cedia
CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA

GSI-IN-2024-0190

ACTA PUESTA EN OPERACIÓN SERVICIO SOC – UNIVERSIDAD LAICA ELOY ALFARO DE MANABI

SOC CSIRT CEDIA

www.cedia.edu.ec
info@cedia.org.ec

(+593) 7 407 9300

© El presente documento se encuentra protegido por Derechos de Autor y es de titularidad exclusiva de CEDIA. Ha sido autorizado su uso exclusivo para fines informativos. Queda totalmente prohibida la distribución total o parcial no autorizada de los contenidos del documento para fines ajenos al previsto. Cualquier duda de aplicación individual o interpretación puede ser comunicada al correo: info@cedia.org.ec.
El presente aviso no podrá ser modificado, ni excluido del texto.

Tabla de contenido

Oficinas_
Gonzalo Cordero 2-122
y J. Fajardo esquina.
DIGITALS_
Miguel Moreno y Av. 10
de Agosto

UIO
Av. 12 de Octubre y
Lizardo García
Edificio Alto Aragón
Oficina 8A

GYE
Av. Del Bombero,
Km 6.5 - Edificio
La Vista de San Eduardo
5to piso Ofics. 510 y 511

PORTOVIEJO
Av. Metropolitana
Eloy Alfaro #2005
y Av. Olimpica.
Univ. San Gregorio

MANTA
Av. Circunvalación
Vía a San Mateo
ULEAM - EP

© El presente documento se encuentra protegido por Derechos de Autor y es de titularidad exclusiva de CEDIA. Ha sido autorizado su uso exclusivo para fines informativos. Queda totalmente prohibida la distribución total o parcial no autorizada de los contenidos del documento para fines ajenos al previsto. Cualquier duda de aplicación individual o interpretación puede ser comunicada al correo: info@cedia.org.ec. El presente aviso no podrá ser modificado, ni excluido del texto.

1 Introducción

En el contexto de la creciente complejidad y sofisticación de las amenazas cibernéticas, la adopción de soluciones avanzadas de seguridad se ha convertido en una prioridad estratégica para las organizaciones. En este sentido, se presenta la presente acta de entrega recepción de los servicios de Análisis de superficie pública, SIEM y monitoreo en Darkweb-Deepweb, herramientas fundamentales para la gestión y monitoreo de la seguridad informática. Este documento formaliza la transferencia de la responsabilidad operativa y administrativa de dichos servicios, garantizando la continuidad y efectividad en la protección de la infraestructura tecnológica de la organización.

En análisis de superficie pública proporciona una visión integral y continua del estado de seguridad de la organización y sus terceros, permitiendo una evaluación dinámica y precisa de los riesgos asociados. SIEM, por su parte, integra capacidades de gestión de eventos e información de seguridad, facilitando la detección, análisis y respuesta a incidentes de manera eficiente y centralizada. Monitoreo Darkeb-Deepweb complementa este ecosistema con sus funciones de reconocimiento proactivo y vigilancia digital, anticipando posibles amenazas y vulnerabilidades antes de que se materialicen en ataques efectivos.

Adicionalmente, el acta incorpora un análisis detallado del nivel de cumplimiento de la organización con la norma ISO 27001 o EGSI V3.0, estándares para la gestión de la seguridad de la información, y con la Ley Orgánica de Protección de Datos Personales (LOPD) vigente en nuestro país. Este análisis es crucial para asegurar que las prácticas y políticas de seguridad no solo sean efectivas desde un punto de vista técnico, sino que también estén alineadas con los requisitos regulatorios y las mejores prácticas internacionales.

En resumen, este documento no solo formaliza la entrega y recepción de servicios críticos de seguridad, sino que también refleja el compromiso de la organización con la mejora continua de su postura de ciberseguridad y con el cumplimiento de las normativas pertinentes, garantizando así la protección integral de sus activos de información y la confianza de sus stakeholders. Así como el compromiso de CEDIA en colaborar con las instituciones miembro a alcanzar niveles de seguridad adaptados a sus necesidades y al cumplimiento normativo.

