

Existen muchos diferentes tipos de usuarios de plataformas de intercambio de información como MISP:

- **Analistas de Malware:** Comparten indicadores de compromiso (IoCs) con sus colegas para fortalecer los análisis y las defensas.
- **Analistas de Seguridad:** Buscan, validan y utilizan indicadores en operaciones de seguridad.
- **Analistas de Inteligencia:** Recopilan información detallada sobre grupos de adversarios y sus tácticas.
- **Fuerzas de Seguridad:** Utilizan indicadores para apoyar investigaciones y casos de análisis forense digital (DFIR).
- **Equipos de Análisis de Riesgos:** Evalúan nuevas amenazas, probabilidades de ocurrencia e impactos potenciales.
- **Analistas de Fraude:** Comparten y utilizan indicadores financieros para detectar y prevenir fraudes.
- **Equipos de Respuesta a Incidentes (CSIRTs):** Comparten información sobre incidentes y amenazas para coordinar respuestas efectivas.

- **Equipos de Ciberseguridad:** Colaboran en la identificación y mitigación de amenazas y vulnerabilidades.
- **Organizaciones Gubernamentales:** Fortalecen la seguridad nacional compartiendo inteligencia de amenazas entre agencias.
- **Empresas Privadas:** Proporcionan y consumen inteligencia de amenazas para proteger sus activos y operaciones críticas.

2.5. Beneficios de Compartir Información de Inteligencia de Amenazas

El intercambio de inteligencia de amenazas a través de MISP aporta múltiples ventajas:

- **Colaboración Eficiente:** Por ejemplo, la comunidad de CSIRT Americas utiliza MISP para intercambiar IoCs como direcciones IP maliciosas, dominios comprometidos, URL sospechosas, direcciones de correo que propagan contenido dañino entre sus CSIRTs miembros.
- **Automatización:** Facilita la integración de datos con herramientas de ciberseguridad para automatizar aspectos clave de las defensas, reduciendo el esfuerzo manual. Por ejemplo, al conectarse con plataformas como RTIR, o soluciones de SOAR⁸, los IoC compartidos en MISP pueden transformarse en alertas automáticas o aplicarse en sistemas como firewalls e IDS⁹.
- **Análisis Avanzado:** Proporciona un repositorio centralizado para registrar, organizar y analizar amenazas, agilizando la respuesta ante nuevos incidentes. Por ejemplo, se puede correlacionar varios eventos y descubre un patrón que apunta a un ataque coordinado, permitiendo ajustar las defensas de manera más estratégica.
- **Reducción de Riesgos:** Al compartir inteligencia, las organizaciones pueden anticiparse a posibles ataques y minimizar su impacto. Un ejemplo claro es cuando una organización detecta un ataque de ransomware y publica rápidamente los indicadores de compromiso en la plataforma. Esta información es utilizada por otras organizaciones que actualizan sus sistemas a tiempo para bloquear la amenaza antes de que pueda afectarlas.

2.6. Casos Prácticos de MISP

⁸ Security Orchestration, Automation, and Response (SOAR) es una tecnología que permite automatizar procesos de respuesta a incidentes de ciberseguridad.

⁹ Un Sistema de Detección de Intrusos (IDS) es una herramienta de ciberseguridad que monitorea la actividad de red en busca de posibles amenazas o anomalías.

A continuación, unos ejemplos de cómo se utiliza la herramienta:

2.6.1. Red Nacional de SOC¹⁰

La **Red Nacional de SOC** (RNS) de España es una iniciativa del CCN-CERT que integra a todos los Centros de Operaciones de Seguridad (SOC) del país, tanto públicos como privados. Su objetivo principal es mejorar la protección de sus miembros mediante el intercambio rápido y eficiente de información sobre **Indicadores de Ataques** (IOA) como los **Indicadores de Compromiso** (IOC), facilitando la detección y mitigación de actividades maliciosas en tiempo real.

¿Cómo comparten la información?

La RNS utiliza una infraestructura tecnológica que incluye instancias de MISP (Malware Information Sharing Platform) para el intercambio de información. Existen dos tipos de instancias:

- **MISP Intermedio o de Ingesta de datos:** Recibe todas las contribuciones de las entidades integrantes de la RNS.
- **MISP Final o de Difusión:** Difunde la información de la RNS, una vez ha sido valorada y procesada.

¿Qué información comparte?

- **Direcciones IP** de atacantes (o supuestos atacantes).
- **Dominios** de sitios comprometidos (o supuestamente comprometidos).
- **URL** específicas con contenido dañino.
- Firmas o **Hashes** de ficheros con contenido dañino.
- **Direcciones de correo** propagadoras de contenido dañino.
- **Reglas** de detección de amenazas, por comportamiento de red (reglas SNORT¹¹), por contenido dañino (reglas YARA¹²).
- Cabeceras específicas de navegación, como "**user-agent**" y otros.

2.6.2. MISP del CSIRT-CL¹³

El **CSIRT de Gobierno de Chile** ha implementado una instancia de MISP (Malware Information Sharing Platform) para facilitar el intercambio de información sobre ciberamenazas entre diversas organizaciones, tanto públicas como privadas.

¹⁰ Red Nacional de SOC. <https://rns.ccn-cert.cni.es/>

¹¹ Snort. <https://www.snort.org/>

¹² YARA. [Welcome to YARA's documentation! — yara 4.5.0 documentation](#)

¹³ CSIRT-CL. <https://csirt.gob.cl/servicios/intercambio-de-indicadores-de-compromiso/>

¿Cómo comparten la información?

El CSIRT ofrece dos métodos para acceder a esta información:

- **Conexión directa entre servidores MISP:** Las organizaciones con su propia instancia de MISP pueden sincronizarse con la del CSIRT, permitiendo un intercambio bidireccional de información en tiempo real.
- **API REST autenticada:** Para aquellas organizaciones que no disponen de un servidor MISP, el CSIRT ha desarrollado una API que permite acceder a los indicadores de compromiso de manera segura y estructurada.

2.6.3. CSIRTAmericas¹⁴

El **MISP Regional de CSIRTAmericas** se ha consolidado como una herramienta clave para el intercambio de información sobre amenazas cibernéticas entre los CSIRT/CERT (Equipos de Respuesta a Incidentes de Seguridad Cibernética) de América Latina y el Caribe que integran la comunidad de la red CSIRTAmericas. Desde su lanzamiento en 2018, el MISP Regional ha ampliado significativamente su alcance, conectando en la actualidad a **22 CSIRTs de 14 Estados Miembros de la OEA**.

Este sistema funciona como un canal de alerta temprana entre países, combinando datos generados por la comunidad con inteligencia de proveedores externos para mejorar la comprensión de las amenazas emergentes. A través del intercambio de indicadores de compromiso (IOC), patrones de ataque y otros datos críticos, el MISP apoya la prevención, detección y mitigación de incidentes de ciberseguridad. Además, incluye una taxonomía propia que permite estandarizar los eventos registrados en la plataforma.

El MISP Regional no solo ha facilitado el intercambio de información en la región, sino que también ha fortalecido la colaboración entre los países, mejorando significativamente su capacidad de respuesta conjunta frente a las amenazas cibernéticas.

¹⁴ CSIRTAmericas. <https://csirtamericas.org/es>

The background is a dark blue gradient. Two circles, one medium blue and one light blue, overlap in the upper left. Concentric white arcs are visible in the lower right.

INSTALACIÓN BÁSICA DE **MISP**

3.1. Dimensionamiento y preparación del servidor para la instalación de MISP

MISP puede instalarse en sistemas operativos GNU/Linux, incluyendo distribuciones como CentOS, Debian, Ubuntu, entre otros. Para obtener una lista completa de sistemas compatibles, puedes consultar la documentación oficial [aquí](#).

La configuración de hardware recomendada para MISP depende del tipo de implementación y uso esperado. A continuación, se presentan algunos ejemplos de configuraciones recomendadas:

- Para pequeñas comunidades de uso compartido o MISP de punto final:
 - 16 GB de memoria RAM.
 - 2 vCPU.
 - 80 GB de espacio en HDD.
- Instancias de entrenamiento o experimentación:
 - 2 GB de memoria RAM.
 - 1 vCPU.

Es importante tener en cuenta que los requisitos de hardware pueden variar en función de varios factores, como el nivel de correlación de datos, la cantidad de eventos y archivos adjuntos, los feeds de información, el número de usuarios simultáneos y el tiempo de retención de la información en el servidor.

Para una estimación más precisa de los recursos necesarios según el tipo de implementación, puedes utilizar la herramienta de dimensionamiento de MISP, disponible en el siguiente enlace: [MISP Sizer](#).

Esta herramienta proporciona una guía personalizada según las características y necesidades de tu organización.

Nota:

MISP ha evolucionado en sus requisitos de PHP a lo largo del tiempo. Inicialmente, las versiones anteriores a la 2.4.135 utilizaban PHP 7.2. A partir de la versión 2.4.135, lanzada en diciembre de 2020, se recomendó actualizar a PHP 7.4 para mejorar el rendimiento y la seguridad. Sin embargo, con el lanzamiento de MISP 2.5.0, se requiere PHP 8.1 o superior para aprovechar las nuevas características y mejoras de la plataforma. Es importante destacar que PHP 7.4 alcanzó su fin de vida útil en noviembre de 2022, por lo que se recomienda actualizar a PHP 8.1 o versiones más recientes para mantener la compatibilidad y seguridad de MISP. Más información [aquí](#).

3.2. Instalación de MISP

En esta sección, se describen dos métodos para instalar MISP: mediante el instalador oficial y utilizando Docker. Ambos métodos ofrecen diferentes ventajas según las necesidades y el entorno de despliegue.

3.2.1. Instalación en Sistema Operativo Linux

- **Descarga e instalación del instalador**

Este manual utiliza Ubuntu 24.04 como sistema operativo e instalará la versión 2.5 de MISP. Para comenzar con la instalación, abre el terminal y descarga el script de instalación ejecutando el siguiente comando:

```
$ wget --no-cache -O /tmp/INSTALL.sh \
https://raw.githubusercontent.com/MISP/MISP/2.5/INSTALL/INSTALL.ubuntu2404.sh
```

Nota:

Si desea descargar MISP 2.4 deberá ejecutar el siguiente comando:

```
wget --no-cache -O /tmp/INSTALL.sh \
https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
```

- **Ejecutar el instalador**

Inicia la instalación ejecutando el script descargado como administrador:

```
sudo bash /tmp/INSTALL.sh -c
```

Resultado:

Figura 3. Proceso de Instalación de MISP en Linux.

```
[STATUS] Ingesting JSON structures
[OK] JSON structures ingestion successfully completed.
[OK] Apache restart successfully completed.
[OK] Settings configured.
[STATUS] Finalising MISP setup...
[NOTICE] Settings saved to /var/log/misp_settings.txt
[NOTICE] You can now access your MISP instance at https://misp.local
[NOTICE] The default admin credentials are:
[NOTICE] Username: admin@admin.test
[NOTICE] Password: 0LXvzuuv40Lue2MUWWUUMFss6NNRs28F
[NOTICE] MISP setup complete. Thank you, and have a very safe, and productive day.
vboxuser@ubuntu24:~/Desktop$
```

Nota: Captura de pantalla del resultado del script de instalación de MISP en un entorno Linux.

El proceso instalará tanto el núcleo de MISP como sus módulos. Esto puede llevar entre 15 y 20 minutos, dependiendo del sistema y la conexión a Internet. Durante la instalación, el script resolverá automáticamente las dependencias necesarias, y al finalizar, se mostrará un mensaje de instalación exitosa.

3.3. Docker en MISP

Docker es una herramienta que permite empaquetar aplicaciones y sus dependencias en contenedores, facilitando su despliegue y asegurando consistencia en diversos entornos. Para MISP, existen imágenes de Docker que simplifican su instalación y gestión. Puede revisar los contenedores sugeridos por MISP en el siguiente [enlace](#). Para esta guía, utilizaremos el siguiente contenedor Docker disponible en [GitHub](#).

Es importante destacar que esta guía asume que Docker ya está instalado en el servidor donde se desplegará MISP. Además, se requiere **git** para clonar el repositorio con los archivos necesarios para la instalación.

La documentación proporcionada en el repositorio ofrece instrucciones detalladas para configurar y ejecutar MISP en un entorno Docker, asegurando una implementación eficiente y segura.

- **Clonar el repositorio oficial de MISP para Docker:**

Descargue el repositorio oficial que contiene las configuraciones necesarias para desplegar MISP en un entorno Docker:

```
git clone https://github.com/MISP/misp-docker.git
```

- **Acceder al directorio del repositorio clonado:**

Ingrese al directorio recién clonado:

```
cd misp-docker
```

- **Copiar y editar el archivo de configuración de entorno:**

Instalación Básica de MISP

Copie el archivo de plantilla `.env` y edítelo en un editor de textos como **nano** o **vim** para personalizar las variables de entorno según sus necesidades. En este ejemplo utilizaremos nano:

```
cp template.env .env  
nano .env
```

En este archivo, ajuste parámetros como `MISP_BASEURL`, `MYSQL_PASSWORD`, entre otros, para adaptarlos a su entorno específico.

Nota:

Para obtener una lista completa de las variables disponibles y su descripción, consulte el archivo [README](#) del repositorio oficial en GitHub. Este documento proporciona información detallada sobre cómo configurar correctamente cada variable.

- **Construir y desplegar los contenedores de Docker:**

Ejecute los siguientes comandos para construir las imágenes de Docker y desplegar los contenedores en segundo plano.

```
docker-compose build  
docker-compose up -d
```

Estos comandos iniciarán los servicios necesarios para que MISP funcione correctamente.

Este método es especialmente útil para entornos en la nube o infraestructuras con necesidades de escalabilidad y administración ágil.

3.4. Iniciar Sesión

Si la instalación en el sistema operativo o mediante Docker se ha completado exitosamente, abre un navegador e ingresa la IP o el dominio asignado al servidor MISP, por defecto esta es `https://misp.local`. Esto te llevará a la pantalla de inicio de sesión de la plataforma. Para el primer acceso, utiliza las credenciales brindadas al finalizar la instalación:

- **Email:** `admin@admin.test`

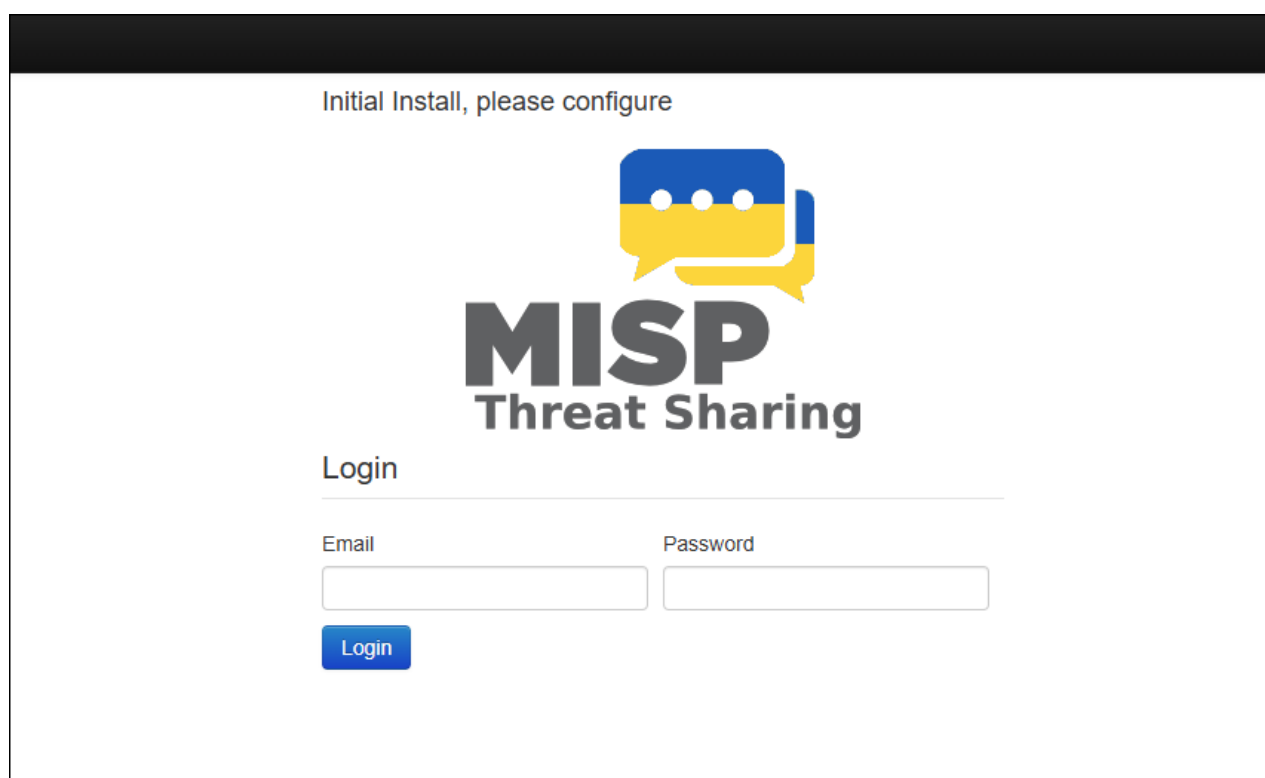
Instalación Básica de MISP

- **Password:** XXXXXXXXXXXXXXXXXXXXXXXX (Esta contraseña es aleatoria y se brinda al finalizar la instalación en la versión 2.5).

También puede encontrar las credenciales de acceso y otros datos importantes en el archivo “**misp_settings.txt**”. Para verlo directamente en la terminal, utilice el siguiente comando:

```
cat /var/log/misp_settings.txt
```

Figura 4. Pantalla de inicio de sesión en MISP.



Nota: Captura de pantalla tomada en la plataforma de MISP, mostrando la interfaz de inicio de sesión.

Una vez que hayas ingresado, se te redirigirá a la interfaz principal de MISP, desde donde podrás comenzar a personalizar la plataforma y gestionar el acceso para otros usuarios.

3.5. Errores comunes en la instalación

Durante la instalación de MISP, es posible que surjan errores. A continuación, se detalla cómo identificar y resolver algunos de los problemas más comunes.

3.5.1. Revisión de registros de errores con el instalador oficial de MISP

Si se presentan problemas durante la instalación oficial, le sugerimos revisar los registros de errores (logs), los cuales se encuentran en la siguiente ruta:

```
/var/www/MISP/app/tmp/logs
```

- **Errores de permisos**

Si encuentras errores relacionados con permisos, es probable que necesites ejecutar los comandos con un usuario que tenga mayores privilegios, como el usuario root. Para elevar temporalmente los privilegios, utiliza:

```
sudo su
```

- **Errores de permisos en la base de datos**

Si encuentras errores relacionados con permisos, es probable que necesites ejecutar los comandos con un usuario que tenga mayores privilegios, como el usuario root. Para elevar temporalmente los privilegios, utiliza:

```
Database connection "Mysql" is missing, or could not be
created. SQLSTATE [HY000] Access denied for user
'misp'@'localhost' (using password: YES)
```

- **Verificar el archivo de configuración de la base de datos**

Para revisar el archivo de configuración de la base de datos (database.php), utiliza el siguiente comando:

```
cat /var/www/MISP/app/Config/database.php
```

- **Acceder a MySQL¹⁵**

El siguiente comando deberá realizarlo con un usuario que tenga permisos de administrador.

¹⁵ Sistema de gestión de bases de datos relacional de código abierto ampliamente utilizado en aplicaciones web y empresariales. Más información: <https://www.mysql.com>

Instalación Básica de MISP

```
sudo mysql -u root
```

- **Crear y ajustar permisos del usuario “misp” en la base de datos**

Una vez dentro de MySQL, puedes crear o actualizar el usuario “misp” y asignarle una nueva contraseña reemplazando ‘contraseña’ con la que desees utilizar:

```
ALTER USER 'misp'@'localhost' IDENTIFIED BY 'contraseña';
```

A continuación, otorga todos los privilegios necesarios para MISP:

```
GRANT ALL PRIVILEGES ON misp.* TO 'misp'@'localhost';
```

Luego, recarga los privilegios para que los cambios tengan efecto:

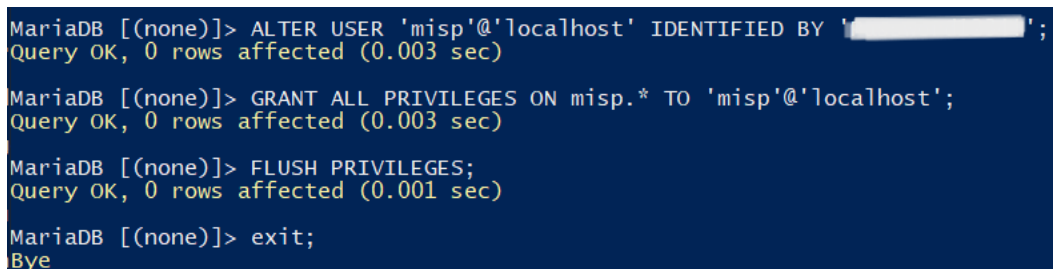
```
FLUSH PRIVILEGES;
```

Cuando hayas terminado, sal de MySQL con:

```
exit;
```

Resultado

Figura 5. Configuración de Permisos en MariaDB para MISP.



```
MariaDB [(none)]> ALTER USER 'misp'@'localhost' IDENTIFIED BY '[redacted]';  
Query OK, 0 rows affected (0.003 sec)  
  
MariaDB [(none)]> GRANT ALL PRIVILEGES ON misp.* TO 'misp'@'localhost';  
Query OK, 0 rows affected (0.003 sec)  
  
MariaDB [(none)]> FLUSH PRIVILEGES;  
Query OK, 0 rows affected (0.001 sec)  
  
MariaDB [(none)]> exit;  
Bye
```

Nota: Captura tomada durante la configuración de permisos en MariaDB.

