UNAD Universidad Nacional Abierta y a Distancia ACREDITADA EN ALTA CALIDAD

Sistema de Gestión de la Seguridad de la Información

ISO 27001 – ISO 20001

| VIEM | GPIT | GCMO | CSIRT

Agenda

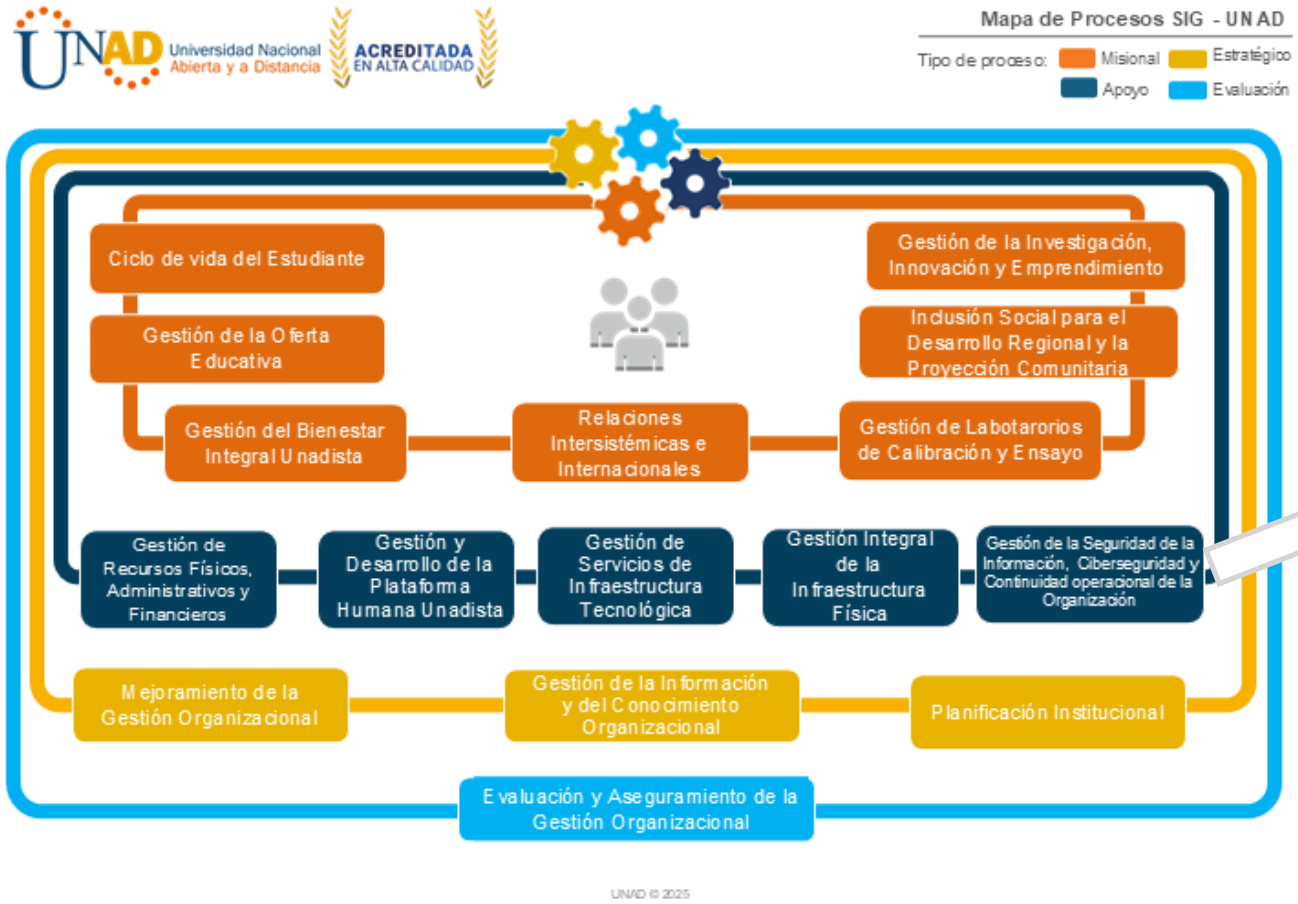
1. Protocolización Proceso C-18
2. Avances en proyectos de I+D+i