Oficinas_
Gonzalo Cordero 2-122
y J. Fajardo esquina.
DIGITALS_
Miguel Moreno y Av. 10
de Agosto

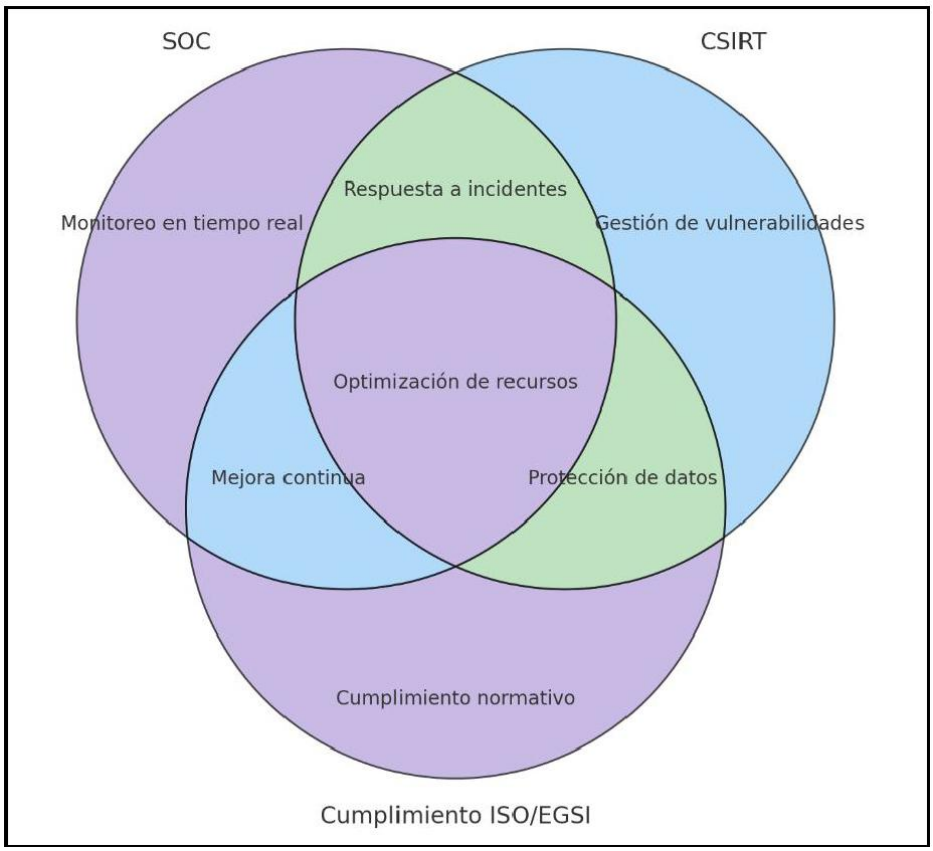
UIO
Av. 12 de Octubre y
Lizardo García
Edificio Alto Aragón
Oficina 8A

GYE
Av. Del Bombero,
Km 6.5 - Edificio
La Vista de San Eduardo
5to piso Ofics. 510 y 511

PORTOVIEJO
Av. Metropolitana
Eloy Alfaro #2005
y Av. Olimpica.
Univ. San Gregorio

MANTA
Av. Circunvalación
Vía a San Mateo
ULEAM - EP

© El presente documento se encuentra protegido por Derechos de Autor y es de titularidad exclusiva de CEDIA. Ha sido autorizado su uso exclusivo para fines informativos. Queda totalmente prohibida la distribución total o parcial no autorizada de los contenidos del documento para fines ajenos al previsto. Cualquier duda de aplicación individual o interpretación puede ser comunicada al correo: info@cedia.org.ec. El presente aviso no podrá ser modificado, ni excluido del texto.



En conjunto, el SOC, el CSIRT y el cumplimiento normativo forman una estrategia integral de seguridad que permite a las organizaciones enfrentar con éxito las amenazas digitales actuales. Esta combinación asegura que las instituciones estén preparadas para gestionar y mitigar riesgos, protegiendo su infraestructura y manteniendo la continuidad de sus operaciones en un entorno cada vez más complejo. Al contar con estos beneficios, las instituciones pueden enfocarse en brindar soluciones de educación de alta calidad, confiando en que su seguridad y cumplimiento están en manos expertas. Sin embargo, es fundamental reconocer que la responsabilidad es compartida: tanto la institución como CEDIA deben trabajar en conjunto para garantizar el éxito de estas estrategias, colaborando estrechamente para fortalecer la seguridad y el cumplimiento normativo.