- **Actualizar la contraseña en el archivo de configuración**

Después de modificar la contraseña en MySQL, asegúrate de actualizarla en el archivo `database.php`. Para ello, abre el archivo con un editor de texto, como `nano`:

```
nano /var/www/MISP/app/Config/database.php;
```

Cambia la contraseña en el archivo para que coincida con la nueva configurada en MySQL. Guarda los cambios presionando **Ctrl + X**, luego confirma con **Y** y presiona **Enter**.

```
cat /var/www/MISP/app/Config/database.php
```

Resultado:

Figura 6. Configuración del Archivo database.php en MISP.

```
root@misp2:/var/www/MISP/app/Config# cat database.php
<?php
class DATABASE_CONFIG {
    public $default = array(
        'datasource' => 'Database/Mysql',
        //'datasource' => 'Database/Postgres',
        'persistent' => false,
        'host' => 'localhost',
        'login' => 'misp',
        'port' => 3306, // MySQL & MariaDB
        //'port' => 5432, // PostgreSQL
        'password' => ' ',
        'database' => 'misp',
        'prefix' => '',
        'encoding' => 'utf8',
    );
}
```

Nota: Captura de pantalla de la configuración de permisos en MariaDB y actualización del archivo database.php en MISP.

3.6. Cambio de base de datos de MySQL a PostgreSQL

Por defecto, MISP utiliza MySQL como su base de datos principal. Aunque es técnicamente posible migrar a PostgreSQL, no se recomienda hacerlo.

PostgreSQL no cuenta con soporte oficial en MISP, y la mayoría de los scripts de actualización y mantenimiento están diseñados exclusivamente para MySQL. Cambiar a PostgreSQL podría generar problemas de compatibilidad con componentes y actualizaciones nuevos, ya que el soporte para PostgreSQL en MISP ha estado inactivo en los últimos años.

Para evitar problemas técnicos y garantizar la estabilidad del sistema, se recomienda seguir utilizando MySQL como la base de datos oficial. Esto permite aprovechar todas las actualizaciones y mejoras de manera fluida, sin necesidad de realizar ajustes adicionales o comprometer el rendimiento del sistema.

CONFIGURACIÓN INICIAL,
PERSONALIZACIÓN
DE LA INSTANCIA DE

MISP

Y GESTIÓN DE
TAXONOMÍAS

4.1. Configuración de la MISP.baseurl

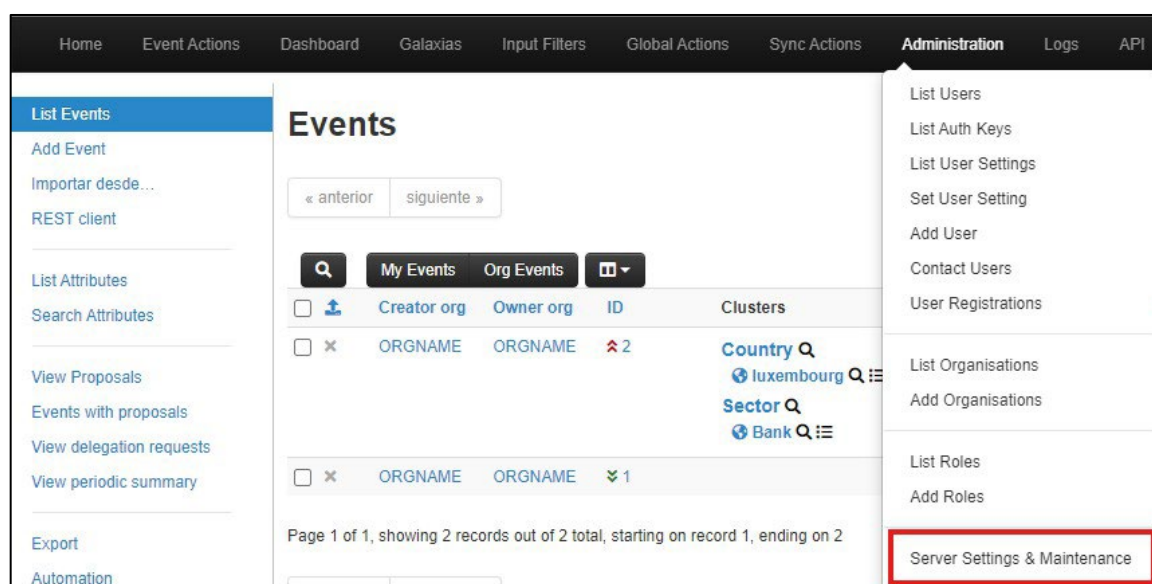
La configuración de `MISP.baseurl` es fundamental para asegurar que la plataforma funcione correctamente y pueda integrarse con otros sistemas. La `baseurl` establece la URL de la aplicación en formato `https://www.mymispinstance.com` o `https://myserver.com/misp`. Esto permite que las características de MISP que dependen de una `baseurl` operen sin problemas.

Por otro lado, `MISP.external_baseurl`¹⁶ define cómo se verá la instancia desde una red externa o por otras instancias de MISP. Si no se establece una, MISP usará la `MISP.baseurl`. Esta configuración garantiza que los datos compartidos incluyan la URL correcta de tu instancia.

4.1.1. Pasos para configurar la BaseURL:

1. En el menú principal de MISP, dirígete a la sección “Administration” y selecciona la opción “Server Settings & Maintenance”.

Figura 7. Acceso a Server Settings & Maintenance en MISP.



Nota: Captura de pantalla del acceso a la sección de configuración en MISP.

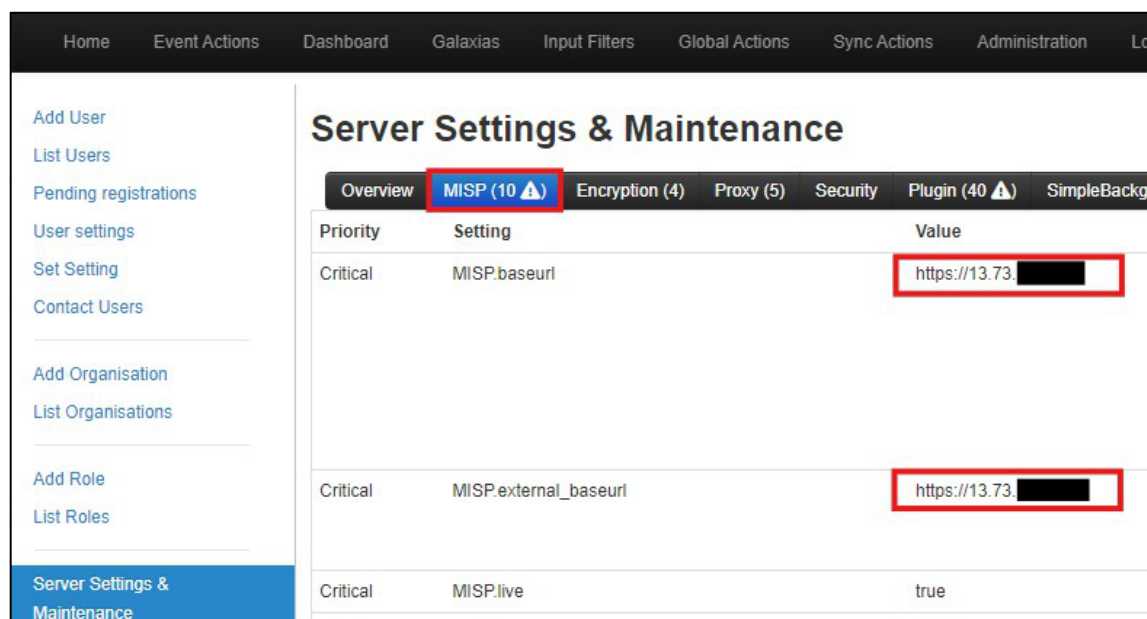
2. Dentro de “Server Settings & Maintenance”, ubica la pestaña “MISP” o “MISP settings”. Aquí, busca los campos “`MISP.baseurl`” y “`MISP.external_baseurl`”.

¹⁶ URL externa configurada en MISP para permitir que otras instancias accedan a la plataforma de manera remota

Personalización de la Instancia de MISP

- En ambos campos, ingresa la URL o dirección IP pública que corresponderá a tu instancia de MISP (por ejemplo, `https://www.mymispinstance.com` o `https://myserver.com/misp`). Esto es necesario para el correcto funcionamiento de la plataforma y para que la URL se incluya automáticamente en los grupos de uso compartido. En caso estés trabajando en un ambiente local, sugerimos dejarlo con los valores por defecto.

Figura 8. Configuración de `MISP.baseurl` y `MISP.external_baseurl`.



Nota: Captura de pantalla del ajuste de parámetros de URL en la sección "Server Settings & Maintenance" de MISP.

Nota:

Si se ingresa una URL o IP incorrecta, la interfaz gráfica de la instancia de MISP no estará accesible. En caso de que esto ocurra, puedes corregir la configuración accediendo al servidor mediante la terminal y ajustando la BaseURL manualmente. [Más información aquí.](#)

4.2. Personalización de la Instancia MISP

En esta sección, aprenderás a personalizar tu instancia de MISP adaptándola a la identidad de tu organización. Esto incluye agregar el logotipo de tu organización en la pantalla de inicio de sesión, personalizar un mensaje de bienvenida y modificar los textos en el pie de página:

Personalización de la Instancia de MISP

1. Acceder a la Configuración de Archivos

Dirígete a la opción “Server Settings & Maintenance” en la sección “Administration” (como en la configuración anterior) y selecciona la pestaña “Manage Files”.

Figura 9. Acceso a Manage Files en MISP.

Server Settings & Maintenance



Nota: Captura de pantalla de la sección "Manage Files" en MISP para gestionar logotipos de la organización.

2. Subir el Logo de tu Organización

En la sección “Additional image files”, selecciona el archivo de logo que desees cargar. Haz clic en “Choose File” para seleccionar el archivo y luego presiona “Upload” para cargarlo en la plataforma. *Recuerda guardar el nombre de la imagen ya que será usada en el siguiente paso.*

Figura 10. Carga de Imágenes en Additional Image Files de MISP.

Additional image files

Descripción: Image files uploaded into this directory can be used for various purposes, such as for the login page logos

Expected Format: PNG or SVG file

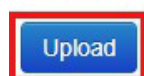
Path: /var/www/MISP/app/files/img/custom

Files set for each relevant setting:

- MISP.footer_logo:
- MISP.home_logo:
- MISP.welcome_logo:
- MISP.welcome_logo2:

Filename	Used by	Size	Permissions	Acciones
csirtamericas.png		42.2 kB	rw	

Seleccionar archivo Sin archivos seleccionados



Nota: Captura de pantalla del ajuste de parámetros de URL en la sección "Server Settings & Maintenance" de MISP.

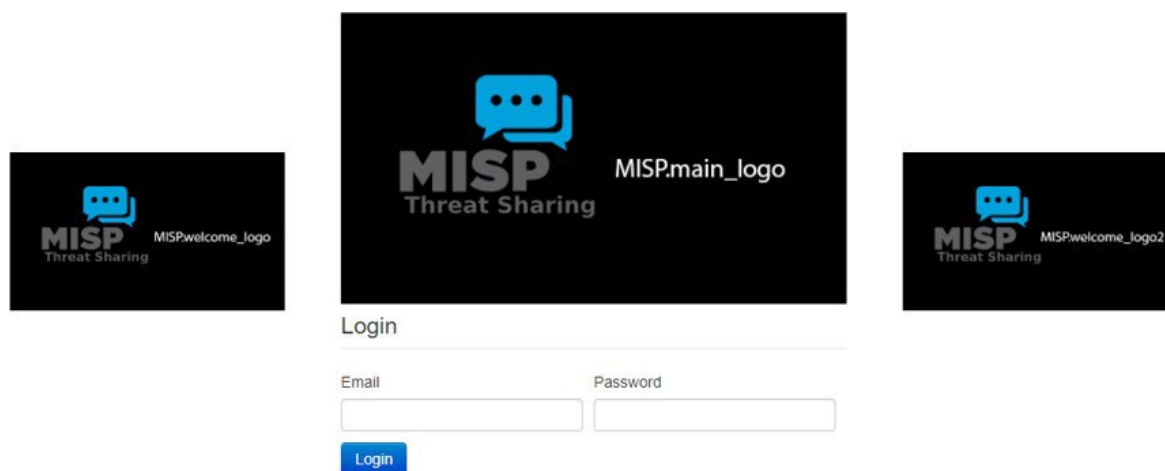
3. Configurar la pantalla de bienvenida y home

Una vez que hayas cargado el logo, regresa a "Administration", luego a "Server Settings & Maintenance" y selecciona la pestaña "MISP". En esta sección, podrás modificar diversos ítems para personalizar la interfaz de MISP. A continuación, te explicamos algunas opciones:

- MISP.main_logo.
- MISP.welcome_logo.
- MISP.welcome_logo2.

Una vez haya ubicado alguna de estas opciones mencionadas, deberás hacer doble click sobre el recuadro y colocar el nombre de la imagen que subiste previamente, por ejemplo: "test.png".

Figura 11. Logotipos en Pantallas de Inicio y Bienvenida en MISP.

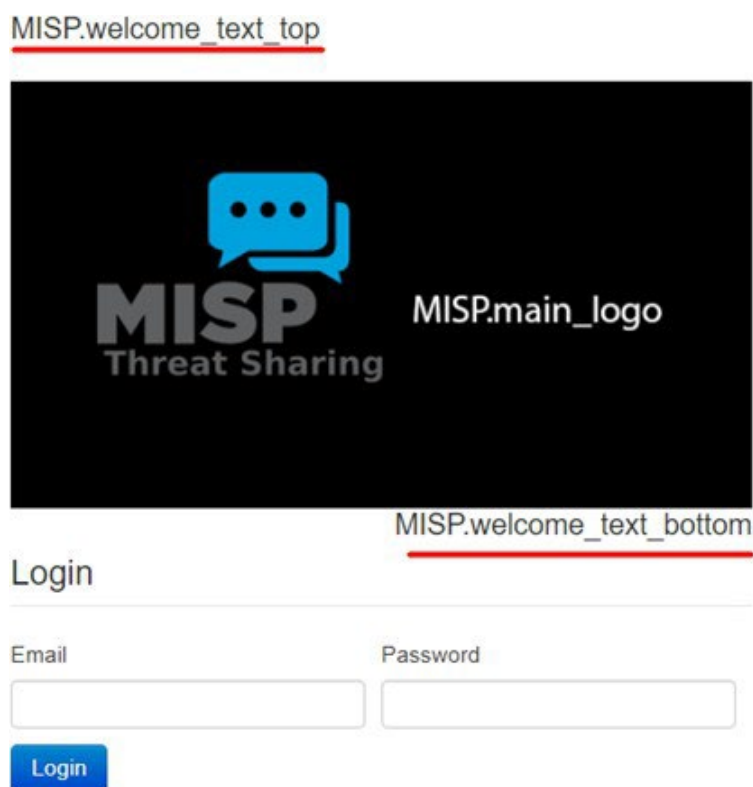


Nota: Captura de pantalla con la configuración de logotipos en MISP.

- MISP.welcome_text_top.
- MISP.welcome_text_bottom.

Personalización de la Instancia de MISP

Figura 12. Textos de Bienvenida en la Pantalla de Inicio de MISP.



Nota: Captura de pantalla con la configuración de MISP.welcome_text_top y MISP.welcome_text_bottom.

Como ejemplo te mostramos como hemos configurado nuestro MISP; no obstante, eres libre de modificarlo según tus preferencias.

Figura 13. Ejemplo de Personalización Final en MISP.

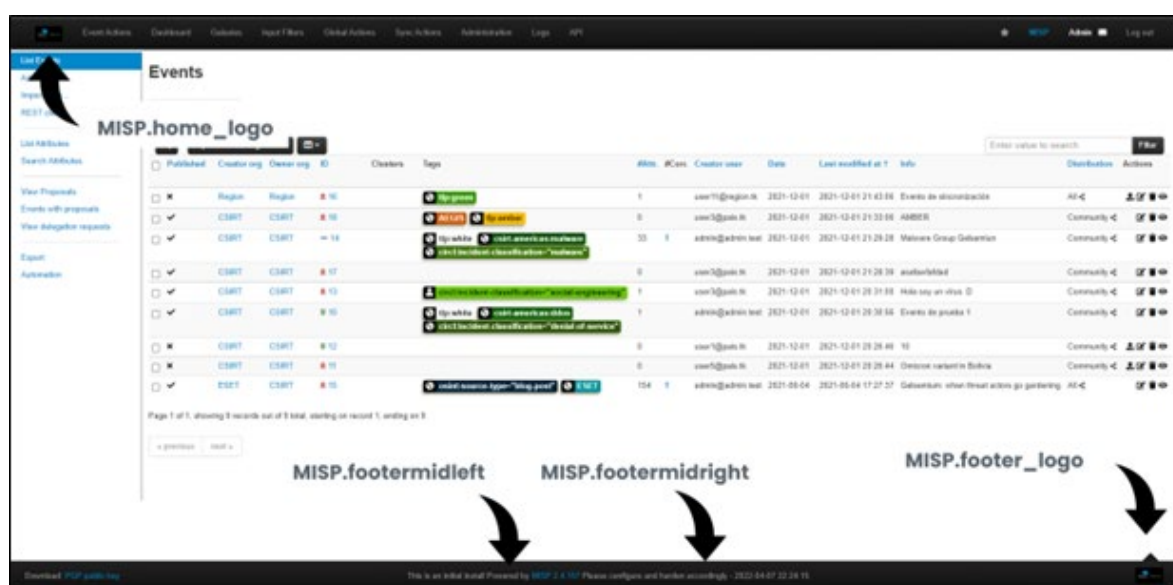


Nota: Captura de pantalla de una pantalla de inicio personalizada en MISP.

Para configurar los elementos visuales de la pantalla de inicio (“Home”) en MISP, tienes las siguientes opciones disponibles:

- MISP.home_logo.
- MISP.footer_logo.
- MISP.footermidright.
- MISP.footermidleft.

Figura 14. Elementos Visuales en la Interfaz de MISP.



Nota: Captura de pantalla que muestra las opciones MISP.home_logo, MISP.footer_logo, MISP.footermidleft y MISP.footermidright en la interfaz de MISP.