   (Endurecimiento Entorno digital UNADISTA)

   Procesos de Educación en Ciberseguridad

Protocolización Proceso C-18

Mapa de procesos SIG



(C-18)
Gestión de la Seguridad de la Información, Ciberseguridad y Continuidad operacional de la Organización

SIG – Universidad Nacional Abierta y a Distancia (UNAD). (19 de marzo de 2025). *Caracterización del proceso de gestión de la seguridad de la información, ciberseguridad y continuidad operacional de la organización (C-18)* [PDF]. Recuperado el 2 de julio de 2025, de https://sig.unad.edu.co/documentos/sgc/caracterizaciones/C-18.pdf

Objetivo

Gestionar el riesgo de los activos críticos de información de la Universidad, siguiendo los estándares y políticas de seguridad de la información y los controles establecidos por la UNAD, para mitigar la probabilidad e impacto de eventos que puedan comprometer la Disponibilidad, Confidencialidad e Integridad de la información

Alcance

El alcance comienza con la **identificación de los activos críticos de información de la Universidad, seguido por la implementación de controles para mitigar los riesgos a los que puedan estar expuestos**. Incluye el monitoreo continuo para la detección de eventos o incidentes de ciberseguridad, y finaliza con la ejecución de planes de respuesta para garantizar la continuidad de los servicios en caso de que se materialice un incidente

Procedimientos

P-18-1	Procedimiento Gestión de Copias de Respaldo y Protección de la Información	0-16-05-2025
P-18-2	Procedimiento Gestión de Eventos e Incidentes de Ciberseguridad	0-16-05-2025

SIG – Universidad Nacional Abierta y a Distancia (UNAD). (c. enero 2024). *Listado Maestro de Caracterizaciones y Procedimientos*. Recuperado el 2 de julio de 2025, de https://sig.unad.edu.co/documentacion/listados-maestros/listado-maestro-caracterizaciones-y-procedimientos

P - 18 - 1

Procedimiento Gestión de Copias de Respaldo y Protección de la Información

Objetivo: Establecer los lineamientos para la gestión de las copias de respaldo a los recursos de los sistemas de información, con el fin de tener la capacidad de recuperación ante eventos adversos que puedan afectar la disponibilidad de los servicios institucionales

Alcance: Este procedimiento inicia con la programación para la realización de las copias de respaldo de los servidores físicos, máquinas virtuales, aplicaciones y bases de datos de la UNAD, continúa con la revisión de la copia de seguridad y finaliza con pruebas aleatorias de las copias realizadas; aplica para los centros de datos Sede Nacional JCM, Data Center Externo (Zona Franca) y servicios de nube
contratado (ORACLE).

P - 18 - 2

Procedimiento Gestión de Eventos e Incidentes de Ciberseguridad

Objetivo: Gestionar de manera efectiva los eventos e incidentes de ciberseguridad en los activos de información críticos de la Universidad Nacional Abierta y a Distancia
- UNAD, a partir de la detección, análisis, respuesta y recuperación oportuna ante amenazas y vulnerabilidades, con el fin de garantizar la Disponibilidad, Integridad y Confidencialidad de la información gestionada

Alcance: Este procedimiento brinda los lineamientos para los eventos e incidentes de ciberseguridad que afecten los activos de información críticos de la Universidad Nacional Abierta y a Distancia, soportados por la infraestructura tecnológica. El alcance contempla la identificación temprana de amenazas, el análisis de vulnerabilidades, la implementación de respuestas efectivas y la ejecución de procesos de recuperación..