2 Servicios habilitados

- Informe del nivel de Madurez en Seguridad de la Información y Protección de Datos Personales
- Acceso a plataforma de supervisión de superficie pública
- Activación de monitoreo de dominios en DarkWeb

Oficinas_
Gonzalo Cordero 2-122 y J. Fajardo esquina.
DIGITALS_
Miguel Moreno y Av. 10 de Agosto

UIO
Av. 12 de Octubre y Lizardo García
Edificio Alto Aragón
Oficina 8A

GYE
Av. Del Bombero, Km 6.5 - Edificio
La Vista de San Eduardo
5to piso Ofics. 510 y 511

PORTOVIEJO
Av. Metropolitana Eloy Alfaro #2005 y Av. Olimpica.
Univ. San Gregorio

MANTA
Av. Circunvalación Vía a San Mateo
ULEAM - EP

© El presente documento se encuentra protegido por Derechos de Autor y es de titularidad exclusiva de CEDIA. Ha sido autorizado su uso exclusivo para fines informativos. Queda totalmente prohibida la distribución total o parcial no autorizada de los contenidos del documento para fines ajenos al previsto. Cualquier duda de aplicación individual o interpretación puede ser comunicada al correo: info@cedia.org.ec. El presente aviso no podrá ser modificado, ni excluido del texto.

- Activación de correlación de eventos en SIEM

2.1 Informe de nivel de Madurez en Seguridad de la Información y Protección de Datos Personales

Se emitió el informe GSI-IN-2024-0154 INFORME NIVEL DE MADUREZ ULEAM con fecha 11 de septiembre del 2024 remitido vía correo electrónico a nombre del Ing. Avelino Carrillo y del Ing. Cesar Cedeño.

2.2 Acceso a plataforma de supervisión de superficie pública

Se entregaron los accesos a la plataforma www.securityscorecard.io desde el 18 de julio del 2024 a los usuarios:

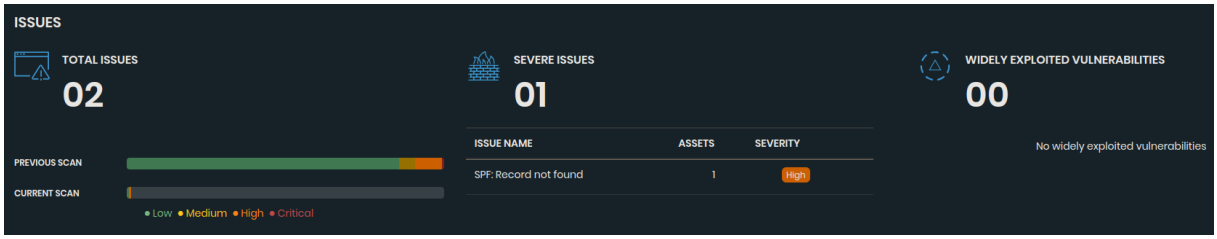
7 filas — Columnas — Pantalla completa

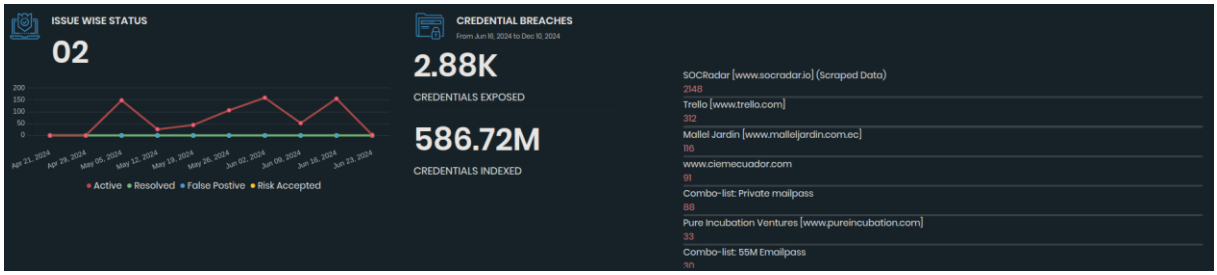
Name	Job title	Added by
Federico Avelino Carrillo Pico avelino.carrillo@uleam.edu.ec	-	paul.astudillo@cedia.org.ec
Cesar Cedeno cesar.cedeno@uleam.edu.ec	-	paul.astudillo@cedia.org.ec
Cesar manrique cesar.manrique@uleam.edu.ec	-	paul.astudillo@cedia.org.ec
leonardo rodriguez leonardo.rodriguez@uleam.edu.ec	-	paul.astudillo@cedia.org.ec
Security Uleam securityscorecard@uleam.edu.ec	-	paul.astudillo@cedia.org.ec

2.3 Activación del monitoreo de dominios en DarkWeb

Se activó el monitoreo del dominio *uleam.edu.ec* en la DarkWeb desde el 29 de abril del 2024.