4.3. Taxonomías

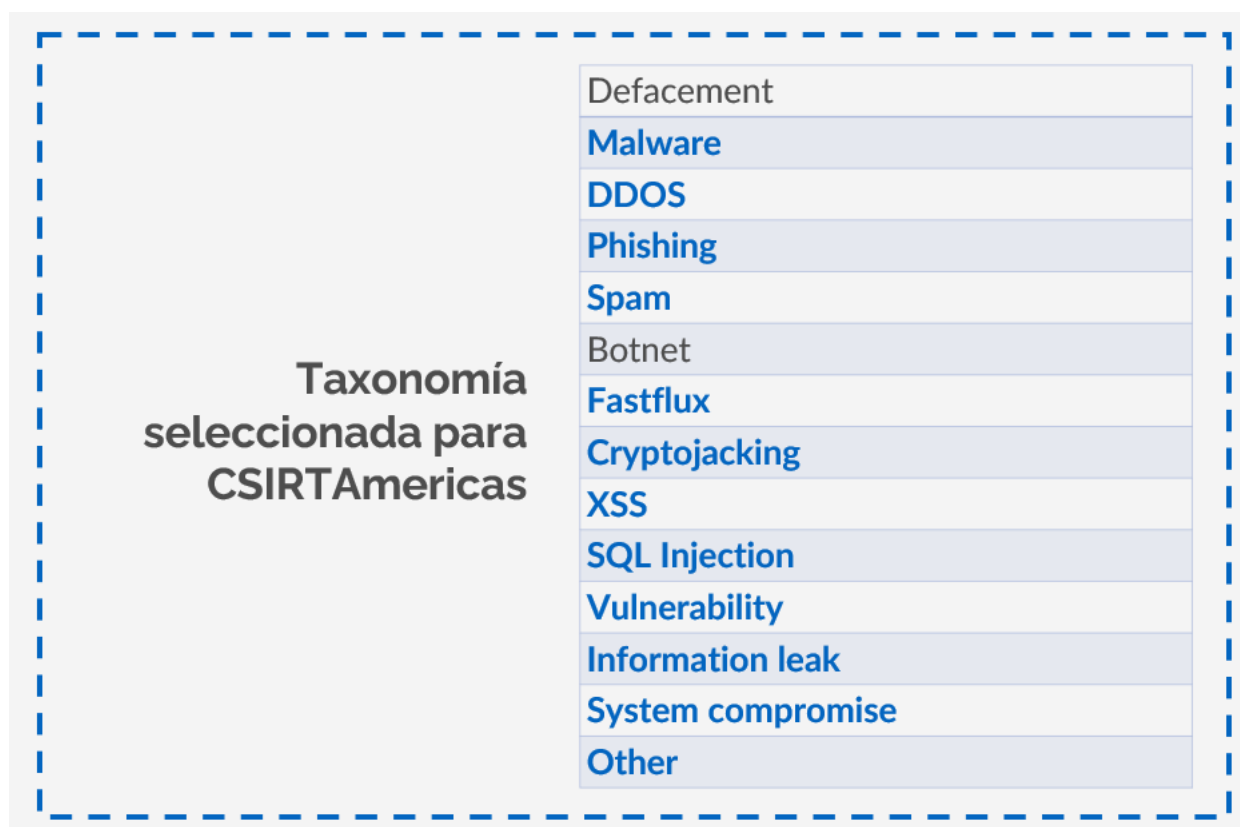
Una taxonomía común permite a los CSIRT compartir y clasificar los incidentes de forma homogénea. CSIRTAméricas utiliza el término “taxonomía” como una forma de esquema de clasificación de incidentes cibernéticos. Al dividir los incidentes cibernéticos en categorías, dicha taxonomía pretende facilitar el intercambio de información y la notificación de incidentes entre los estados miembros, contribuyendo al desarrollo de estadísticas sobre patrones y tendencias de incidentes cibernéticos en la región. En concreto, esta taxonomía facilita el intercambio de información de bajo nivel y de indicadores de detección a través del

Personalización de la Instancia de MISP

MISP regional y de la central de Feeds, respectivamente. Al homogeneizar las categorías de respuesta y detección de incidentes, CSIRTAméricas pretende facilitar no sólo la notificación de incidentes cibernéticos y el intercambio de información con sus miembros, sino también la producción de informes y estudios sobre amenazas de incidentes en toda América Latina y el Caribe.

El equipo de CSIRTAméricas desarrolló la taxonomía que se presenta a continuación basándose en la taxonomía desarrollada por el Centro de Respuesta a Incidentes Informáticos de Luxemburgo (circl.lu) en combinación con la taxonomía de ENISA. Esta taxonomía permite la producción de informes que proporcionan una visión general de la seguridad tanto en términos técnicos como sectoriales para un público más amplio (por ejemplo, profesionales técnicos, responsables políticos, fuerzas de seguridad, autoridades de alto nivel).

Figura 15. Taxonomía CSIRTAméricas



Nota: Taxonomía representativa de CSIRTAméricas para la clasificación de incidentes

CSIRTAméricas trabaja con sus miembros para revisar periódicamente la taxonomía y actualizarla cuando se considere necesario teniendo en cuenta la evolución del panorama

de amenazas en la región y los nuevos métodos empleados por los atacantes. La taxonomía actual ya incluye una categoría «otros» para clasificar los nuevos ataques que no encajan en ninguna de las categorías predefinidas. En algunos casos, las nuevas amenazas se vuelven tan comunes que requieren la creación de una nueva categoría, como ha ocurrido recientemente con el criptojacking. Los miembros de CSIRTAméricas también reciben formación en el uso de esta taxonomía para garantizar que la información se comparte de forma homogénea dentro de la plataforma.

4.3.1. Taxonomías en MISP

MISP ofrece una amplia variedad de taxonomías predefinidas, cada una adaptada a necesidades específicas de organizaciones y comunidades. Entre ellas se incluyen:

- **CSIRTAméricas ([csirt-americas](#)):** Una taxonomía diseñada por CSIRTAméricas, adecuada para la clasificación de incidentes en las Américas.
- **CSIRT Luxemburgo ([circl](#)):** Taxonomía utilizada por el CSIRT de Luxemburgo, adaptada a sus necesidades específicas de clasificación.
- **Traffic Light Protocol ([tlp](#)):** Un sistema de clasificación de sensibilidad de la información para compartir de forma controlada.
- **Event Recording and Incident Sharing ([veris](#)):** Taxonomía centrada en la grabación y el intercambio de incidentes de seguridad.

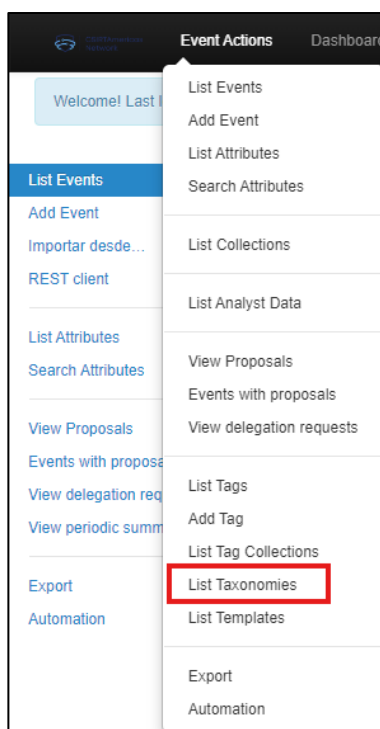
Es importante señalar que ninguna taxonomía es mejor que otra; todas son simplemente diferentes maneras de etiquetar y clasificar la información en función de las necesidades específicas de cada organización o comunidad.

4.3.2. Agregar la taxonomía de CSIRTAméricas a tu instancia MISP

1. Acceder a la Lista de Taxonomías

En el menú principal, dirígete a “Event Actions” y selecciona “List taxonomies”.

Figura 16. Acceso a la Lista de Taxonomías en MISP.



Nota: Captura de pantalla del menú para acceder a la lista de taxonomías en MISP.

2. Buscar y Habilitar la Taxonomía

Para habilitar una taxonomía, haz clic en el ícono “▶” junto a la taxonomía que deseas activar. Para fines de demostración, en este ejemplo se habilitará la taxonomía de CSIRT Americas. En la lista de taxonomías, busca **csirt-americas**.

Figura 17. Habilitación de Taxonomías en MISP.

x	☐	☐	0 / 14	▶  
x	☐	☐	0 / 22	▶  
x	☐	☐	0 / 6	▶  

Nota: Captura que muestra cómo activar todas las etiquetas de una taxonomía.

3. Habilitar Todas las Etiquetas

De manera predeterminada, las etiquetas asociadas a la taxonomía no estarán activas. Para activarlas, selecciona la opción “enable all”, lo que habilitará todas las etiquetas de la taxonomía.

Figura 18. Confirmación de Etiquetas Habilitadas.

✓	☐	☐	0 / 14 (enable all)	 
x	☐	☐	0 / 22	  
x	☐	☐	0 / 6	  

Nota: Captura que muestra cómo activar todas las etiquetas de una taxonomía.

Al hacerlo, la taxonomía mostrará un “✓” para indicar que está habilitada, y el contador de etiquetas se actualizará (por ejemplo, “14/14”).

Figura 19. Confirmación de Etiquetas Habilitadas.

✓	☐	☐	14 / 14	 
x	☐	☐	0 / 22	  
x	☐	☐	0 / 6	  

Nota: Captura que indica la habilitación completa de las etiquetas.

4. Uso de la Taxonomía en Eventos

Una vez habilitada, podrás agregar la taxonomía seleccionada al crear nuevos eventos en MISP. Esto facilita la organización y clasificación de los datos. Para obtener más información sobre la creación de eventos, consulta el manual 5, “Creación de Eventos en MISP”.

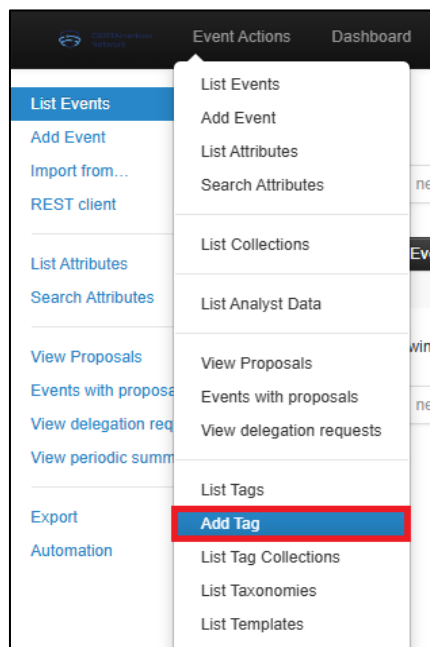
4.3.3. Agregar una Etiqueta a tu instancia MISP

1. Acceder a la opción “Add Tag”

Personalización de la Instancia de MISP

En el menú principal, dirígete a “Event Actions”, selecciona “List Events”, despliega el menú y haz clic en “Add Tag”.

Figura 20. Acceso a la Opción Add Tag en MISP



Nota: Captura de pantalla del menú para acceder a Add Tag de MISP.

2. Configurar los detalles de la etiqueta

En la pantalla de "Add Tag", completa los siguientes campos:

- **Name:** Ingresa el nombre de la etiqueta.
- **Colour:** Selecciona un color para la etiqueta utilizando el selector de color.
- **Restrict tagging to org:** Define si la etiqueta estará restringida a una organización específica (opcional).
- **Restrict tagging to user:** Define si la etiqueta estará restringida a un usuario específico (opcional).
- **Exportable:** Marca esta opción para que la etiqueta sea exportable.
- **Opciones adicionales:** Puedes seleccionar "Hide Tag" para ocultar la etiqueta o "Enforce this tag to be used as local only" si deseas que la etiqueta sea de uso exclusivo en tu instancia.

Figura 21. Formulario de Configuración de Etiquetas en MISP.

The screenshot displays the MISP web interface for adding a new tag. The top navigation bar includes links for Event Actions, Dashboard, Galaxies, Input Filters, and Global Actions. On the left sidebar, the 'Add Tag' option is highlighted. The main content area is titled 'Add Tag' and contains the following fields and options:

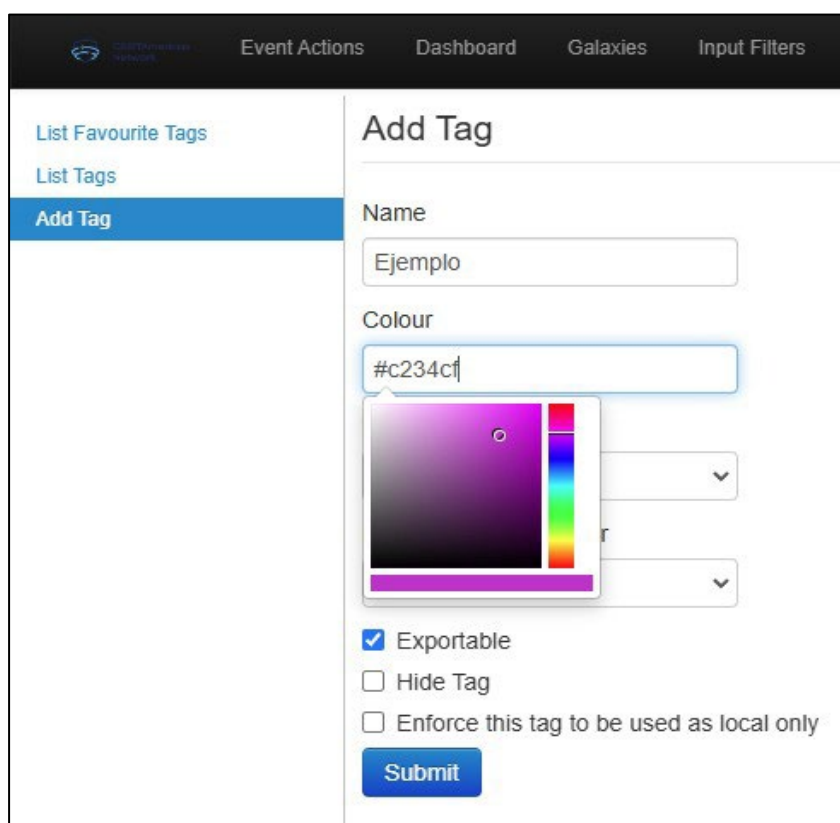
- Name:** A text input field.
- Colour:** A text input field for specifying a hex color.
- Restrict tagging to org:** A dropdown menu currently set to 'Unrestricted'.
- Restrict tagging to user:** A dropdown menu currently set to 'Unrestricted'.
- Exportable:** A checked checkbox.
- Hide Tag:** An unchecked checkbox.
- Enforce this tag to be used as local only:** An unchecked checkbox.
- Submit:** A blue button to save the configuration.

Nota: Captura de pantalla del menú para acceder a Add Tag de MISP.

3. Elegir el color de la etiqueta

Haz clic en el campo de color (**Colour**) para abrir el selector de colores. Escoge el color que desees asignar a la etiqueta ingresando un valor hexadecimal o seleccionando manualmente el tono deseado.

Figura 22. Selección de Color para Etiquetas en MISP.



The screenshot shows the MISP web interface. On the left, a sidebar contains links: 'List Favourite Tags', 'List Tags', and 'Add Tag' (which is highlighted in blue). The main area is titled 'Add Tag'. It contains a 'Name' field with the text 'Ejemplo'. Below it is a 'Colour' field with the hex code '#c234cf'. A color picker is open over the 'Colour' field, showing a spectrum of colors with a purple hue selected. Below the color picker, there are three checkboxes: 'Exportable' (checked), 'Hide Tag' (unchecked), and 'Enforce this tag to be used as local only' (unchecked). At the bottom of the form is a blue 'Submit' button.

Nota: Captura de pantalla del selector de color en el formulario "Add Tag".

4. Guardar la etiqueta

Una vez que hayas configurado todos los detalles de la etiqueta, haz clic en el botón **Submit** para guardar los cambios. La nueva etiqueta se agregará a tu instancia de MISP y estará disponible para su uso en eventos futuros.

**CREACIÓN DE
EVENTOS EN
MISP**

5.1. Introducción

Esta sección define conceptos clave relacionados con la creación y gestión de eventos en MISP, basados en la documentación oficial. Estos términos serán esenciales para seguir y aplicar los pasos del manual de manera adecuada.

5.1.1. Evento en MISP

En MISP, un evento es una colección estructurada de información relacionada con una amenaza o incidente de ciberseguridad. Incluye detalles como direcciones IP, hashes de archivos y otros indicadores de compromiso (IoCs), que ayudan a identificar y caracterizar la amenaza. Cada evento es el punto central para el intercambio de información en MISP.

5.1.2. Atributos del Evento

Los atributos son elementos de datos individuales dentro de un evento en MISP. Cada atributo está categorizado y tiene un tipo y valor específicos, proporcionando información detallada sobre el evento. Los atributos permiten describir los distintos aspectos de una amenaza, como IPs, URLs, o hashes de archivos (para más información acerca de los atributos, visite el siguiente [enlace](#)).

5.1.3. Organización

En MISP, una organización representa una entidad en la que trabajan usuarios con roles y responsabilidades definidos. Cada usuario pertenece a una organización específica, que puede ser:

1. **Organización local:** Agrupa usuarios dentro de la instancia de MISP.
2. **Organización remota:** Representa una organización de una instancia externa de MISP, facilitando la sincronización entre instancias.

5.2. Alcance de distribución de eventos

El alcance de distribución en MISP define el nivel de visibilidad de un evento. Los niveles de distribución permiten especificar quién puede ver el evento, desde una única organización hasta todas las comunidades conectadas. Esta funcionalidad asegura un control granular sobre la difusión de la información. Cada vez que se crea un evento, se puede elegir uno de los siguientes tipos de distribución:

- **Your organisation only (Solo su organización):** El evento es visible solo para la organización del usuario que lo creó.
- **This community only (Solo esta comunidad):** Visible para todas las organizaciones locales y sincronizadas dentro de la misma instancia.

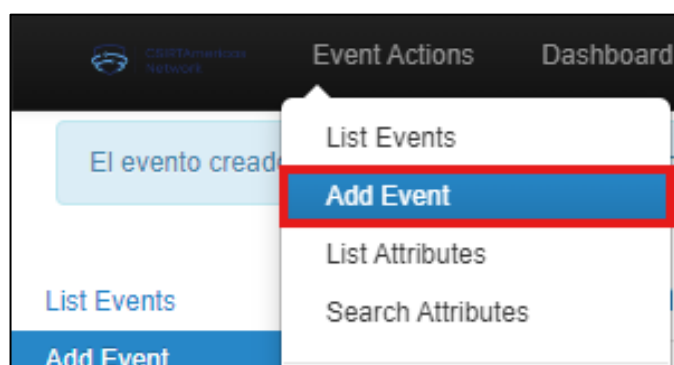
Creación de Eventos

- **Connected communities (Comunidades conectadas):** Accesible para todas las organizaciones y servidores sincronizados a dos niveles.
- **All communities (Todas las comunidades):** El evento se comparte con todas las comunidades de MISP, permitiendo su propagación sin restricciones.
- **Sharing group (Grupo de intercambio):** Permite seleccionar organizaciones específicas para compartir el evento, tanto locales como remotas.

5.3. Creación de eventos en MISP

Para crear un evento en MISP, dirígete a la barra superior, haz clic en "Event Actions" y selecciona "Add Event". Esta acción abrirá una ventana donde podrás ingresar la información básica del evento.

Figura 23. Creación de eventos en MISP.



Nota: Captura que muestra la sección "Add Event" en MISP.

En esta pantalla, completa los datos mínimos necesarios para definir el evento, incluyendo el tipo de distribución (quién puede ver el evento), el nivel de amenaza, el estado del análisis y cualquier información que identifique el evento. Una vez completados los campos requeridos, haz clic en "**Submit**" o "**Enviar**". De forma predeterminada, el evento se guardará como borrador y no será publicado inmediatamente.

Figura 24. Formulario de creación de eventos en MISP.

Add Event

Date

2024-09-06

Distribution 

This community only 

Threat Level 

Low 

Analysis 

Initial 

Event Info

Evento de Ejemplo 001

Extends Event

Event UUID or ID. Leave blank if not applicable.

Enviar

Nota: Captura que muestra el formulario para agregar un evento en MISP.

Figura 25. Detalles del evento en MISP.

[Event Actions](#)
[Dashboard](#)
[Galaxias](#)
[Input Filters](#)
[Global Actions](#)
[Sync Actions](#)

El evento se ha guardado

Ver Evento

[Ver gráfico de correlación](#)
[Ver historia del eventos](#)

[Editar Evento](#)
[Eliminar Evento](#)
[Add Attribute](#)
[Añadir objeto](#)
[Añadir adjunto](#)
[Add Event Report](#)
[Populate from...](#)
[Enriquecer Evento](#)
[Merge attributes from...](#)

[Publicar Evento](#)
[Publicar \(sin email\)](#)
[Contactar con el Informador](#)

Evento de Ejemplo 001

Event ID	142
UUID	cda58278-86ed-43e1-aefe-4d17affb3188  
Creator org	ORNAME
Owner org	ORNAME
Creator user	admin@admin.test
Protected Event (experimental) 	 Event is in unprotected mode. Switch to protected mode
Etiquetas	Missing taxonomies: tlp   
Date	2024-09-06
Threat Level	 Low
Analysis	Initial
Distribution	This community only  

Nota: Captura que muestra los detalles del evento llamado “Evento de Ejemplo 001” en MISP.