Indicadores Positivos

Indicador	Resultado	Observación
No conformidades mayores	0	No se identificaron durante la auditoría interna.
Cumplimiento normativo y legal	Sí	Se evidencia seguimiento de requisitos legales aplicables.
Revisión por la dirección	Sí	Identifica idoneidad y eficacia continuada del SGSI.
Auditoría interna implementada	Sí	Funciona como herramienta de mejora continua.
Objetivos del SGSI establecidos	Sí	Existe un objetivo general documentado y protocolarizado.
Política de seguridad de la información	Sí	Documentada en el Marco de referencia.
Matriz de partes interesadas (stakeholders)	Si	Se cuenta con una matriz de partes interesadas construidas y consolidada dentro de la matriz de partes interesadas del SIG
Contexto organizacional documentado	Si	Numeral 4.1 de la norma. Se encuentra documentado
Matriz de comunicaciones	Si	Se solicitó a la GCMK la creación del proceso C18 para la consolidación de la matriz dentro de la matriz del SIG

SGS Colombia. (2024). *Informe de preauditoría ISO/IEC 27001:2022 – Vigencia 2024* [Informe]. Universidad Nacional Abierta y a Distancia – UNAD. https://informacion.unad.edu.co/images/2025/Informe-preauditoria-ISO-27001-2022-Vig-2024.pdf

Indicadores parciales

Indicador	Estado	Observación
Indicadores del SGSI definidos	Parcial	Identifican 2 indicadores (incidentes y vulnerabilidades). Se encuentra en proceso de ampliación
Clasificación y etiquetado de la información	Parcial	Solo para archivo. Se encuentra en construcción
Dueños de riesgo identificados	Parcial	Numeral 6.1.2(c). Se encuentra en construcción Inventario de activos de información
Planes para alcanzar objetivos del SGSI	Parcial	Numeral 6.2. Se encuentra en construcción
Declaración de aplicabilidad (SoA)	No	Numeral 6.1.3(c). Se encuentra en construcción
Sistema en proceso de implementación	En proceso	Cumple con estructura documental y objetivos generales.

Incumplimiento especifico a 2024

Indicador	Estado	Observación
Plan de continuidad de negocio y DRP	En construcción	DRP en construcción. Numerales A.5.29 y A.5.30.
Control de acceso (matriz de acceso a sistemas)	En proceso	Falta documentación. A.5.15.
Control de proveedores (riesgos)	No	En proceso de documentación. A.5.19.
Divulgación de la política de seguridad	Si	Procesos de educación A.5.2.
Control de filtrado web	En proceso	Acceso no restringidos (Pinterest). Numeral A.8.23.
Gestión del código fuente	Débil	Código almacenado sin protección adecuada. No hay trazabilidad. Incumple A.8.4.
Pruebas de seguridad y paso a producción	En proceso	Requiere evidencia documental. Numerales A.8.31 y A.8.32.

Oportunidades de mejora

Diseñar un conjunto de indicadores clave de desempeño (KPIs) alineados a los objetivos del SGSI, que incluyan métricas sobre cumplimiento de controles, capacitación, tiempos de respuesta a incidentes, gestión de riesgos y auditorías.

Beneficio esperado:
Fortalece el seguimiento continuo, la toma de decisiones basadas en datos y la evidencia de mejora continua ante futuras auditorías de certificación.