© El presente documento se encuentra protegido por Derechos de Autor y es de titularidad exclusiva de CEDIA. Ha sido autorizado su uso exclusivo para fines informativos. Queda totalmente prohibida la distribución total o parcial no autorizada de los contenidos del documento para fines ajenos al previsto. Cualquier duda de aplicación individual o interpretación puede ser comunicada al correo: info@cedia.org.ec. El presente aviso no podrá ser modificado, ni excluido del texto.





2.4 Activación de correlación de eventos en SIEM

Se procedió a configurar, capacitar y entregar credenciales para el servicio del SIEM a partir del 26 abril del 2024.

De acuerdo al monitoreo de los EPS hasta la presente fecha: 829

Despliegue de colector:

Organization	Collector ID	Collector Name	IP Address	Health	Last Status Updated	Last File Received	Collector Type	Version	Memory Size	Uptime	EPS
ULEAM	10011	collector01_uleam	10.253.254.250	Critical	Dec 10, 2024, 02:30:22 PM	Dec 10, 2024, 02:29:05...	VM	7.1.4.0177	23GB	15d 6h	466.38

Plataformas monitorizadas:

Name	IP	Device Type	Status	Discovered	Method
collector01_uleam	10.253.254.250	Fortinet FortiSIEM	Approved	Apr 26, 2024, 09:51:22 AM	MANUAL
HOST-10.253.254.3	10.253.254.3	Generic Unix	Approved	May 02, 2024, 09:44:39 AM	LOG
ULEAM_FortiGate	10.253.254.136	Fortinet FortiOS	Approved	Apr 26, 2024, 10:08:27 AM	LOG

Plataforma de gestión:

Oficinas_
Gonzalo Cordero 2-122
y J. Fajardo esquina.
DIGITALS_
Miguel Moreno y Av. 10
de Agosto

UIO
Av. 12 de Octubre y
Lizardo García
Edificio Alto Aragón
Oficina 8A

GYE
Av. Del Bombero,
Km 6.5 - Edificio
La Vista de San Eduardo
5to piso Ofics. 510 y 511

PORTOVIEJO
Av. Metropolitana
Eloy Alfaro #2005
y Av. Olimpica.
Univ. San Gregorio

MANTA
Av. Circunvalación
Vía a San Mateo
ULEAM - EP

www.cedia.edu.ec
info@cedia.org.ec

(+593) 7 407 9300

CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA

Para constancia de la entrega y aceptación de los servicios firman:

Por CEDIA

Firmado electrónicamente por:
JORGE LUIS MERCHAN LIMA

Ing. Jorge Merchán
GERENTE DE SEGURIDAD DE LA INFORMACIÓN

Por ULEAM

Firmado electrónicamente por:
FEDERICO AVELINO CARRILLO PICO

Ing. Avelino Carrillo
ADMINISTRADOR DEL CONTRATO

© El presente documento se encuentra protegido por Derechos de Autor y es de titularidad exclusiva de CEDIA. Ha sido autorizado su uso exclusivo para fines informativos. Queda totalmente prohibida la distribución total o parcial no autorizada de los contenidos del documento para fines ajenos al previsto. Cualquier duda de aplicación individual o interpretación puede ser comunicada al correo: info@cedia.org.ec. El presente aviso no podrá ser modificado, ni excluido del texto.

Oficinas_
Gonzalo Cordero 2-122
y J. Fajardo esquina.
DIGITALS_
Miguel Moreno y Av. 10
de Agosto

UIO
Av. 12 de Octubre y
Lizardo García
Edificio Alto Aragón
Oficina 8A

GYE
Av. Del Bombero,
Km 6.5 - Edificio
La Vista de San Eduardo
5to piso Ofics. 510 y 511

PORTOVIEJO
Av. Metropolitana
Eloy Alfaro #2005
y Av. Olimpica.
Univ. San Gregorio

MANTA
Av. Circunvalación
Vía a San Mateo
ULEAM - EP