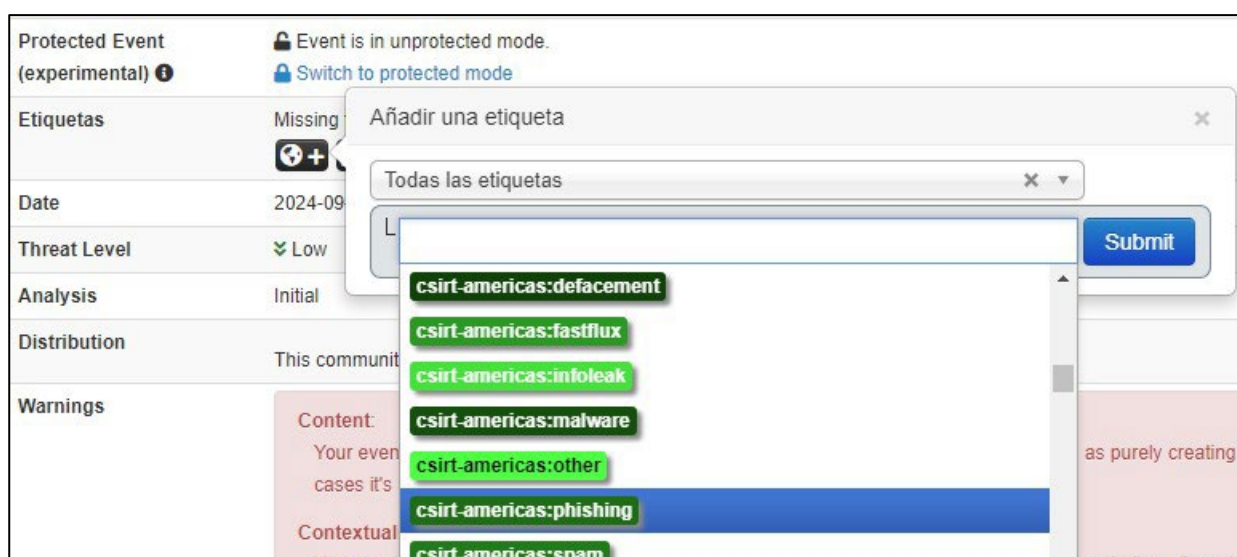
5.3.1. Añadir etiquetas al evento

Después de crear el evento, puedes añadir etiquetas para clasificarlo según la taxonomía seleccionada, como CSIRT Americas o TLP. Haz clic en el ícono de etiquetas globales (representado por un ícono de mundo), busca y selecciona la etiqueta deseada, y confirma haciendo clic en **"Submit"** o **"Enviar"**.

Nota:

Las etiquetas locales, representadas con el ícono de una persona, no serán visibles para las organizaciones remotas.

Figura 26. Añadir etiquetas al evento en MISP.



Nota: Captura que muestra la sección “Añadir una etiqueta” en MISP.

Figura 27. Detalles del evento con etiquetas en MISP.

Evento de Ejemplo 001	
Event ID	142
UUID	cda58278-86ed-43e1-aefe-4d17afb3188  
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental) 	 Event is in unprotected mode.  Switch to protected mode
Etiquetas	 csirt-americas:phishing   tlp:white   
Date	2024-09-06
Threat Level	 Low
Analysis	Initial
Distribution	This community only  

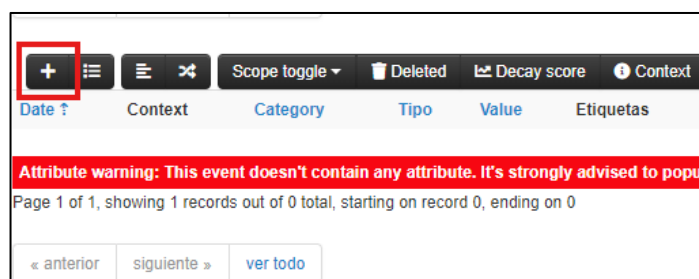
Nota: Captura que muestra la sección “Evento de Ejemplo 001” con etiquetas añadidas en MISP.

5.3.2. Agregar atributos al evento

Para describir el evento en mayor detalle, puedes agregar al menos un atributo, como una dirección IP o un hash de archivo. Hay dos formas de acceder a la sección para añadir atributos:

- **Desde la parte inferior de la pantalla del evento:** Desplázate hacia la parte inferior y selecciona “Add Attribute”.

Figura 28. Agregar atributos al evento en MISP.

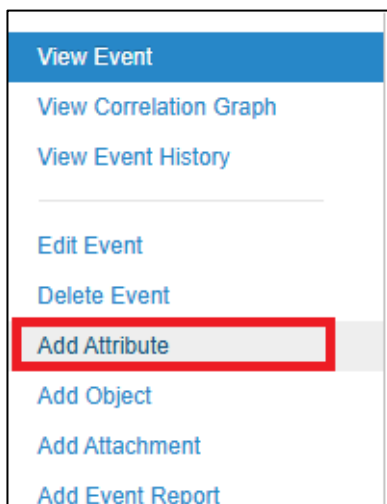


Nota: Captura que muestra la sección “Add Attribute” en MISP.

Creación de Eventos

- **Desde la barra lateral izquierda:** Haz clic en “**Add Attribute**” en el menú de la barra lateral izquierda.

Figura 29. Menú para agregar atributos al evento en MISP.



Nota: Captura que muestra la sección “Add Attribute” en el menú lateral de MISP.

Se abrirá una nueva ventana en la que podrás seleccionar la categoría, el tipo y el valor del atributo. Una vez completados estos campos, haz clic en “**Submit**” o “**Enviar**” para guardar el atributo en el evento:

Figura 30. Formulario para agregar atributos al evento en MISP.



Nota: Captura que muestra la sección “Add Attribute” en MISP.

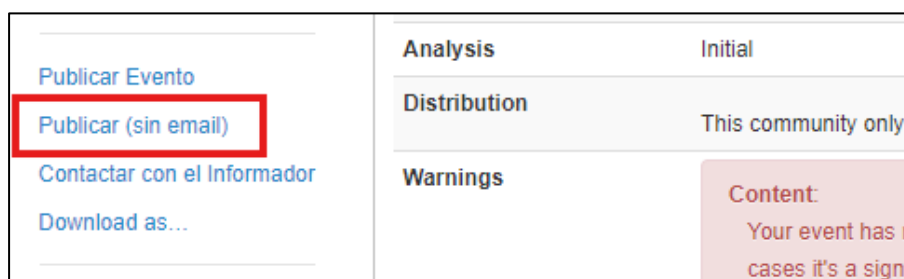
5.3.3. Publicar el evento

Para compartir el evento con otros usuarios y organizaciones, publícalo manualmente. Tienes dos opciones para hacerlo:

- **"Publish Event"**: se publicará y se enviará un correo a los usuarios dentro de su organización, comunicando la creación de un nuevo evento. En español, encontrarán la opción como "Publicar Evento".
- **"Publish Event (no email)"**: se publicará, pero no se enviará ningún correo. En español, encontrarán la opción como "Publicar (sin email)".

Una vez publicado el evento, este será distribuido acorde a la distribución seleccionada (ver [Alcance de distribución de eventos](#)).

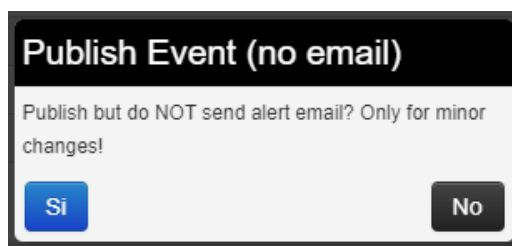
Figura 31. Opciones para publicar eventos en MISP



Publicar Evento	Analysis	Initial
Publicar (sin email)	Distribution	This community only
Contactar con el Informador	Warnings	Content: Your event has n cases it's a sign
Download as...		

Nota: Captura que muestra la sección "Publicar (sin email)" en MISP.

Figura 32. Confirmación para publicar evento en MISP.



Publish Event (no email)

Publish but do NOT send alert email? Only for minor changes!

Nota: Captura que muestra la sección "Publish Event (no email)" en MISP.

5.4. Enriquecimiento de eventos

Para enriquecer un evento con información adicional, puedes importar atributos desde el menú **“Populate from...”** en el panel izquierdo, seleccionando alguna de las opciones disponibles. También puedes automatizar este proceso utilizando la API REST de MISP; para obtener más detalles, consulta la documentación de la API REST en el siguiente [enlace](#).

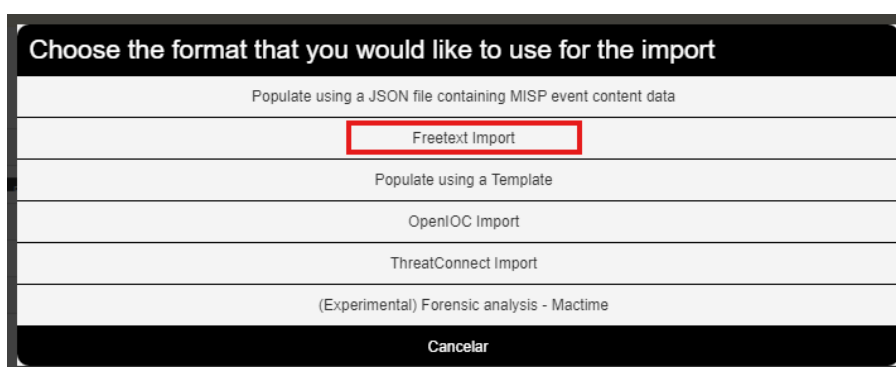
Figura 33. Enriquecimiento de eventos en MISP.



Nota: Captura que muestra la sección “Populate from...” en MISP.

Dentro del menú **“Populate from...”**, selecciona la opción **“Freetext Import”**¹⁷ para agregar atributos basados en texto libre.

Figura 34. Importación de atributos con texto libre en MISP.



Nota: Captura que muestra la sección “Freetext Import” en MISP.

¹⁷ Función de MISP que permite importar atributos basados en texto libre desde reportes o indicadores de compromiso (IoCs).

Creación de Eventos

Introduce los datos de indicadores de compromiso (IoCs) o copia el texto de un reporte de IoCs en el campo de texto libre. Luego, haz clic en **"Submit"** para procesar el contenido.

Figura 35. Herramienta de importación de texto libre en MISP.

Freetext Import Tool

Paste a list of IoCs into the field below for automatic detection.

Ejemplo de texto de IoC con ataques desde la IP 200.30.44.55 y con piezas de malware llamada demo.exe con hash SHA2
95f066c9789dc095cfb1ad5bfa3f1ec874fadb00b5624558b3850662a13dfa7

Enviar Cancelar

Nota: Captura que muestra la sección “Freetext Import” en MISP.

Finalmente, selecciona y configura los atributos generados y confirma la acción haciendo clic en **"Submit attributes"** para incorporarlos al evento.

Figura 36. Resultados de importación de texto libre en MISP

Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic

Warning: You are missing warninglist(s) that are used to recognise TLDs. Make sure your MISP has the warninglist submodule enabled and updated or else this tool might e

☐ Proposals instead of attributes

Value	Similar Attributes	Category	Tipo	IDS	Disat
200.30.44.55		Network activity	ip-dst	☒	☐
demo.exe		Payload delivery	filename	☒	☐
95f066c9789dc095cfb1ad5bfa3f1ec874fadb00b5624558b3850662a13dfa7		Payload delivery	sha256	☒	☐

Submit attributes Create object

Nota: Captura que muestra la sección “Freetext Import Results” en MISP.

**GESTIÓN DE
USUARIOS Y
ORGANIZACIONES**

MISP

6.1. Introducción

La gestión de usuarios consiste en administrar los permisos que va a tener cada persona que se conecte a su instancia de MISP. Una mala configuración podría conllevar a la pérdida de confidencialidad de los datos transmitidos en MISP. A continuación, se definirán conceptos necesarios para entender el presente manual:

6.1.1. Usuario

Un usuario en MISP es cualquier persona con acceso a la plataforma para interactuar con los datos, ya sea visualizándolos, editándolos o administrándolos según sus permisos asignados.

6.1.2. Instancia de MISP

Cuando se habla de una "Instancia de MISP", se hace referencia al despliegue de dicha herramienta dentro de un servidor, en otras palabras, si se ha instalado el software MISP en un servidor, este se convierte en una instancia MISP.

6.1.3. Sincronización

Sincronización es el proceso por el cual dos instancias MISP pueden compartir eventos entre sí. Esto mejora la cooperación entre organizaciones y permite un intercambio rápido de datos y/o IoC.

6.1.4. Administrador en MISP

Un administrador es la persona que tiene la responsabilidad de configurar, mantener, monitorear, documentar y asegurar el correcto funcionamiento de un sistema informático, o algún aspecto de este. Dentro de MISP, existen dos tipos de administradores:

1. **Admin** (los administradores de instancia): Tienen acceso a todas las funciones de MISP, incluidas las funciones globales como la creación, modificación y eliminación de usuarios, de los roles, las organizaciones, los archivos de configuración, entre otros.
2. **Org Admin** (administradores de una organización): Sólo pueden realizar una administración limitada de los usuarios dentro de la organización asignada.

6.2. Gestión de usuarios

Como administrador de la instancia (Admin), se pueden crear nuevas cuentas para los usuarios, eliminarlos, listar todos los existentes, editar sus roles o agregar nuevos roles. Por

otro lado, los administradores de la organización (Org Admin) están restringidos a ejecutar estas acciones exclusivamente dentro de los usuarios de su propia organización.

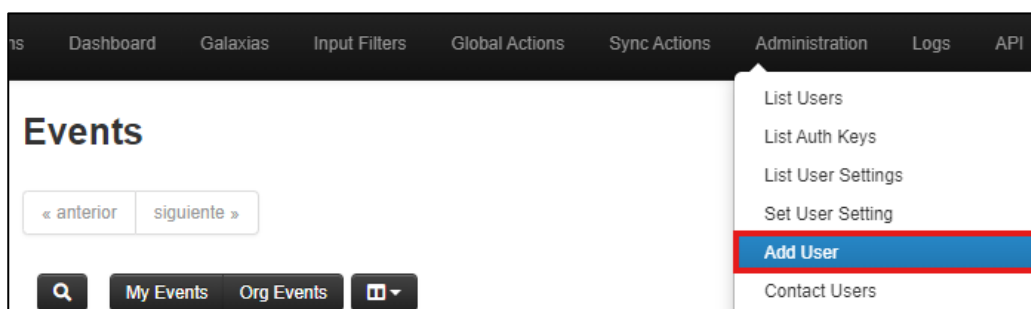
6.2.1. Cómo añadir un nuevo usuario

Para agregar un nuevo usuario en MISP, sigue estos pasos:

1. Accede al menú de administración

Ve a la barra superior y haz clic en “Administration”, luego selecciona “Add User”.

Figura 37. Menú para añadir un nuevo usuario en MISP.



Nota: Captura que muestra la sección “Add User” en MISP.

Nota:

Debes tener privilegios administrativos para realizar esta acción.

2. Rellena el formulario

Ve a la barra superior y haz clic en “Administration”, luego selecciona:

- **Email:** la dirección de correo electrónico del usuario, este se utilizará como su nombre de inicio de sesión.
- **Set password:** marque la casilla si desea definir una contraseña temporal para el usuario. Si decides no configurar una contraseña temporal en este momento, deberás asignarle una manualmente después de crear el usuario. Para hacerlo, accede a la sección Administration y selecciona List users, donde podrás restablecer su contraseña.
 - **Password** (sólo se muestra cuando se marca la opción Set password): Esta contraseña temporal se deberá cambiar después del primer inicio de sesión. Asegúrese que la contraseña cumple con la política de contraseñas de MISP.

- **Confirm Password:** (sólo se muestra cuando se marca la opción Set password). Debe ser una copia exacta del campo Password.
- **Organization:** es una lista desplegable que le permite elegir una organización local para el usuario.
- **Role:** es una lista desplegable que permite seleccionar un rol de usuario. Los roles definen los privilegios atribuidos al usuario. Más adelante encontrará información acerca de estos roles.
- **Sync user for:** utilice esta opción para conceder al usuario el derecho a sincronizar el evento con el servidor MISP. Esta opción está disponible para los roles admin y Sync user.
- **PGP key:** la clave utilizada para cifrar los correos electrónicos enviados a través del sistema.
- **Fetch PGP key:** obtiene la clave pública PGP.
- **Receive email alerts when events are published:** esta opción suscribirá al nuevo usuario a correos electrónicos generados automáticamente cada vez que se publique un evento.
- **Receive email alerts from "Contact reporter" requests:** esta opción suscribirá al nuevo usuario a los correos electrónicos que se generen cuando otro usuario intente ponerse en contacto con la organización informante de un evento que coincida con la del nuevo usuario.
- **Immediately disable this user account:** esta opción desactiva esta cuenta de usuario (es preferible a eliminar una cuenta).
- **Send credentials automatically:** envía las credenciales del usuario creado al correo provisto.

Figura 38. Formulario de administración para añadir usuarios en MISP.

Admin Add User

Email

☐ Set password

Organisation

Choose organisation ▼

Rol

User ▼

NIDS SID

PGP key

Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

Fetch PGP key

☒ Receive email alerts when events are published

☒ Receive email alerts from "Contact reporter" requests

☐ Immediately disable this user account

☒ Send credentials automatically

Create user

Nota: Captura que muestra la sección “Admin Add User” en MISP.

3. Crear el usuario

Haz clic en el botón **Create user**.

Nota:

MISP incluye varios roles que puedes usar como referencia:

- **Admin:** Tiene control total sobre la instancia de MISP, incluyendo la gestión de usuarios, organizaciones y configuraciones globales.
- **Org Admin:** Posee permisos administrativos limitados a su propia organización, permitiéndole gestionar usuarios y eventos dentro de su entidad.
- **User:** Es el rol estándar que permite visualizar y crear eventos dentro de su organización, pero sin la capacidad de publicarlos para compartirlos externamente.
- **Publisher:** Además de las capacidades de un usuario estándar, tiene la habilidad de publicar eventos, haciéndolos visibles y compartibles con otras organizaciones o instancias de MISP.
- **Sync User:** Está autorizado para sincronizar eventos entre diferentes instancias de MISP, facilitando el intercambio de información entre servidores.

6.2.2. Cómo añadir un nuevo usuario

Para ver todos los usuarios de la instancia:

1. Abre la lista de usuarios

Dirígete a **Administration** y selecciona **List User**.

2. Abre la lista de usuarios

Veras una tabla de información como:

Figura 39. Listado de usuarios existentes en MISP.

The screenshot shows the 'Users index' page in MISP. It includes a search bar, filters for 'All', 'Enabled', 'Disabled', and 'Inactive', and a table of users. The table has columns for ID, Org, Role, Email, and various status indicators like TOTP, Contact Alert, Notifications, PGP public key, Terms accepted, NIDS SID, Last Login, Created, Last API Access, and Actions.

ID	Org	Role	Email	TOTP	Contact Alert	Notifications	PGP public key	Terms accepted	NIDS SID	Last Login	Created	Last API Access	Actions
1	ORNAME	admin	admin@admin.test	X	X	X	X	X	4000000	2024-11-19 21:12:39		X	

Nota: Captura que muestra la sección “List Users” en MISP.

- **ID:** Número de identificación único asignado automáticamente al usuario.

- **Org:** Organización a la que pertenece el usuario.
- **Role:** Rol del usuario dentro de la instancia.
- **Email:** Dirección de correo electrónico utilizada como nombre de inicio de sesión.
- **TOTP (Autenticación de doble factor):** Indica si el usuario tiene habilitada la autenticación de doble factor.
- **Contact Alert:** Muestra si el usuario recibe alertas cuando otro usuario intenta contactarlo.
- **Notifications:** Indica si el usuario está suscrito a las notificaciones automáticas del sistema.
- **PGP Public Key:** Muestra si el usuario ha configurado una clave PGP para comunicaciones cifradas.
- **NIDS SID:** Identificador único asociado a configuraciones específicas del Sistema de Detección de Intrusos (SID).
- **Terms Accepted:** Indica si el usuario ha aceptado los términos y condiciones de uso.
- **Last Login:** Fecha y hora del último inicio de sesión del usuario.
- **Created:** Fecha en la que se creó la cuenta del usuario.
- **Last API Access:** Fecha y hora del último acceso del usuario a la API del sistema.

3. Opciones de acción disponibles

En la columna **Actions**, puedes realizar las siguientes acciones para cada usuario.

Figura 40. Opciones de acción para usuarios en MISP.



Nota: Captura que muestra la sección “Actions” en MISP.

- **Reset Password:** Restablece la contraseña del usuario. Al seleccionar esta opción, se enviará un correo electrónico al usuario con instrucciones para establecer una nueva contraseña.
- **Edit User:** Permite modificar la información del usuario, incluyendo roles, organización y otros detalles.

- **Destroy sessions:** Desconecta al usuario de cualquier sesión activa en el sistema, útil en casos de seguridad.
- **Delete User:** Elimina la cuenta del usuario del sistema. Se recomienda deshabilitar la cuenta en lugar de eliminarla, para mantener registros históricos.
- **View User:** Muestra información detallada del perfil del usuario.