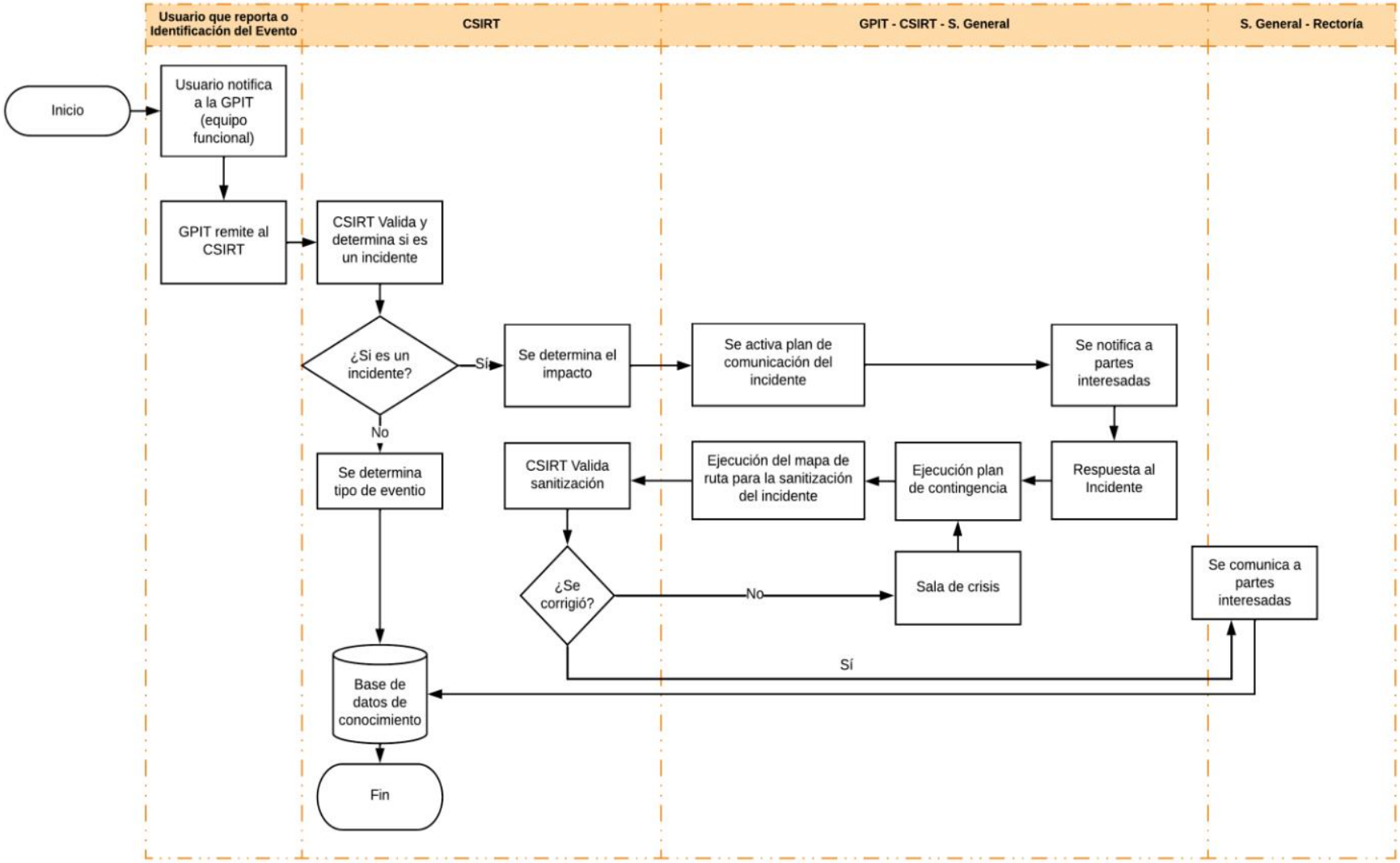
Implementar un sistema de control de versiones seguro (como GitLab o GitHub Enterprise) con políticas de acceso, trazabilidad de cambios, etiquetado, documentación técnica y validaciones de seguridad integradas en el ciclo DevSecOps.

Beneficio esperado:
Se garantiza la integridad y protección del código fuente, se mitiga el riesgo de vulnerabilidades en desarrollos propios y se mejora el cumplimiento de los controles de seguridad en el ciclo de vida del software.

Actualizar el inventario de activos de información para que incluya todos los activos críticos, su clasificación (según confidencialidad, integridad y disponibilidad), propietarios, ubicación, responsables y nivel de protección requerido.

Beneficio esperado:
Facilita la gestión del riesgo, la aplicación de controles específicos, el cumplimiento de la norma y la preparación ante incidentes, asegurando trazabilidad y gobernanza sobre los activos digitales.

Diagrama de Flujo



Avances en proyectos de I+D+i (Endurecimiento Entorno digital UNADISTA)

Cumplimento Normativo

- Resolución 1519 DE 2020 MinTIC
- MIPG (Modelo Integrado de Planeación y Gestión)
- FURAG (Formulario Único de Reporte de Avances de la Gestión)
- Requisitos ISO 27001 - ISO 20000

  Control A.8. - Desarrollo Seguro de Software - Gestión del Cambio

  Control A.5.7 - Inteligencia de amenazas
- Resolución No. 007298 DE 10 DE MAYO DE 2023

Sistema de Firma Digital UNADSignature

Información de Firma Digital

ID de Firma: 26

Fecha de Creación: 12/03/2025 16:32:27

Nombre Documento: blanco.pdf

Hash del Documento: 7f19aa32a1c309f8aca0b75feb1fde41748f4ba4fddc133921fc2ba3d6bcd34d

Nombre Firmante: Hernando Jose Peña Hidalgo

Fecha de Firmado: 12/03/2025 20:05:44

Observación: prueba ar 1

Descargar Documento

Este documento ha sido verificado frente al sistema Blockchain, fecha de consulta: 02/07/2025 15:52:42

Co-firmantes

Orden	Nombre	Correo Electrónico	Estado	Fecha
1	Hernando Jose Peña Hidalgo	hernando.pena@unad.edu.co	Aprobado para firma	12/03/2025 20:05:44

Registro historico

Fecha	Usuario	Actividad
12/03/2025 16:32:27	Hernando Jose Peña Hidalgo	Registro de solicitud de firma
12/03/2025 16:32:49	Hernando Jose Peña Hidalgo	Firma del documento
12/03/2025 16:38:06	Hernando Jose Peña Hidalgo	Firma del documento
12/03/2025 16:38:53	Hernando Jose Peña Hidalgo	Firma del documento

https://firmadigital.unad.edu.co/verifica/?id=WXgwOGt2bDhEVCtjYTV5bWp3OVNrQT09

Capacidades Desarrolladas

UNADSignature: Sistema de Gestión de Firma Documentos Digitales

Función principal: Garantizar la integridad del documento y la autenticidad del firmante, reduciendo el riesgo de manipulación y suplantación

Estado: Fase de integración al SIG (ONAC)

Sistema de Análisis de Riesgos UNADSar

UNADSar
Sistema de Análisis de Riesgos de Ciberseguridad
CSIRT Académico UNAD

Matriz de Criticidad basada en las dimensiones de la Seguridad

Criticidad de Activos (Dimensiones de la seguridad - MAGERIT)

Alta	Media	Baja
Sistema de información EDUNAT C: Alta I: Alta D: Alta T: Alta A: Alta Criticidad: Alta Puntaje: 15	Horus System Manager C: Media I: Alta D: Media T: Alta A: Alta Criticidad: Media Puntaje: 13	*Sin activos*
THUMANO - Sistemas de información de Gestión Humana C: Alta I: Alta D: Media T: Alta A: Alta Criticidad: Alta Puntaje: 15	XDR wazuh ZF - JCM C: Media I: Alta D: Media T: Alta A: Media Criticidad: Media Puntaje: 12	
Campus Virtual UNAD C: Alta I: Alta D: Alta T: Alta A: Alta Criticidad: Alta Puntaje: 15	XDR wazuh - SII 5.0 C: Media I: Alta D: Media T: Media A: Alta Criticidad: Media Puntaje: 12	
Sistema Integrado de Autenticación (Intranet) C: Alta I: Alta D: Alta T: Alta A: Alta Criticidad: Alta Puntaje: 15	XDR wazuh Campus C: Media I: Alta D: Media T: Media A: Media Criticidad: Media Puntaje: 11	
SII 5.0 C: Alta I: Alta D: Alta T: Alta A: Alta Criticidad: Alta Puntaje: 15	UNADSar C: Alta I: Media D: Media T: Media A: Media Criticidad: Media Puntaje: 11	
Sistema de Gestión de Identidades C: Alta I: Alta D: Alta T: Alta A: Alta Criticidad: Alta Puntaje: 15	Sitios web unad.edu.co (joomal) C: Media I: Alta D: Media T: Media A: Media Criticidad: Media Puntaje: 11	
UNADSignature C: Alta I: Alta D: Media T: Alta A: Alta Criticidad: Alta Puntaje: 14		
Data Protector C: Alta I: Alta D: Alta T: Media A: Media Criticidad: Alta Puntaje: 13		