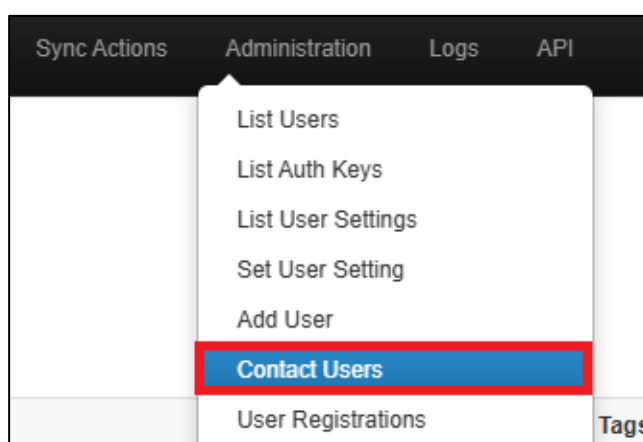
6.2.3. Contactar a un usuario

En MISP, los administradores tienen la capacidad de enviar correos electrónicos a usuarios específicos o a todos los usuarios registrados. Esto se realiza a través de la función **Contact Users**, disponible en el menú de administración. Los usuarios que tienen una clave PGP configurada recibirán sus correos electrónicos cifrados automáticamente. A continuación, los pasos para contactar a un usuario:

1. Accede a la función de contacto

- Ve al menú superior y selecciona **Administration**.
- Haz clic en **Contact Users**.

Figura 41. Función para contactar usuarios en MISP.



Nota: Captura que muestra la sección “Contact Users” en MISP.

2. Completa el formulario de contacto:

- **Action:** Selecciona el tipo de correo que deseas enviar:
 - Un mensaje personalizado.
 - Un mensaje de bienvenida.
 - Un correo para restablecer la contraseña.

- **Subject:** Introduce un asunto, especialmente si estás enviando un mensaje personalizado.
- **Recipient:** Especifica el destinatario:
 - Un usuario en particular.
 - Todos los usuarios registrados.
 - Todos los usuarios de una organización específica.
- **Message:** Escribe el contenido del correo.

Figura 42. Formulario para contactar usuarios en MISP.

Contact User(s)

Messaging - here's a quick guide on how this feature works

You can use this view to send messages to your current or future users or send them a temporary password.

- When adding a new user to the system, or when you want to manually reset the password for a user, just use the "Send" action.
- After selecting the action, choose who the target of the e-mails should be (all users, a single user or a user not yet in the system).
- You can then specify (if eligible) what the e-mail address of the target is (for existing users you can choose from a dropdown menu).
- In the case of a new user, you can specify the future user's PGP key, to send his/her new key in an encrypted e-mail.
- The system will automatically generate a message for you, but it is also possible to write a custom message if you tick the "Custom message" checkbox.

Action

Subject

Custom message ▼

Recipient

Recipient Email

A single user ▼

admin@admin.test ▼

Message

Enviar

Nota: Captura que muestra la sección "Contact Users" en MISP.

3. Enviar correo electrónico:

Haz clic en el botón **Enviar** o **Submit** para enviar el mensaje.

Nota:

Esta funcionalidad es útil para comunicarse rápidamente con usuarios en casos de actualizaciones críticas, instrucciones de seguridad o recordatorios.

6.3. Gestión de usuarios

6.3.1. Contactar a un usuario

MISP permite asignar diferentes roles a los usuarios según sus responsabilidades. Cada rol define un conjunto específico de permisos y niveles de acceso. A continuación, se describen los pasos para crear roles:

1. Accede al menú de roles:

Ve a **Administration** y selecciona **Add Role**.

2. Accede al menú de roles:

Introduce el nombre del rol y selecciona los permisos que se aplicarán:

Figura 43. Formulario para añadir roles en MISP.

Add Role

☐ Restrict to site admins

Name

Permissions

Manage and Publish Organisations ▼

Memory limit (2048M)

Maximum execution time (300s)

☐ Enforce search rate limit

☐ Site Admin

☐ Org Admin

☐ Sync Actions

☐ Audit Actions

☐ Auth key access

☐ Regex Actions

☐ Tagger

☐ Tag Editor

☐ Template Editor

☐ Sharing Group Editor

☐ Delegations Access

☐ Sighting Creator

☐ Object Template Editor

☐ Galaxy Editor

☐ Decaying Model Editor

☐ ZMQ publisher

☐ Kafka publisher

☐ Warninglist Editor

☐ View Feed Correlations

☐ Analyst Data Creator

☐ Skip OTP Reqs

Nota: Captura que muestra la sección “Add Role” en MISP.

A continuación, una explicación detallada de cada sección:

- **Nombre del Rol:** Asigna un nombre descriptivo que refleje las responsabilidades o permisos asociados al rol.

- **Permisos Básicos:** Selecciona los permisos que deseas otorgar al rol. MISP ofrece una variedad de permisos que puedes ajustar según las necesidades de tu organización.
 - **Read Only:** Permite a los usuarios visualizar eventos y atributos sin posibilidad de modificarlos.
 - **Manage Own Events:** Autoriza a los usuarios a crear, editar y eliminar eventos que ellos mismos han creado.
 - **Manage Organisation Events:** Faculta a los usuarios para gestionar eventos creados por cualquier miembro de su organización.
 - **Manage and Publish Organisation Events:** Además de gestionar, permite a los usuarios publicar eventos en nombre de su organización.

- **Permisos Avanzados:** Estos permisos están diseñados para roles específicos que requieren capacidades adicionales.
 - **Enforce search rate limit:** Limita la frecuencia de búsquedas para evitar el uso excesivo de recursos del sistema.
 - **Sync Actions:** Permite al usuario realizar operaciones de sincronización con otras instancias de MISP.
 - **Audit Actions:** Habilita el acceso a los registros de auditoría para monitorear las acciones realizadas en el sistema.
 - **Auth key access:** Permite al usuario generar y administrar claves de autenticación (API keys).
 - **Sighting Creator:** Autoriza al usuario a registrar avistamientos de atributos o eventos, útiles para análisis colaborativos.
 - **Decaying Model Editor:** Permite modificar modelos de decaimiento que controlan la relevancia de los atributos a lo largo del tiempo.
 - **View Feed Correlations:** Habilita la visualización de correlaciones derivadas de feeds, útil para análisis de eventos relacionados.
 - **Site Admin:** Concede privilegios administrativos completos sobre toda la instancia de MISP.
 - **Org Admin:** Otorga permisos de administración limitados a la propia organización del usuario.
 - **Regex Actions:** Permite al usuario crear y modificar reglas regex que afectan la validación de datos.
 - **Tagger:** Autoriza al usuario a asignar etiquetas a eventos y atributos.
 - **Tag Editor:** Habilita la creación, modificación y eliminación de etiquetas.

- **Template Editor:** Permite la creación y edición de plantillas para eventos.
- **Sharing Group Editor:** Autoriza la creación y gestión de grupos de compartición.
- **Delegations Access:** Facilita compartir o delegar acceso a datos con otras organizaciones.
- **Object Template Editor:** Permite la creación y edición de plantillas de objetos personalizados.
- **Galaxy Editor:** Habilita la edición de estructuras de datos en MISP para clasificar información.
- **ZMQ publisher:** Permite usar el protocolo ZeroMQ para publicar mensajes en tiempo real.
- **Kafka publisher:** Facilita la integración con Apache Kafka para transmitir datos en tiempo real.
- **Warninglist Editor:** Permite gestionar listas de advertencia que identifican información potencialmente no confiable.
- **Analyst Data Creator:** Autoriza a los usuarios a añadir datos analíticos en los eventos.
- **Skip OTP Reqs:** Exime al usuario de la autenticación de dos factores (OTP) al iniciar sesión.

3. Guarda el rol:

Una vez configurado, haz clic en **Enviar** o **Submit**.

6.3.2. Cómo listar roles

En MISP, puedes visualizar y gestionar los roles existentes mediante la opción **List Roles** en el menú de administración. Esta funcionalidad te permite identificar los permisos habilitados para cada rol y realizar acciones específicas, como editar o eliminar roles. A continuación, se describen los pasos para listar roles:

1. Accede al listado de roles:

- Dirígete al menú superior y selecciona **Administration**.
- Haz clic en **List Role**.

2. Accede al menú de roles:

Al cargar la vista, se mostrará una tabla con todos los roles registrados en el sistema. Cada fila representa un rol y contiene la siguiente información clave.

Figura 44. Listado de roles en MISP.

Roles

Instance specific permission roles.

< anterior

siguiente >

+ Add role

Enter value to search

Filter

ID	Default	Nombre	Permission	Site Admin	Org Admin	Sync Actions	Audit Actions	Auth key access	Regex Actions	Tagger	Template Editor	Sharing Group Editor	Delegations Access	Signing Creator	Object Template Editor	Galaxy Editor	Decryption Model Editor	ZMQ publisher	Kafka publisher	Verminator Editor	View Feed Correlations	Analysis Data Creator	Site OTP Range	Memory Limit	Max execution time	Searches / 15 mins	Acciones
1	☐	admin	Manage and Publish Organisation Events	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2048M	300 s	Unlimited	
2	☐	Org Admin	Manage and Publish Organisation Events	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	2048M	300 s	Unlimited	
3	☒	User	Manage Organisation Events	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	2048M	300 s	Unlimited		
4	☐	Publisher	Manage and Publish Organisation Events	✗	✗	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	2048M	300 s	Unlimited		
5	☐	Sync user	Manage and Publish Organisation Events	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	2048M	300 s	Unlimited	
6	☐	Read Only	Read Only	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	2048M	300 s	Unlimited		

Nota: Captura que muestra la sección “Roles” en MISP.

- **Id:** número de identificación asignado automáticamente al rol.
- **Name:** nombre del rol.
- **Permission:** uno de los 4 permisos (**Read Only**, **Manage Own Events**, **Manage Organisation Events** y **Manage and Publish Organisation Events**).
- **Banderas de permisos Extra** (bandera para cada uno de los permisos extra). Algunos son los siguientes:

- **Site Admin:** brinda al usuario privilegios completos de administrador, esta configuración se utiliza para los administradores del sitio.
- **Org Admin:** brinda al usuario privilegios de administrador limitados, esta configuración se utiliza para los administradores de una organización.
- **Sync Actions:** permite utilizar a los usuarios del rol como usuarios de sincronización.
- **Audit Actions:** permite el acceso a los logs. A excepción de los administradores del sitio, sólo son visibles los logs generados por la propia organización del usuario.
- **Regex Actions:** los usuarios con este permiso pueden modificar las reglas regex que afectan cómo se introducen los datos en el MISP. Se recomienda tener mucho cuidado al dar este permiso, las expresiones regulares ejecutadas por el usuario pueden ser muy perjudiciales (para más información acerca de las reglas regex, visite el siguiente [enlace](#)).
- **Tagger:** permite al usuario asignar etiquetas a los eventos.
- **Tag Editor:** permite a los usuarios crear, modificar o eliminar etiquetas.
- **Template Editor:** permite crear o modificar las plantillas que se utilizarán para rellenar los eventos.

- **Sharing Group Editor:** concede acceso para editar o crear sharing groups.

En la columna Actions, encontrarás las siguientes opciones para cada rol:

- **Editar rol:** Permite modificar los permisos y configuraciones del rol.
- **Eliminar rol:** Borra el rol del sistema (se requiere desvincularlo previamente de todos los usuarios asignados).

Nota:

Configura con cuidado permisos avanzados como Regex Actions o Sync Actions, ya que pueden afectar significativamente el comportamiento del sistema.

6.4. Gestión de organizaciones

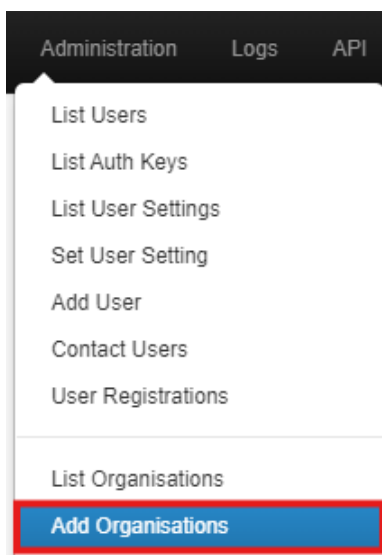
6.4.1. Cómo añadir una nueva organización

Para agregar una nueva organización:

1. Accede al menú de organizaciones:

Ve a **Administration** y selecciona **Add Organisation**.

Figura 45. Menú para añadir una nueva organización en MISP.



Nota: Captura que muestra la sección “Add Organisation” en MISP.

2. Completa el formulario:

Figura 46. Formulario para añadir una nueva organización en MISP.

Mandatory Fields

☒ Local organisation

If the organisation should have access to this instance, make sure that the Local organisation setting is checked. If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Organisation Identifier

UUID

Optional Fields

A brief description of the organisation

Bind user accounts to domains (line separated)

Logo (48x48 PNG)

Sin archivos seleccionados

Nationality

Sector

Type of organisation

Contact details

Nota: Captura que muestra la sección “Add Organisation” en MISP.

- **Local Organisation:** si la organización debe tener acceso a esta instancia, marque la casilla. Si solo desea añadir una organización externa conocida para incluirla en los sharing groups, desmarque la casilla.
- **Organisation Identifier:** nombre de su organización.
- **UUID:** identificador único de la organización.
- **A brief description of the organisation:** Duna breve descripción de la organización.
- **Bind user accounts to domains (line separated):** Esta opción se utiliza para restringir la creación de cuentas de usuario en una organización a correos electrónicos que pertenezcan a dominios específicos definidos.
- **Nationality:** lista desplegable para seleccionar el país de la organización
- **Sector:** el sector de la organización (financiero, transporte, telecomunicaciones, entre otras).
- **Type of organisation:** el tipo de organización.
- **Contact details:** puede añadir algunos datos de contacto de la organización.

3. Filtra las organizaciones:

Haz clic en Enviar o Submit para finalizar.

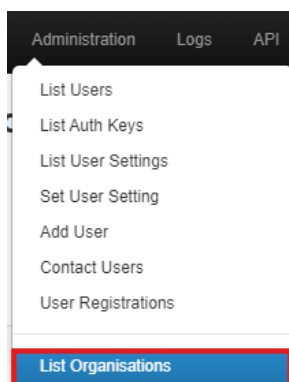
6.4.2. Cómo listar organizaciones

En MISP, puedes visualizar y gestionar todas las organizaciones registradas en el sistema a través de la función **List Organisations**. Esta herramienta permite identificar las organizaciones locales y remotas, y realizar acciones específicas sobre ellas. A continuación, describen paso a paso para listar las organizaciones.

1. Accede al listado de organizaciones:

- En el menú superior, selecciona **Administration**.
- Haz clic en **List Organisations**.

Figura 47. Menú para listar organizaciones en MISP.



Nota: Captura que muestra la sección “List Organisations” en MISP.

2. Filtra las organizaciones:

En la parte superior de la vista, encontrarás tres pestañas:

Figura 48. Opciones para filtrar organizaciones en MISP.



Nota: Captura que muestra la sección “Local organisations, both local and remote” en MISP.

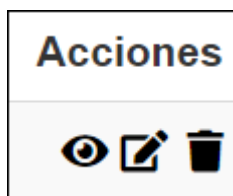
- **Local:** Muestra únicamente las organizaciones configuradas como locales.
- **Remote:** Muestra las organizaciones remotas, relacionadas con otras instancias de MISP.
- **All:** Muestra tanto las locales como las remotas.

Cada fila de la tabla representa una organización y contiene los siguientes campos clave:

- **ID:** Es el identificador único asignado automáticamente a cada organización dentro de la instancia de MISP. Facilita la referencia y gestión de organizaciones.
- **Name:** Muestra el nombre de la organización. Este nombre es utilizado para identificar la organización dentro del sistema.
- **UUID (Universally Unique Identifier):** Es un identificador único asignado a la organización que sirve para distinguirla de otras en diferentes instancias de MISP. Es crucial para sincronización entre múltiples sistemas.
- **Description:** Contiene una breve descripción de la organización, la cual puede incluir su propósito o rol en la plataforma. Por ejemplo, en este caso, "Automatically generated admin organisation" indica que es una organización generada automáticamente para administradores.
- **Nationality:** Especifica el país asociado a la organización, si se ha configurado. Este dato puede ser útil para fines de clasificación y análisis.
- **Sector:** Indica el sector al que pertenece la organización (por ejemplo, financiero, telecomunicaciones, gubernamental). Si no se ha configurado, aparece como vacío.

- **Type:** Describe el tipo de organización. En este caso, "ADMIN" indica que se trata de una organización con fines administrativos.
- **Contacts:** Proporciona información de contacto asociada a la organización. Si no se ha especificado ningún contacto, el campo permanecerá vacío.
- **Added by:** Indica el usuario que creó o añadió la organización al sistema. En este caso, "Unknown" sugiere que no se registró el usuario que la creó, probablemente porque fue generada automáticamente.
- **Local:** Este campo indica si la organización es local a la instancia de MISP o si se trata de una organización remota sincronizada desde otra instancia.
- **Users:** Muestra la cantidad de usuarios asociados a la organización dentro de la instancia de MISP.
- **Restrictions:** Este campo puede contener restricciones o políticas específicas aplicadas a la organización, como limitaciones en la sincronización. En este caso, no se muestra ninguna restricción.
- **Actions:** Contiene las acciones que puedes realizar para cada organización:
 - **Ver:** Permite visualizar detalles completos de la organización.
 - **Editar:** Permite modificar los datos de la organización.
 - **Eliminar:** Elimina la organización de la instancia (requiere confirmación).

Figura 49. Opciones de acciones para organizaciones en MISP.



Nota: Captura que muestra la sección “Actions” en MISP.



SINCRONIZACIÓN DE INSTANCIAS

7.1. Introducción

A continuación, se definirán conceptos necesarios para entender el presente capítulo:

7.1.1. Servidor de Sincronización

Es una instancia de MISP configurada para facilitar el intercambio de datos entre servidores. Este servidor actúa como un punto de conexión que permite sincronizar eventos, atributos y actualizaciones relevantes entre diferentes organizaciones o comunidades. El servidor de sincronización utiliza claves de autenticación y usuarios con permisos específicos para garantizar la seguridad y el control del flujo de información.

7.1.2. Grupos de intercambio (Sharing Groups)

Conjunto de organizaciones o instancias que tienen acceso a eventos y atributos específicos en MISP. Los grupos de intercambio permiten gestionar la visibilidad y el acceso a la información de manera controlada, asegurando que solo las partes autorizadas tengan acceso a ciertos eventos.

7.1.3. Authkey (Clave de autenticación)

Código único utilizado para autenticar de manera segura las comunicaciones entre servidores MISP durante la sincronización. La clave de autenticación garantiza que los servidores puedan intercambiar datos de forma confiable y protegida.

7.2. Sincronización entre dos instancias de MISP

En este ejemplo, se tendrán dos países, denominados País A y País B, cada uno con su respectivo Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT). Actualmente, ambos operan de manera independiente y no cuentan con una conexión o mecanismo de intercambio de información entre sí. El objetivo es establecer una sincronización utilizando la plataforma MISP.

Nota:

Es importante considerar que, además de la configuración a nivel de aplicación en MISP, puede ser necesario ajustar las reglas de los firewalls en ambas instancias para permitir la conectividad adecuada.

La siguiente imagen ilustra dos instancias de MISP correspondientes a cada país. Cada una cuenta con una organización local denominada CSIRT País A y CSIRT País B, respectivamente.

Figura 50. Sincronización entre dos instancias de MISP.



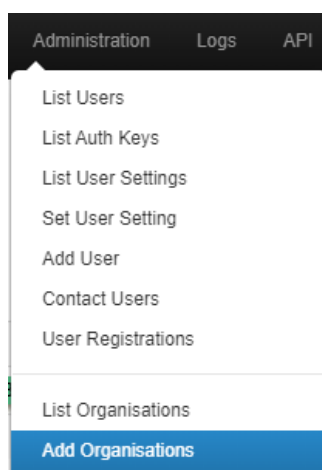
Nota: Captura que muestra el esquema de sincronización entre las instancias “Nodo País A” y “Nodo País B” en MISP.

Para este ejemplo, se generará un servidor de sincronización en la instancia del País A, por lo que los siguientes pasos deberán ser ejecutados en la instancia del País B.

7.2.1. Crear una organización local

- En la **Instancia País B** se deberá dirigir a la sección **Administration** y seleccionar **Add Organisations**.

Figura 51. Menú para añadir una nueva organización en MISP.



Nota: Captura que muestra la sección “Add Organisations” en MISP.

Sincronización de Instancias MISP

- Deberá completar el siguiente formulario.

Figura 52. Formulario para crear una organización local en MISP.