https://sar.unad.edu.co:8081/

Capacidades Desarrolladas

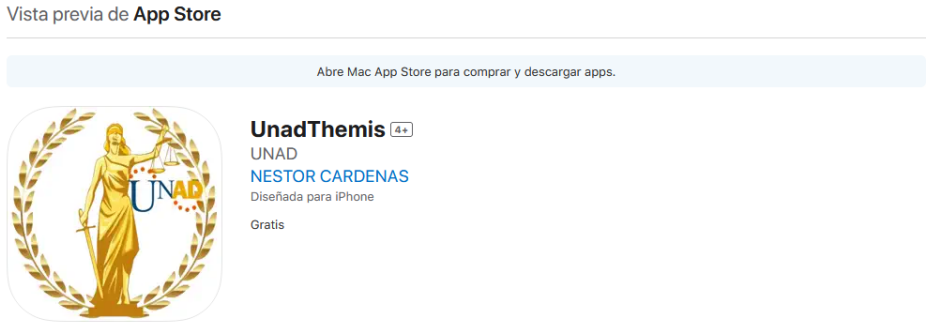
UNADSar: Sistema para el análisis y gestión de riesgos de ciberseguridad.

Función principal: Bajo una estructura de gobernanza, permite realizar análisis de riesgo sistemáticos, vinculados a políticas institucionales y supervisados

Estado: Fase de implementación (ISO 27000)

Sistema de Doble Factor de Autenticación UNADThemis

https://play.google.com/store/apps/details?id=com.unad.themis



https://apps.apple.com/co/app/unadthemis/id6743343950

Capacidades Desarrolladas

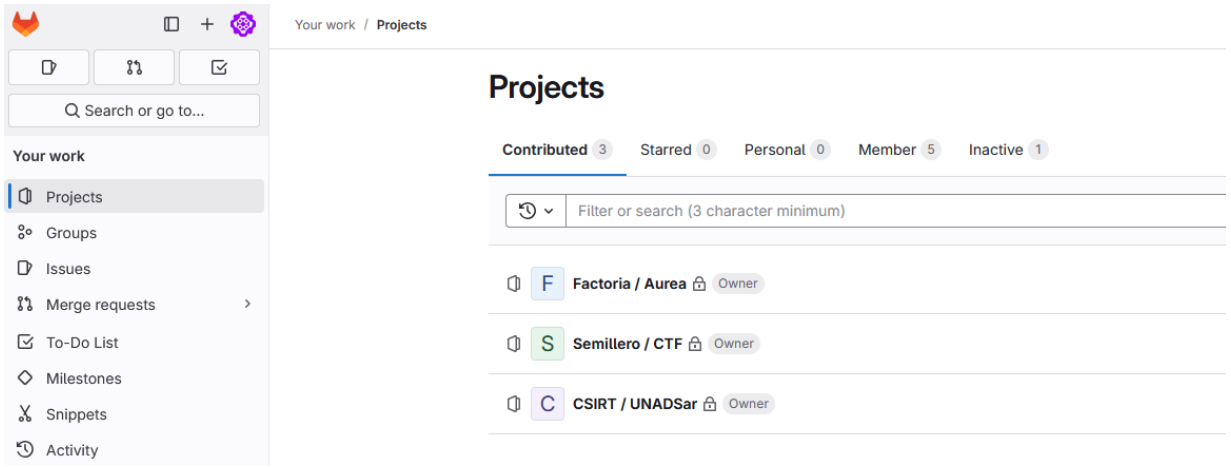
Función principal: Reforzar el proceso de verificación de identidad mediante un mecanismo adicional al nombre de usuario y contraseña, aportando en la reducción significativa del riesgo de accesos no autorizados, **incluso si las credenciales principales han sido comprometidas**.