Mandatory Fields

☒ Local organisation

If the organisation should have access to this instance, make sure that the Local organisation setting is checked. If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Organisation Identifier

UUID

Optional Fields

A brief description of the organisation

Bind user accounts to domains (line separated)

Logo (48×48 PNG)

Sin archivos seleccionados

Nationality

Sector

Type of organisation

Contact details

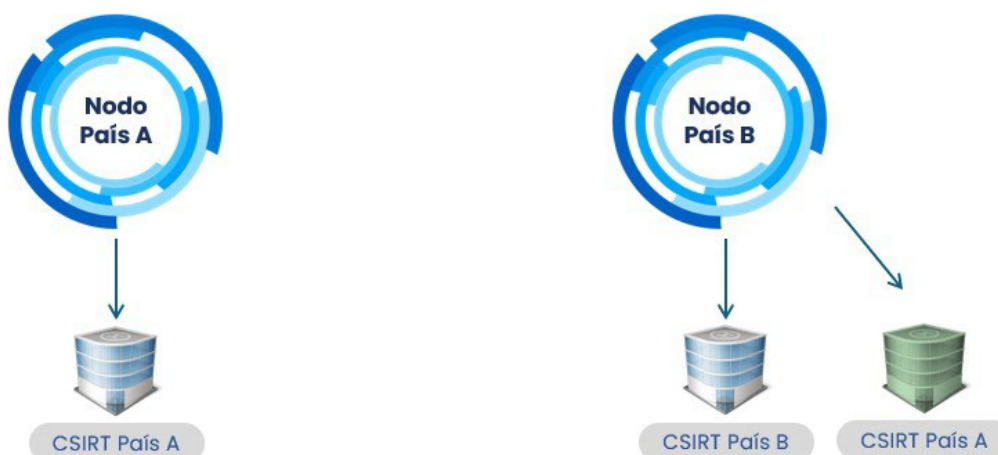
Nota: Captura que muestra la sección “Local Organisation” en MISP.

- Deberá estar seleccionado el checkbox **Local Organisation**.
- Deberá ingresar el nombre de la organización de la otra instancia (Instancia País A) en el campo **Organisation Identifier**. Para este ejemplo, se ingresará CSIRT País A.
- Deberá introducir el **identificador único** (UUID) de la organización con la que se desea sincronizar (CSIRT País A). No deberá presionar el botón "Generate UUID".
- Deberá hacer clic en **Submit** para guardar los cambios.

Nota:

Los datos del nombre de la organización y del identificador único deberán haberse solicitado previamente mediante correo, mensaje u otro medio.

Figura 53. Proceso de creación de una organización local en MISP.

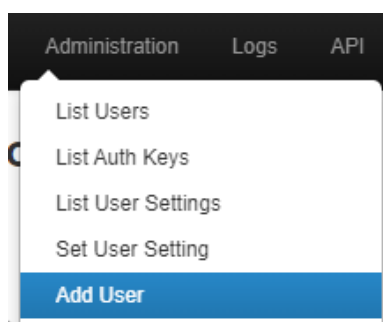


Nota: Captura que muestra el esquema de sincronización y la creación de una organización local en la instancia “País B” en MISP.

7.2.2. Crear un usuario de sincronización (Sync User)

- En la Instancia País B, se deberá dirigir a la sección **Administration** y seleccionar **Add User**.

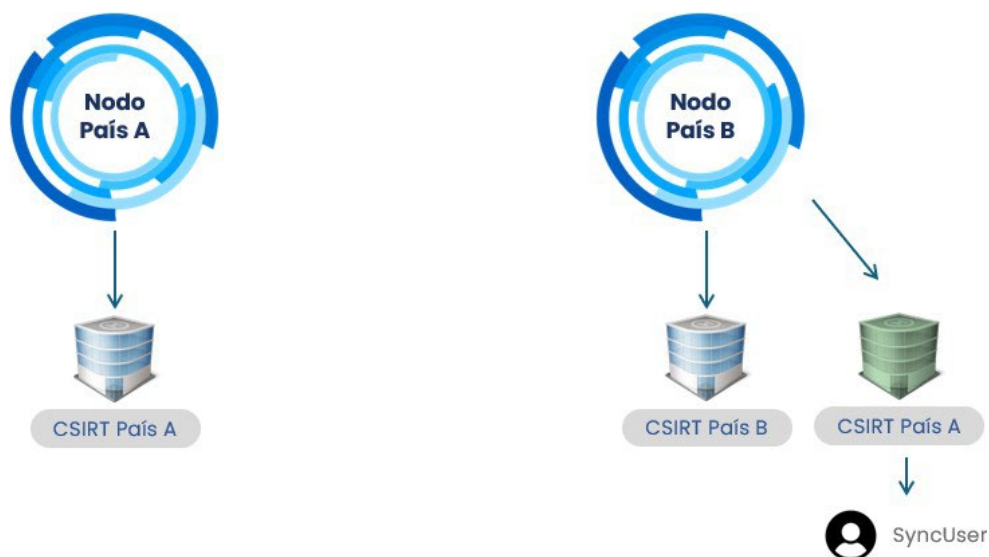
Figura 54. Menú para crear un usuario de sincronización en MISP.



Nota: Captura que muestra la sección “Add User” en MISP.

- Complete el formulario con la siguiente información:
 - **Email:** Introduzca un correo identificativo, por ejemplo: syncuser@paisb.server.
 - **Contraseña:** Cree una contraseña segura para este usuario.
 - **Organización:** Seleccione la organización configurada en el paso anterior (CSIRT País A).
 - **Rol:** Asigne el rol de Sync User a esta cuenta.

Figura 55. Usuario de sincronización entre nodos en MISP.



Nota: Captura que muestra el esquema de sincronización con el usuario “SyncUser” entre las instancias de los nodos País A y País B en MISP.

- Haga clic en **Create user** para guardar la nueva cuenta

Nota:

Este usuario será responsable de gestionar las comunicaciones entre servidores. Es fundamental que las credenciales de esta cuenta se mantengan en estricta confidencialidad.

Figura 56. Formulario para crear un usuario de sincronización en MISP.

Admin Add User

Email

syncuser@paisb.server

☒ Set password

Password ⓘ

.....

Confirm Password

.....

Organisation

CSIRT Pais A ▼

Role

Sync user ▼

NIDS SID

Sync user for

Not bound to a server ▼

PGP key

Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

Fetch PGP key

☒ Receive email alerts when events are published
☒ Receive email alerts from "Contact reporter" requests
☐ Immediately disable this user account
☒ Send credentials automatically

Create user

Nota: Captura que muestra la sección “Admin Add User” con el rol “Sync User” en MISP.

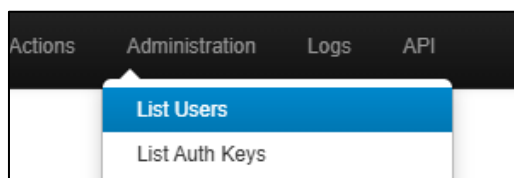
7.2.3. Crear la llave de autenticación

Para generar una clave de autenticación, existen dos caminos según el perfil utilizado:

1. Desde el perfil del administrador:

- Acceda a la sección **Administration** y seleccione **List Users**

Figura 57. Acceso al listado de usuarios en MISP.



Nota: Captura que muestra la sección “List Users” en MISP.

- Localice el usuario de sincronización (Sync User) creado previamente.

Figura 58. Usuario de sincronización en el listado de usuarios en MISP.

Org	Role	Email
CSIRT País A	Sync user	syncuser@paisb.server

Nota: Captura que muestra el usuario “Sync User” asociado a “CSIRT País A” en MISP.

- Haga clic en **View** en la columna de acciones para acceder al perfil del usuario.

Figura 59. Opciones de acciones para usuarios en MISP.



Nota: Captura que muestra la sección “Actions” con la opción “View” resaltada en MISP.

Sincronización de Instancias MISP

- En la sección **Auth Keys**, seleccione **Add authentication key** y genere la clave.

Figura 60. Perfil del usuario de sincronización en MISP.

User syncuser@paisb.server

ID	6
Email	syncuser@paisb.server
Organisation	CSIRT País A
Role	Sync user
TOTP	No
Email notifications	Event published notification Yes Daily notifications No Weekly notifications No Monthly notifications No
Contact alert enabled	Yes
Invited By	admin@admin.test
Org admin	
NIDS Start SID	4929819
Terms accepted	Yes
Must change password	No
PGP key	No
Created	2024-12-06 12:35:30
Last password change	2024-12-06 12:35:30
News read at	N/A
Disabled	No

Download user profile for data portability
Review user logs
Review user logins

Auth keys

Nota: Captura que muestra la sección del perfil del usuario “Sync User” con la opción “Auth keys” en MISP.

Figura 61. Gestión de claves de autenticación en MISP.

Auth keys

« previous next »

+ Add authentication key

#	User	Auth Key	Expiration
Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0			

« previous next »

Nota: Captura que muestra la sección “Auth keys” con la opción “Add authentication key” en MISP.

- Luego, seleccionaremos el botón **Submit** y tendremos la llave de autenticación.

Figura 62. Configuración de claves de autenticación en MISP.

Add auth key

Auth keys are used for API access. A user can have more than one authkey, so if you would like to use separate keys per tool that queries MISP, add additional keys. Use the comment field to make identifying your keys easier.

User

syncuser@paisb.server

Comment

Allowed IPs

Expiration (keep empty for indefinite)

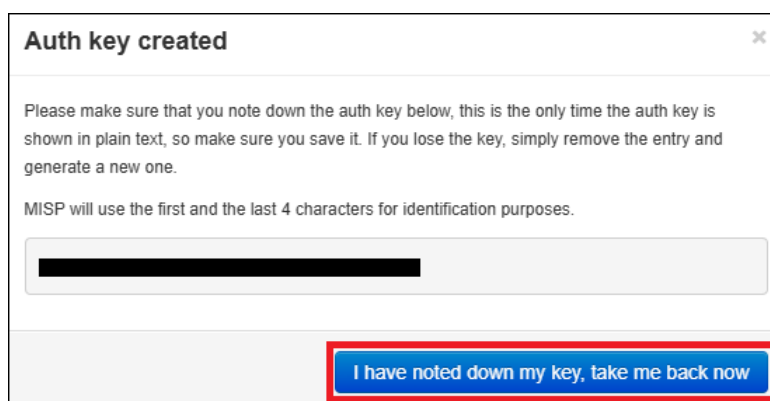
YYYY-MM-DD

☐ Read only (it will unset all permissions. This should not be used for sync users)

Submit Cancel

Nota: Captura que muestra la sección “Add auth key” en MISP.

Figura 63. Confirmación de clave de autenticación en MISP.

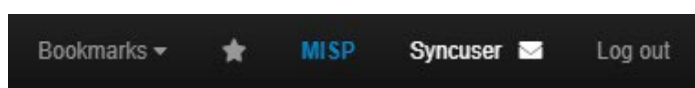


Nota: Captura que muestra la sección “Auth key created” en MISP.

2. Desde el perfil del usuario de sincronización (Sync User):

- Inicie sesión con las credenciales del usuario de sincronización (Sync User).

Figura 64. Perfil de usuario Sync User en MISP.



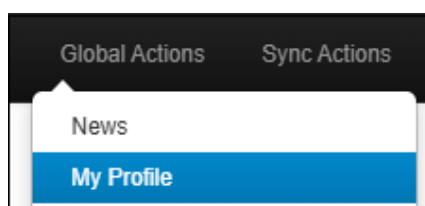
Nota: Captura que muestra la sección del usuario Sync User en MISP.

Nota:

Se dará cuenta que está en el usuario Sync User ya que en la parte superior derecha aparecerá el rol del usuario.

- Acceda a la opción **My Profile** desde el menú **Global Actions**.

Figura 65. Acceso a My Profile en MISP.



Sincronización de Instancias MISP

Nota: Captura que muestra la opción “My Profile” en el menú “Global Actions” en MISP.

- En la sección **Auth Keys**, seleccione **Add authentication key** y genere la clave.

Figura 66. Perfil de usuario en MISP.

User syncuser@paisb.server

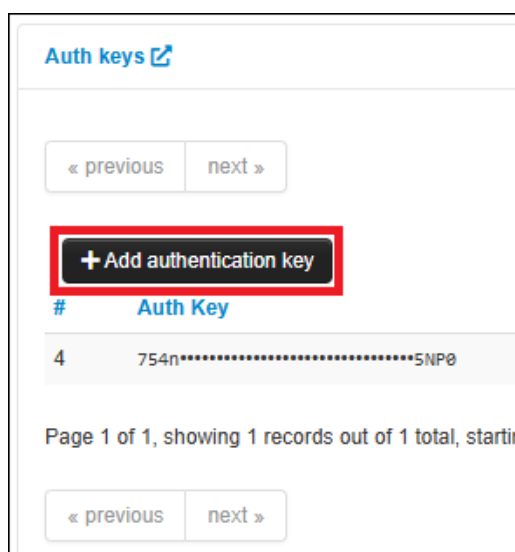
ID	6
Email	syncuser@paisb.server
Organisation	CSIRT País A
Role	Sync user
TOTP	No Generate
Email notifications	Event published notification Yes
	Daily notifications No
	Weekly notifications No
	Monthly notifications No
Contact alert enabled	Yes
Invited By	N/A
NIDS Start SID	4929819
PGP key	No
Created	2024-12-06 12:35:30
Last password change	2024-12-06 12:35:30

Download user profile for data portability
Review user logs
Review user logins

Auth keys [↗](#)

Nota: Captura que muestra el perfil de usuario con la opción “Auth keys” en MISP.

Figura 67. Gestión de claves de autenticación en MISP.



Auth keys [↗](#)

« previous next »

+ Add authentication key

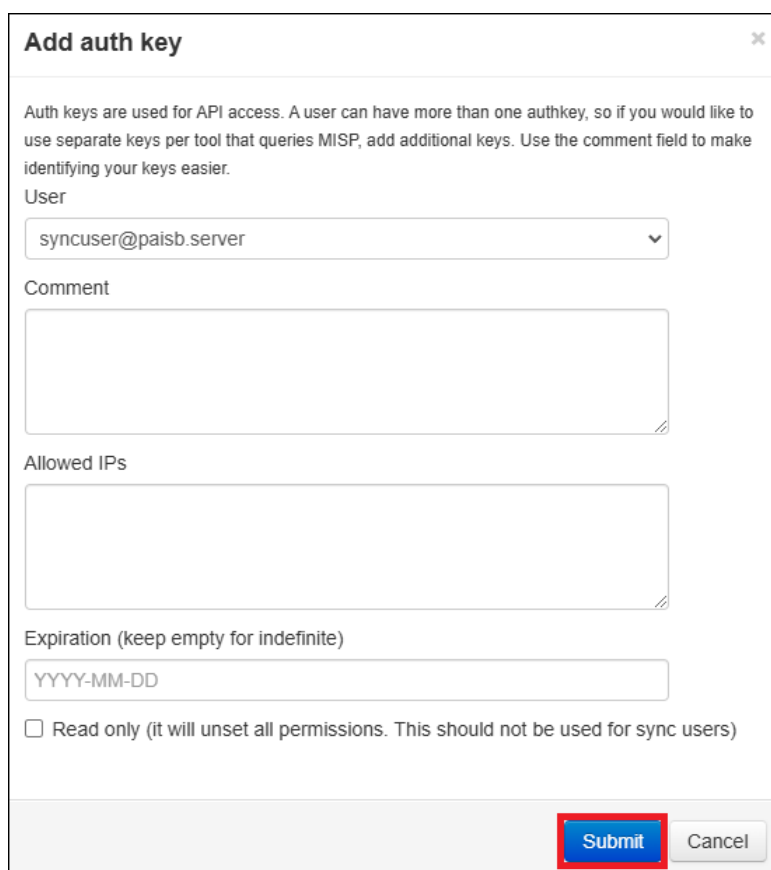
#	Auth Key
4	754n.....SNP0

Page 1 of 1, showing 1 records out of 1 total, starting

« previous next »

Nota: Captura que muestra la opción “Add authentication key” en la sección “Auth keys” en MISP.

Figura 68. Ventana para agregar clave de autenticación en MISP.



Add auth key ✕

Auth keys are used for API access. A user can have more than one authkey, so if you would like to use separate keys per tool that queries MISP, add additional keys. Use the comment field to make identifying your keys easier.

User

syncuser@paisb.server ▼

Comment

Allowed IPs

Expiration (keep empty for indefinite)

YYYY-MM-DD

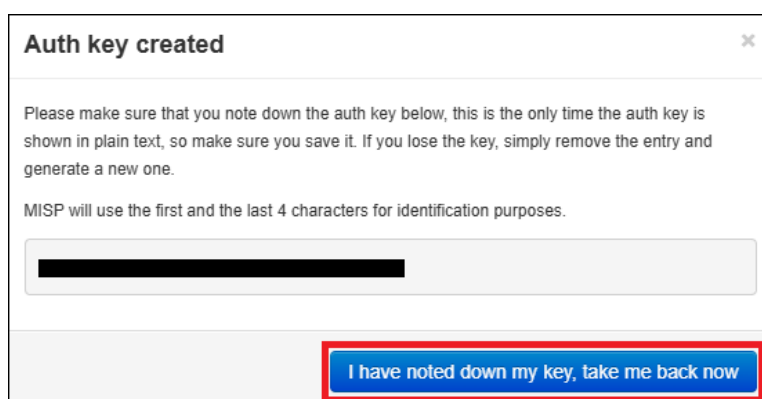
☐ Read only (it will unset all permissions. This should not be used for sync users)

Submit Cancel

Nota: Captura que muestra el formulario “Add auth key” con el botón “Submit” en MISP.

- Seleccionaremos el botón **Submit** y tendremos la llave de autenticación.

Figura 69. Clave de autenticación creada en MISP.



Auth key created

Please make sure that you note down the auth key below, this is the only time the auth key is shown in plain text, so make sure you save it. If you lose the key, simply remove the entry and generate a new one.

MISP will use the first and the last 4 characters for identification purposes.

[Masked Auth Key]

I have noted down my key, take me back now

Nota: Captura que muestra la confirmación “Auth key created” en MISP.

Nota:

La clave de autenticación se mostrará una sola vez. Asegúrese de guardarla en un lugar seguro. Si la pierde, puede generar una nueva.

7.2.4. Recopilar y enviar la información

Método manual

1. **Obtener el nombre de la organización y su UUID.**
 - Acceda a **Administration** → **List Organizations**
 - Localice la organización con **ID = 1**, ya que esta es la primera organización creada en MISP por defecto.
 - Copie el **nombre de la organización** y su **UUID**
2. **Enviar la información**

Sincronización de Instancias MISP

- Comparta estos datos junto con la AuthKey del usuario de sincronización con el administrador de la otra instancia.

Figura 70. Vista general de la organización local



ID	Name	UUID	Des
2	CSIRT País A	80b808f7-e188-4266-a8b7-23163b68ed55	
1	ORGNAME	09bd2f79-7ee2-4ba6-a2f5-1a026da4bd74	Auto

Nota: Captura que muestra la vista de “List Organizations”

Método automático

1. Acceder al usuario de sincronización

- Inicie sesión con el usuario de sincronización previamente configurado.

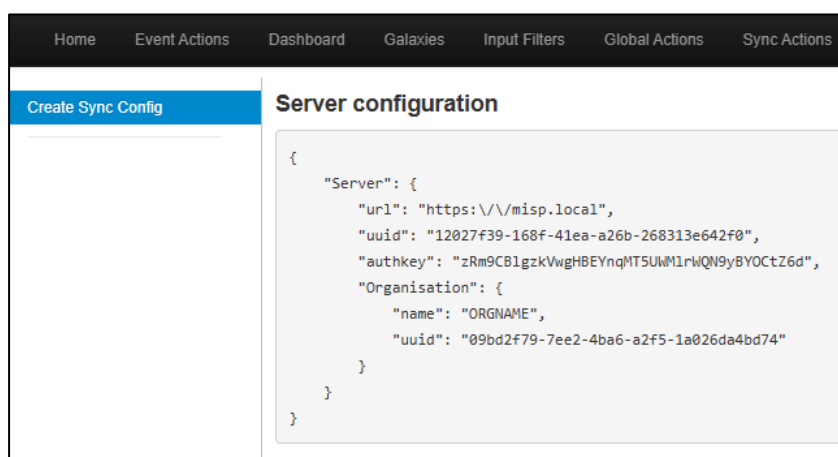
2. Generar la configuración de sincronización

- Vaya a **Sync Actions** → **Create Sync Config**.
- Copie la información generada en el formato JSON.

3. Compartir la configuración

- Envíe el JSON generado al administrador de la otra instancia para su integración.

Figura 71. Vista general del JSON Sync User



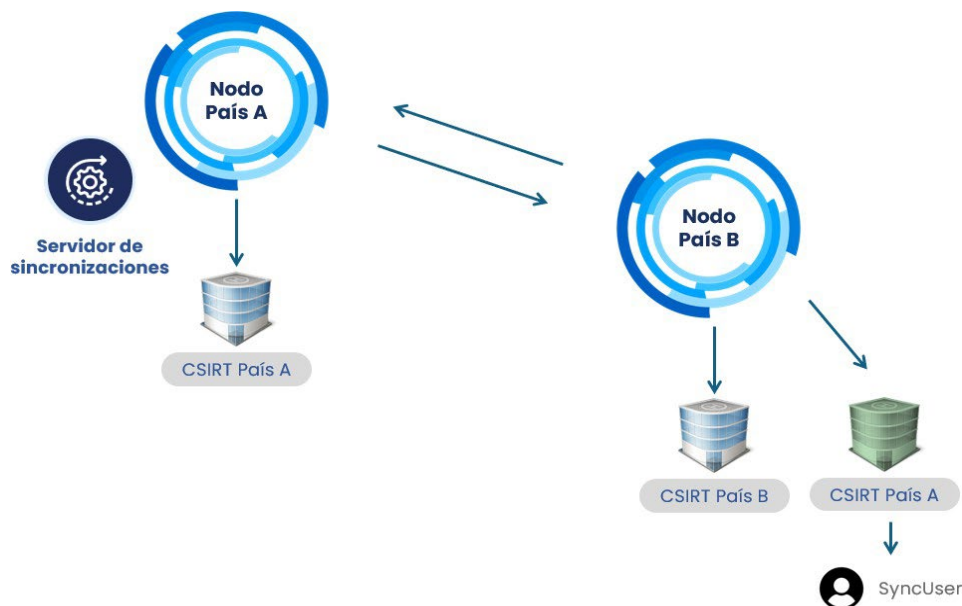
Home	Event Actions	Dashboard	Galaxies	Input Filters	Global Actions	Sync Actions
Create Sync Config Server configuration <pre>{ "Server": { "url": "https://misp.local", "uuid": "12027f39-168f-41ea-a26b-268313e642f0", "authkey": "zRm9C81gzkVwGHBEYnqMT5UwM1rWQ9yBYOCtZ6d", "Organisation": { "name": "ORGNAME", "uuid": "09bd2f79-7ee2-4ba6-a2f5-1a026da4bd74" } } }</pre>						

Nota: Captura que muestra la vista de Sync User

7.2.5. Configurar el servidor de sincronización en la Instancia País A

Con la clave de autenticación generada en la **Instancia País B**, el siguiente paso es configurar la **Instancia País A** para establecer la sincronización entre ambas instancias.

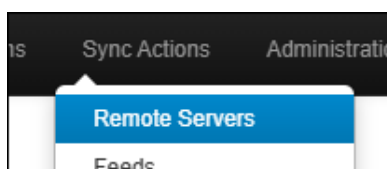
Figura 72. Configuración del servidor de sincronización en MISP.



Nota: Diagrama que muestra la sincronización entre las instancias País A y País B en MISP.

1. Acceda a la sección **Sync Actions** en la **Instancia País A** y seleccione la opción **Remote Servers**.

Figura 73. Acceso a Remote Servers en MISP.

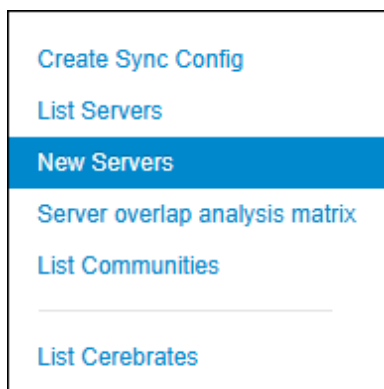


Nota: Captura que muestra la opción "Remote Servers" en el menú "Sync Actions" en MISP.

Sincronización de Instancias MISP

- Haga clic en **New Server** para agregar un nuevo servidor remoto.

Figura 74. Selección de New Server en MISP.



Nota: Opción “New Server” en MISP.

- Complete el formulario con la siguiente información.
 - URL del servidor remoto:** Introduzca la URL del **Instancia País B**, por ejemplo, `https://[Ingrese URL]`.
 - Nombre de Instancia:** Asigne un nombre descriptivo al servidor, como **Instancia País B**.
 - Tipo de Organización:** Seleccione “New external organization” e ingrese los datos del Nombre de la organización remota (CSIRT País B) y el UUID.
 - Clave de autenticación:** Pegue la clave de autenticación generada en el perfil del **Sync User** de la **Instancia País B**.
- Active las opciones **Push** y **Pull** para habilitar el intercambio bidireccional de eventos y atributos entre los servidores.
- Habilite “Allow self-signed certificates” (opcional):

Si el servidor remoto utiliza un certificado autofirmado o si los certificados válidos no están disponibles o se han vencido, marque la casilla **Allow self-signed certificates (unsecure)** para permitir la sincronización temporalmente.

Nota:

El uso de certificados autoafirmados puede reducir la seguridad del canal de comunicación entre las instancias. Utilice esta opción solo como medida temporal y asegúrese de implementar certificados válidos tan pronto como sea posible para mantener la seguridad y autenticidad de las comunicaciones.

Sincronización de Instancias MISP

- Haga clic en **Submit** para guardar los cambios.

Figura 75. Configuración de servidor en MISP.

Add Server

Instance identification

Base URL

Instance name

Instance ownership and credentials

Information about the organisation that will receive the events, typically the remote instance's host organisation.

Organisation Type

Remote Organisation's Name

Remote Organisation's UUID

New external organisation ▼

Ask the owner of the remote instance for a sync account on their instance, log into their MISP using the sync user's credentials and actions -> My profile. This key is used to authenticate with the remote instance.

Authkey

Enabled synchronisation methods

☒ Push
 ☒ Pull
 ☐ Push Sightings
 ☐ Caching Enabled
 ☐ Push Galaxy Clusters
 ☐ Pull Galaxy Clusters

Misc settings

☐ Unpublish event when pushing to remote server
 ☐ Publish Without Email
 ☒ Allow self signed certificates (unsecure)
 ☐ Skip proxy (if applicable)
 ☐ Remove Missing Attribute Tags (not recommended)

Server certificate file (*.pem): Not set.

Client certificate file: Not set.

Push rules:

Pull rules:

Nota: Formulario “Add Server” en MISP.

Nota:

Los métodos de sincronización Push y Pull son esenciales al configurar un servidor en MISP:

- Push: Envía eventos desde la instancia local a una instancia remota, compartiendo información dentro de los límites de distribución establecidos.
- Pull: Obtiene datos de una instancia remota y los almacena localmente, garantizando que la información compartida esté actualizada.

Activar ambos métodos permite un intercambio bidireccional de datos, facilitando la colaboración y asegurando que las instancias compartan y reciban información relevante para la gestión de amenazas cibernéticas.

7. Navegue a **List Servers** para confirmar que el servidor remoto se haya agregado exitosamente.
8. Ejecute un “test de sincronización” haciendo clic en **Run**.

Figura 76. Lista de servidores en MISP

Servers										
« previous		next »								
ID	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push	Pull	Push Sightings	
4	Instancia País B	⬆️ ⬆️	Run	View	Reset x	✓	✓	✓	x	

Nota: Opción “Run” en la sección “List Servers” en MISP.

Figura 77. Resultados de prueba de conexión en MISP.

Servers							
« previous		next »					
ID	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push
4	Instancia País B		Local version: 2.4.198 Remote version: 2.4.198 Status: OK Compatibility: Compatible POST test: Received sent package	View	Reset	x	✓

Nota: Estado de conexión en la sección “Servers” en MISP.

7.2.6. Verificación de la Sincronización

Una vez configuradas ambas instancias, es importante verificar que los eventos y atributos se están sincronizando correctamente entre los servidores. Siga estos pasos para realizar la verificación.

- En la **Instancia País A**, cree un evento de prueba:
 - Diríjase a la sección de eventos y seleccione **Add Event**.
 - Asigne un nivel de distribución adecuado para que sea accesible desde la **Instancia País B**.
 - Guarde el evento.
- En la **Instancia País B**, verifique que el evento de prueba creado en la **Instancia País A** aparezca en la lista de eventos (Eso se realizará de manera automática, solo si activó las opciones de **Push**):
 - Acceda a la lista de eventos y localice el evento creado desde la **Instancia País A**.
 - Confirme que los atributos y datos del evento se reflejen correctamente.
- Repita el proceso a la inversa:
 - Cree un evento de prueba en la **Instancia País B** siguiendo el mismo procedimiento.
 - Verifique que este evento sea visible en la **Instancia País A**.
- Compruebe la sincronización de atributos y actualizaciones:
 - Realice cambios en los atributos de los eventos de prueba desde una instancia.
 - Verifique que los cambios se reflejen correctamente en la otra instancia.

Sugerencia:

Si los eventos o atributos no se sincronizan correctamente, revise las configuraciones de los servidores y las claves de autenticación. Consulte los logs de ambas instancias para identificar posibles errores o problemas de conectividad.

7.3. Modelos de Intercambio de información

7.3.1. Solo tu organización (Your organisation only)

Este modelo de intercambio restringe el acceso a los eventos y atributos exclusivamente a la organización que los creó. Los datos no son visibles para organizaciones externas ni locales, incluidas aquellas conectadas a la misma instancia o servidor de MISP.

Características:

- **Alcance limitado:** Solo los miembros de la organización creadora pueden ver y gestionar el evento.
- **Uso recomendado:** Ideal para información altamente sensible que no debe compartirse más allá de la organización.
- **Restricciones de acceso:** Las organizaciones locales afiliadas (como socios o suborganizaciones) y las instancias remotas quedan excluidas del acceso.

Figura 78. Modelo de intercambio "Solo tu organización" en MISP.



Nota: Diagrama que muestra el alcance del modelo "Your organisation only" en MISP.

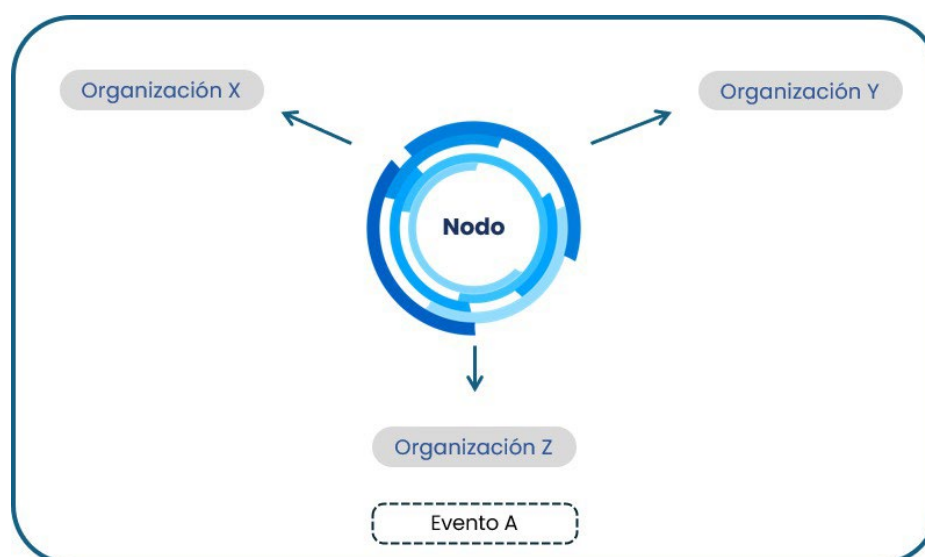
7.3.2. Solo tu comunidad (This community only)

Este modelo permite compartir eventos y atributos exclusivamente con organizaciones que pertenecen a la misma comunidad definida dentro del servidor de MISP. No se permite el acceso a nodos u organizaciones fuera de esta comunidad, a menos que haya configuraciones específicas.

Características

- **Alcance comunitario:** Los datos se comparten solo dentro de nodos comunitarios locales (por ejemplo, un nodo regional o nacional).
- **Limitación del método Push:** Las organizaciones externas no pueden recibir eventos automáticamente mediante Push. Sin embargo, pueden obtener datos a través de Pull, si así se configura.
- **Uso recomendado:** Adecuado para compartir información dentro de un entorno colaborativo confiable, como un grupo regional o sectorial.

Figura 79. Modelo de intercambio "Solo tu comunidad" en MISP.



Nota: Diagrama que muestra el alcance del modelo "This community only" en MISP.

7.3.3. Comunidades conectadas (Connected communities)

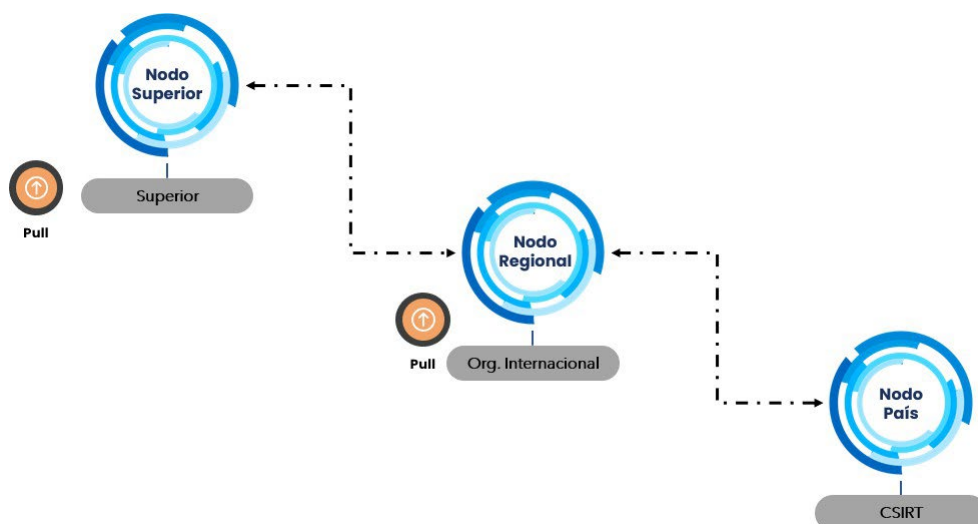
Este modelo permite compartir información entre comunidades que están interconectadas mediante nodos sincronizados. La información fluye de forma controlada entre nodos superiores, regionales y locales.

Características

Sincronización de Instancias MISP

- **Distribución escalonada:** Los datos se comparten solo entre nodos que tienen configuraciones de sincronización establecidas.
- **Control granular:** Cada nodo puede establecer sus propias restricciones de distribución.

Figura 80. Modelo de intercambio "Comunidades conectadas" en MISP.



Nota: Diagrama que muestra el modelo "Connected communities" en MISP.

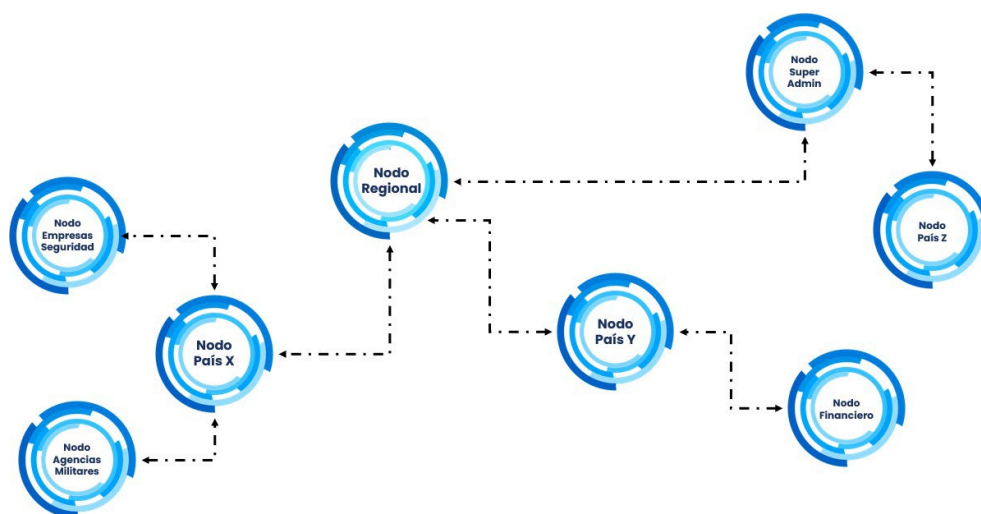
7.3.4. Todas las comunidades (All communities)

Este modelo es el más amplio de todos, permitiendo que la información llegue a cualquier nodo o comunidad conectada sin restricciones.

Características

- **Acceso universal:** Los datos se comparten con todas las instancias conectadas, sin importar su nivel o ubicación.
- **Distribución automática:** Una vez que se publica un evento con este nivel de distribución, todas las comunidades conectadas tendrán acceso a él.
- **Ideal para colaboración global:** Facilita la difusión de información crítica, como indicadores de amenazas, a la mayor cantidad de nodos posibles.

Figura 81. Modelo de intercambio "Todas las comunidades" en MISP.



Nota: Diagrama que muestra el modelo "All communities" en MISP.

¡Con estos pasos, habrás completado la sincronización entre las dos instancias de MISP! Esta configuración te permitirá compartir eventos y atributos de manera segura, mejorando la colaboración y la gestión de inteligencia de amenazas en tu organización.

Si necesitas realizar ajustes o resolver problemas específicos, consulta los logs de cada servidor o revisa los permisos asignados a las organizaciones y usuarios.



ANEXO 1

HARDENING

BÁSICO

8.1. Introducción

En un mundo digital cada vez más complejo, la seguridad de los sistemas es fundamental para proteger la información y garantizar el funcionamiento seguro de las organizaciones.

8.1.1. Hardening

El "hardening" o "endurecimiento" es el proceso de fortalecer la seguridad de un sistema o aplicación, reduciendo vulnerabilidades y protegiéndolo contra posibles amenazas. Consiste en la implementación de medidas de seguridad que disminuyen la superficie de ataque de un sistema, tales como configuraciones específicas, la eliminación de servicios innecesarios y la restricción de accesos. Este proceso es fundamental para minimizar el riesgo de explotación de debilidades en la infraestructura de TI.

8.1.2. Backup (Respaldo)

El término backup o respaldo se refiere a la creación de una copia de seguridad de archivos o bases de datos. En MISP, realizar respaldos regulares asegura que la configuración, los datos y otros archivos críticos estén protegidos y puedan ser restaurados en caso de pérdida de información o fallo del sistema.

8.2. Actualización del sistema operativo

Las actualizaciones permiten corregir vulnerabilidades conocidas, mejorar el rendimiento y asegurar la compatibilidad con otros componentes. A continuación, se explican las principales actualizaciones recomendadas para el sistema operativo.

Advertencia:

Antes de proceder con la actualización de un sistema operativo Linux, es altamente recomendable realizar un **snapshot** (instantánea) del estado actual del sistema. Esto permite restaurar la máquina a un estado previo en caso de que la actualización genere errores, incompatibilidades o fallas críticas.

Para actualizar sistemas basados en Debian o Ubuntu, puedes utilizar el siguiente comando. Antes de proceder con la actualización, es recomendable revisar qué paquetes se van a modificar, ya que esto podría afectar otros servicios en ejecución dentro del sistema operativo.

```
$ sudo apt update && sudo apt upgrade
```

8.3. Copias de seguridad y actualizaciones en MISP

8.3.1. Backup (Respaldo)

Para realizar respaldos en sistemas operativos Linux, puedes utilizar el comando `tar`, que comprime los archivos especificados en un solo archivo de respaldo. Primero, asegúrate de estar ubicado en el directorio donde deseas almacenar el archivo de respaldo. En este caso hemos creado previamente una carpeta llamada “backups” en el directorio raíz.

```
$ cd /backups  
$ tar -zcvf respaldo.tar.gz $path1 $path2 $path3 ... $pathN
```

En este comando, el primer paso (`cd /backups`) cambia el directorio de trabajo al lugar donde se almacenará el respaldo. Luego, el comando `tar -zcvf respaldo.tar.gz` crea un archivo comprimido llamado `respaldo.tar.gz`, que contiene todos los archivos y carpetas especificados en las rutas (`$path1`, `$path2`, etc.).

Nota:

Recuerda reemplazar `$path1`, `$path2`, etc., con las rutas de los archivos y carpetas que deseas incluir en el respaldo.

Advertencia:

Se recomienda **no almacenar los backups en el mismo servidor**. Si el servidor falla, se corre el riesgo de perder tanto los datos originales como la copia de seguridad. Es preferible guardar los respaldos en un servidor externo, almacenamiento en la nube o una unidad externa.

Asegúrate de incluir los archivos y carpetas críticos de MISP que se detallan en la siguiente lista:

- **Código fuente y configuración de MISP:**

```
/var/www/MISP
```

- **Certificados y Apache:**

```
/etc
```

Hardening Básico

Para respaldar la base de datos de MISP, realiza un "dump" (una copia completa de los datos actuales) con el siguiente comando, especificando el nombre de la base de datos misp:

```
$ mysqldump -u {db_user} -p {name_database} > misp_db_bkp.sql.dump
```

Este comando usa mysqldump, una herramienta de respaldo para bases de datos MySQL, con las opciones -u y -p para especificar el nombre de usuario y la contraseña. La información se guardará en un archivo de salida llamado misp_db_bkp.sql.dump, que contiene el estado actual de la base de datos.

Nota:

Reemplaza {db_user} y {name_database} con el nombre de usuario y la base de datos de MISP, la cual se llama "misp". Puede encontrar el usuario y la contraseña en el archivo "/var/log/misp_settings.txt"

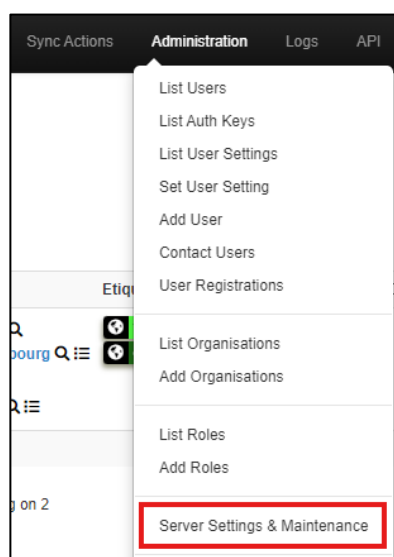
```
$ mysqldump -u misp -p misp > misp_db_bkp.sql.dump
```

8.3.2. Actualizaciones de MISP

Si existe una nueva versión, realiza la actualización primero en un ambiente de pruebas para confirmar que todo funcione correctamente. Una vez verificado, puedes aplicar el proceso en el entorno de producción.

Para actualizar la plataforma, accede al menú "Administration", selecciona "Server Settings & Maintenance" y haz clic en "Diagnostics". Esto te permitirá verificar si hay una nueva versión de MISP disponible.

Figura 82. Acceso a Server Settings & Maintenance.



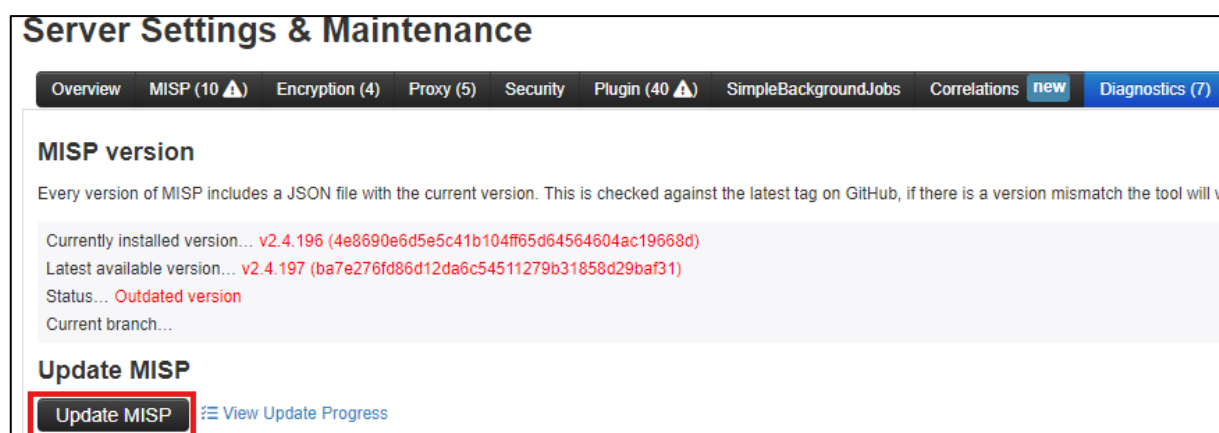
Nota: Captura del menú con "Server Settings & Maintenance".

Figura 83. Sección Diagnostic en Server Settings & Maintenance.



Nota: Captura de la pestaña "Diagnostic" en Server Settings & Maintenance.

Figura 84. Opciones de Actualización en Diagnostic.



Nota: Captura de pantalla que muestra la opción "Update MISP" en la sección "Diagnostic".

Cuando solicites la actualización, se mostrará un cuadro de confirmación para proceder.

Figura 85. Confirmación para Actualizar MISP.



Nota: Captura de pantalla que muestra la opción "Update MISP" en la sección "Diagnostic".

Nota:

No es aconsejable omitir más de dos actualizaciones consecutivas, ya que podrían requerirse cambios significativos que implicarían una reinstalación completa para mantener la versión al día.

8.4. Configurar el firewall

Configurar un firewall es una de las primeras medidas de seguridad para proteger el acceso a sistemas críticos. Este proceso consiste en definir qué puertos pueden ser accedidos, permitiendo solo aquellos necesarios para la operación de los servicios principales.

Para MISP, es importante señalar que **utiliza el puerto 443**, que se destina a conexiones HTTPS¹⁸ seguras. Este puerto permite que los datos se transmitan de manera cifrada, garantizando la confidencialidad e integridad de la información. En la configuración del firewall, asegúrate de habilitar el puerto 443 para MISP.

Si se requiere acceso remoto para administración, también puedes habilitar el puerto 22, destinado a conexiones SSH. Sin embargo, es recomendable restringir el acceso a este puerto a direcciones IP autorizadas, o bien implementar métodos de autenticación

¹⁸ Protocolo de comunicación segura en la web que cifra los datos transmitidos entre el cliente y el servidor.

Hardening Básico

reforzados, como el uso de claves SSH. Más adelante en el manual, sugerimos cambiar el número de puerto.

Para realizar esta configuración en sistemas basados en Linux, puedes usar los comandos `iptables` o `ufw` en sistemas basados en Ubuntu/Debian:

Nota:

Es altamente recomendable realizar auditorías periódicas y revisar la configuración del firewall para asegurar que solo los puertos esenciales se mantengan abiertos y que cualquier cambio no autorizado sea detectado a tiempo.

Esta configuración básica de firewall, centrada en el principio de "mínimo acceso necesario," mejora significativamente la seguridad del entorno de MISP y reduce la exposición a potenciales amenazas.

8.5. Cifrado de Datos

8.5.1. Uso de HTTPS

Implementar HTTPS asegura que el tráfico entre los usuarios y el servidor esté protegido mediante un cifrado SSL/TLS¹⁹. Aunque los datos transmitidos podrían ser interceptados, no pueden ser leídos ni manipulados por terceros sin la clave de cifrado correspondiente. HTTPS crea una conexión segura que protege las credenciales, datos personales y cualquier otra información sensible que los usuarios compartan en línea.

Para implementar HTTPS en su servidor, puede utilizar Certbot²⁰, una herramienta que simplifica el proceso de configuración de un certificado SSL gratuito de Let's Encrypt. Esta opción es compatible tanto con servidores [Nginx](#) como [Apache](#), y permite que el tráfico de su sitio sea automáticamente cifrado.

Nota:

Si bien Certbot automatiza el proceso de instalación y renovación de certificados, es recomendable que revise periódicamente la configuración de su servidor para garantizar que el certificado se renueva correctamente y que cualquier cambio en los requisitos de seguridad de TLS sea atendido.

¹⁹ Protocolos criptográficos que proporcionan comunicación segura en internet mediante cifrado de datos.

²⁰ Software que automatiza la obtención y renovación de certificados SSL/TLS de Let's Encrypt. Más información: <https://certbot.eff.org>

8.6. Políticas de Seguridad

8.6.1. Autenticación multifactor (MFA)

Para fortalecer la seguridad de su cuenta en MISP, es recomendable habilitar la autenticación de dos factores (2FA²¹) utilizando contraseñas de un solo uso basadas en tiempo (TOTP²²). A continuación, se detallan los pasos para activar esta función en su perfil de usuario:

1. Acceda a su perfil de usuario:

- Inicie sesión en su instancia de MISP.
- Haga clic en “Admin” ubicado en la esquina superior derecha.

Figura 86. Acceso a la Configuración de Usuario en MISP.



Nota: Captura que muestra el botón "Admin" para acceder al perfil de usuario.

2. Habilite TOTP

- En la sección de su perfil, busque la opción para habilitar TOTP.

Figura 87. Habilitación de TOTP en el Perfil de Usuario.

User user1@org2.tld	
ID	4
Email	user1@org2.tld
Organisation	ORG2
Role	User
TOTP	No Generate

²¹ Autenticación en dos pasos que requiere una segunda forma de verificación, además de la contraseña, para acceder a un sistema.

²² Código de un solo uso basado en el tiempo, generado por aplicaciones como Google Authenticator o Authy para la autenticación de dos factores.

Nota: Captura que muestra la opción para generar TOTP en el perfil de usuario.

- En la sección de su perfil, busque la opción para habilitar TOTP.

Figura 88. Generación de Código QR para TOTP.

Validate your One Time Password

To enable TOTP for your account, scan the following QR code with your TOTP application and validate the token.



Alternatively you can enter the following secret in your TOTP application:

B3SPVI42N4XQCXL4HNQMVI42TY53JVJGLF2FO4H5H5IIP6MV7C6QLYP5SKVOZ3MIGGZLLOZGZBXL7TTGBX

One Time Password verification

Enter your OTP code here

Submit

Nota: Captura que muestra el código QR generado para habilitar TOTP.

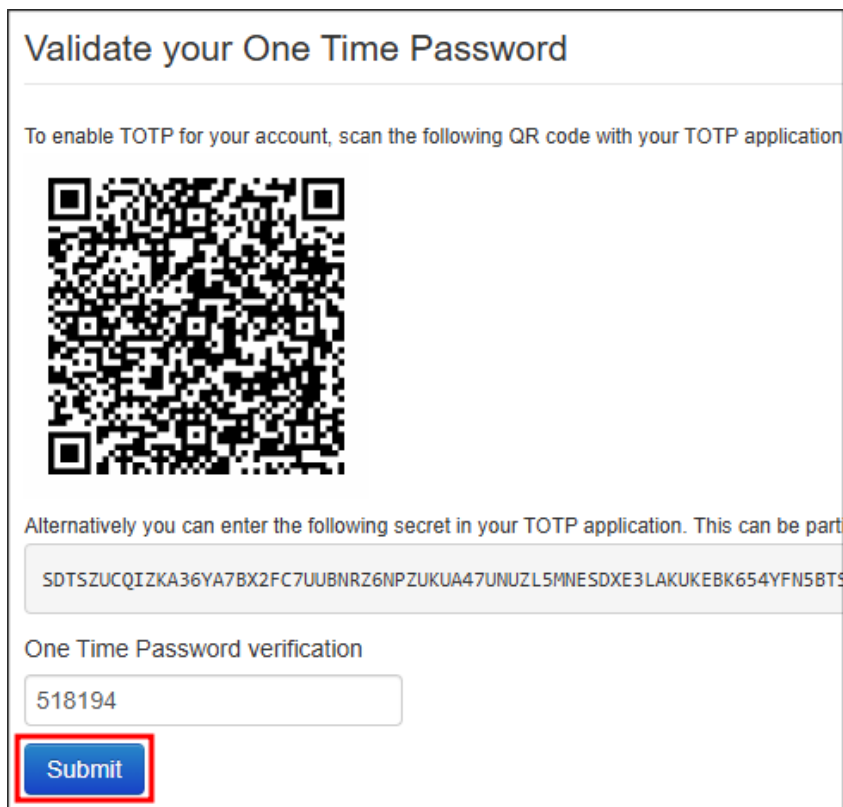
3. Configure la aplicación de autenticación:

- Utilice una aplicación de autenticación compatible con TOTP, como Google Authenticator, Microsoft Authenticator o Authy.
- Abra la aplicación en su dispositivo móvil.
- Seleccione la opción para agregar una nueva cuenta y escanee el código QR proporcionado por MISP.
- Después de escanear el código QR, la aplicación generará códigos temporales de seis dígitos.

Hardening Básico

- Ingrese uno de estos códigos en el campo de verificación en MISP para confirmar la configuración y de click al botón "Submit" para guardar.

Figura 89. Validación del Código TOTP.



Validate your One Time Password

To enable TOTP for your account, scan the following QR code with your TOTP application



Alternatively you can enter the following secret in your TOTP application. This can be part

SDTSZUCQIZKA36YA7BX2FC7UUBNRZ6NPZUKUA47UNUZL5MMESDXE3LAKUKEBK654YFN5BT5

One Time Password verification

518194

Submit

Nota: Captura que muestra el ingreso y envío del código TOTP para validación.

4. Guarde sus códigos de recuperación (HOTP):

- Una vez verificado el TOTP, MISP le proporcionará una lista de códigos de un solo uso (HOTP) que puede utilizar en caso de no tener acceso a su dispositivo móvil.
- Guarde los códigos en un lugar seguro, ya que serán esenciales para acceder a su cuenta si pierde el acceso a la aplicación de autenticación.
- A partir de ahora, al iniciar sesión, después de ingresar su nombre de usuario y contraseña, se le solicitará un código TOTP generado por su aplicación de autenticación.

Figura 90. Códigos de Respaldo de TOTP.

Paper based Single Use Tokens

The following list contains the next tokens in case you do not have your phone/software.
Make sure you print these out.

2: 067437	3: 380057	4: 902452	5: 363735	6: 019000
7: 631344	8: 243925	9: 870901	10: 806546	11: 268213
12: 154437	13: 397186	14: 241387	15: 157215	16: 688274
17: 810158	18: 974530	19: 844798	20: 378160	21: 886323
22: 417730	23: 806694	24: 156150	25: 016791	26: 476100
27: 676720	28: 932189	29: 094909	30: 199175	31: 271528
32: 909074	33: 985491	34: 439831	35: 317910	36: 836166
37: 313385	38: 798692	39: 446264	40: 188740	41: 161885
42: 826448	43: 021330	44: 475906	45: 823078	46: 370093
47: 117676	48: 817608	49: 773854	50: 882291	51: 653254

Nota: Captura que muestra la lista de códigos de un solo uso (HOTP) generados como respaldo.

Figura 91. Solicitud de TOTP al Iniciar Sesión.

Validate your One Time Password

Enter either your TOTP or paper based Single Use Token number 2

Enter your OTP here

Nota: Captura que muestra el campo para ingresar el código TOTP o un token de respaldo al iniciar sesión.

Nota:

Se puede habilitar la autenticación de dos factores (2FA) mediante la configuración del parámetro `MISP.totp_required`. Al activarlo, todos los usuarios deberán configurar TOTP en su próximo inicio de sesión y no podrán acceder a otras páginas hasta completar este proceso. Es esencial asegurarse de que las bibliotecas PHP necesarias estén instaladas para evitar que los administradores queden bloqueados. Las bibliotecas requeridas son:

- `spomky-labs/otphp`
- `bacon/bacon-qr-code`

Estas pueden instalarse mediante Composer.

8.6.2. Política de contraseñas

Por defecto, MISP implementa una política de contraseñas que exige a los usuarios crear contraseñas con un mínimo de 12 caracteres, combinando letras mayúsculas, minúsculas, números y caracteres especiales.

- Navegue a "Administration" y seleccione "Server Settings & Maintenance".
- Busque la categoría "Security".
- Busque las siguientes configuraciones y modifíquelo según sus necesidades:
 - `Security.password_policy_length`: Define la longitud mínima requerida para las contraseñas.
 - `Security.password_policy_complexity`: Define los requisitos de complejidad de las contraseñas, incluyendo la necesidad de letras mayúsculas, minúsculas, números y caracteres especiales. Por defecto, se acepta una contraseña que cumpla con estos criterios o que tenga más de 16 caracteres, permitiendo en este último caso el uso exclusivo de caracteres alfanuméricos.

8.6.3. Restringir el acceso SSH

- Permite el acceso SSH únicamente desde IPs autorizadas para reducir riesgos.
- Desactiva el acceso SSH para el usuario root y crea un usuario con privilegios específicos en su lugar.
- Cambia el puerto SSH para evitar ataques básicos de escaneo.

Hardening Básico

- Ajusta el firewall para permitir conexiones solo en el nuevo puerto SSH configurado.
- Implementa un sistema como Fail2Ban para prevenir ataques de fuerza bruta y bloquear intentos de acceso no autorizados.

Configura `sshd_config`

```
$ sudo nano /etc/ssh/sshd_config
```

Ajusta las siguientes líneas:

```
PermitRootLogin no  
Port 2222
```

Luego, reinicia SSH:

```
$ sudo systemctl restart ssh
```

8.7. Hardening del Sistema Operativo

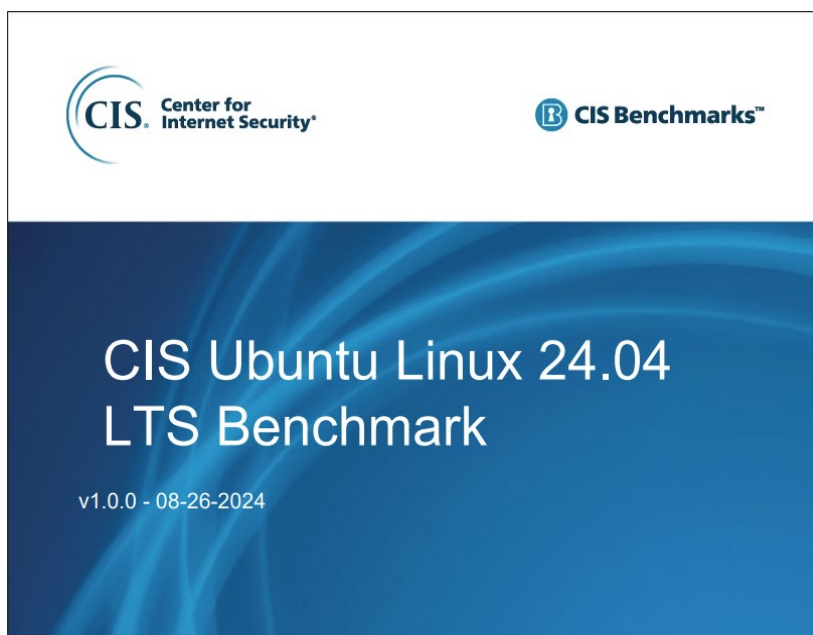
8.7.1. Utilizar CIS Benchmarks

Los CIS Benchmarks, desarrollados por el Center for Internet Security, son guías de configuración de seguridad consensuadas que proporcionan recomendaciones detalladas para diversos sistemas operativos y aplicaciones. Estas guías ayudan a las organizaciones a establecer configuraciones seguras y a mantenerlas actualizadas.

Es **fundamental revisar las guías de CIS Benchmarks antes de instalar el sistema operativo base**, ya que muchas configuraciones recomendadas deben aplicarse durante la instalación. Si no se consideran desde el inicio, ajustarlas posteriormente puede ser complejo y afectar el porcentaje de cumplimiento.

Por ejemplo, algunos CIS Benchmarks requieren que ciertos sistemas de archivos, como `/var`, `/tmp` o `/home`, se monten en particiones separadas o en discos distintos para mejorar la seguridad y la resiliencia. Además, también pueden recomendar el uso de ciertos tipos de sistemas de archivos o configuraciones específicas en `/etc/fstab`. Si estas decisiones no se toman durante la instalación, corregirlas después puede implicar reinstalaciones o cambios arriesgados en el sistema.

Figura 92. Guía de CIS Benchmarks para Ubuntu 24.04 LTS.



Nota: Captura que muestra la portada de la guía de configuración de seguridad publicada por el Center for Internet Security (CIS).

Nota:

En el manual de instalación de MISP, se recomienda, además de realizar un hardening al sistema operativo, aplicar medidas de seguridad adicionales a los servicios **Apache** y **MySQL**.

Recommended actions

- By default CakePHP exposes its name and version in email headers. Apply a patch to remove this behavior.
- You should really harden your OS
- You should really harden the configuration of Apache
- You should really harden the configuration of MySQL
- Keep your software up2date (MISP, CakePHP and everything else)
- Log and audit

Para ello, los **CIS Benchmarks** proporcionan manuales específicos que detallan las mejores prácticas de configuración y endurecimiento (hardening) para estos servicios. Puedes consultar dichos manuales directamente desde la documentación de [CIS Benchmarks](#).

CRÉDITOS

● Luis Almagro ●

Secretario General de la Organización
de Estados Americanos

● Equipo técnico de la OEA ●

Alison August Treppel

Kerry-Ann Barrett

Diego Subero

Carmen Quintos

Volker Esteves

Nelson Guanilo

Einar Lanfranco

Alejandro Sabolansky

Manuel Panero

Fermin Baudino

Gloria Cisneros

● Diseño ●

María Paula Lozano

Agradecimientos a

 UK Government

REFERENCIAS

Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016).
MISP: The Design and Implementation of a Collaborative
Threat Intelligence Sharing Platform. In *Proceedings of the
2016 ACM on Workshop on Information Sharing and
Collaborative Security* (pp. 49–56).

Manual Técnico de **MISP**

Facilitando el intercambio de información
en comunidades de ciberseguridad



OEA | CICTE



| CSIRT Americas
Network