Estado: Producción (UNADSignature)

Estado: Fase de Pruebas (SII 4.0 y THUMANO)

Repositorio de Código Fuente Institucional

GitLab



https://sar.unad.edu.co:8929/

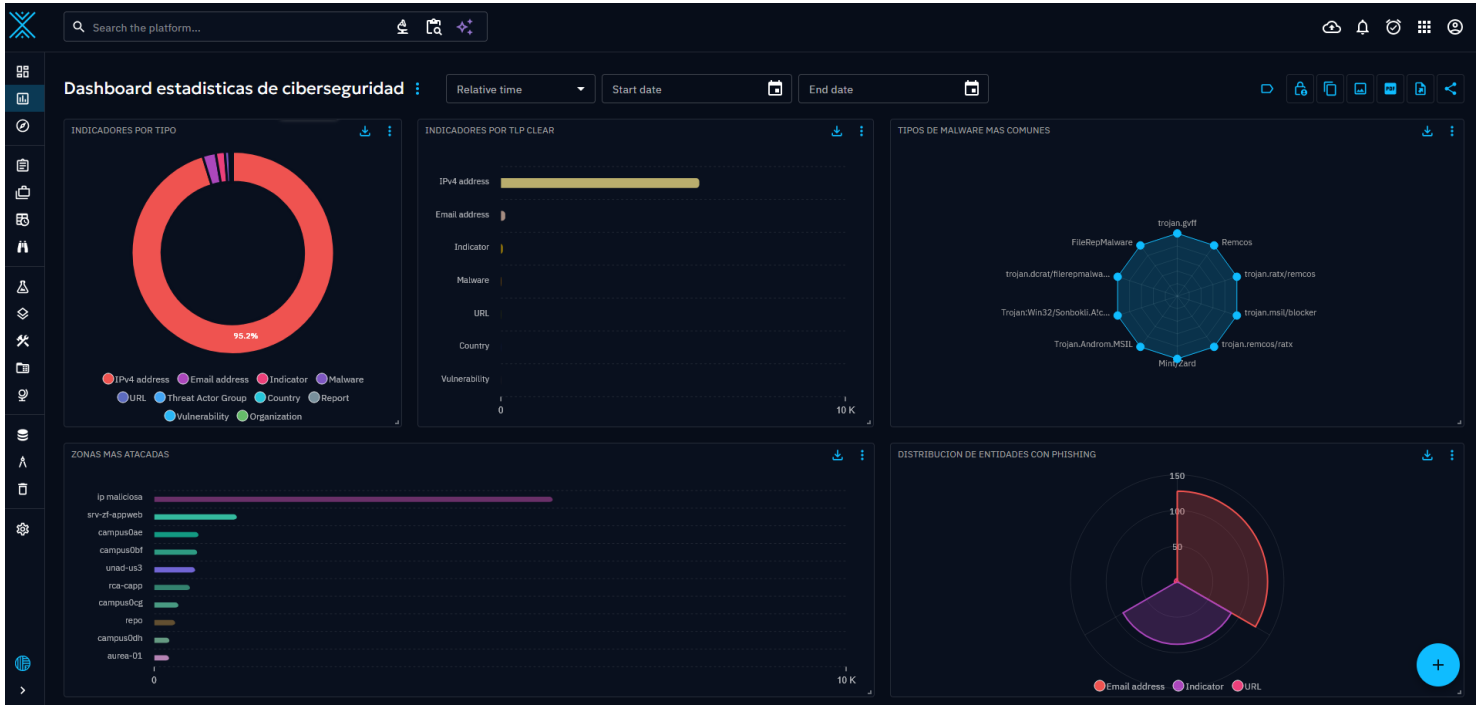
Fortalecimiento de Capacidades

GitLab: Sistema que apoya en la gestión del ciclo de vida del software.

Función principal: Gestionar de forma segura y centralizada el ciclo de vida del código fuente, permitiendo consolidar, evaluar y controlar los cambios realizados en las aplicaciones institucionales, con trazabilidad, gobernanza y mecanismos de protección frente a amenazas internas y externas.

Estado: Producción

Sistema de Inteligencia de Amenazas OPEN-CTI



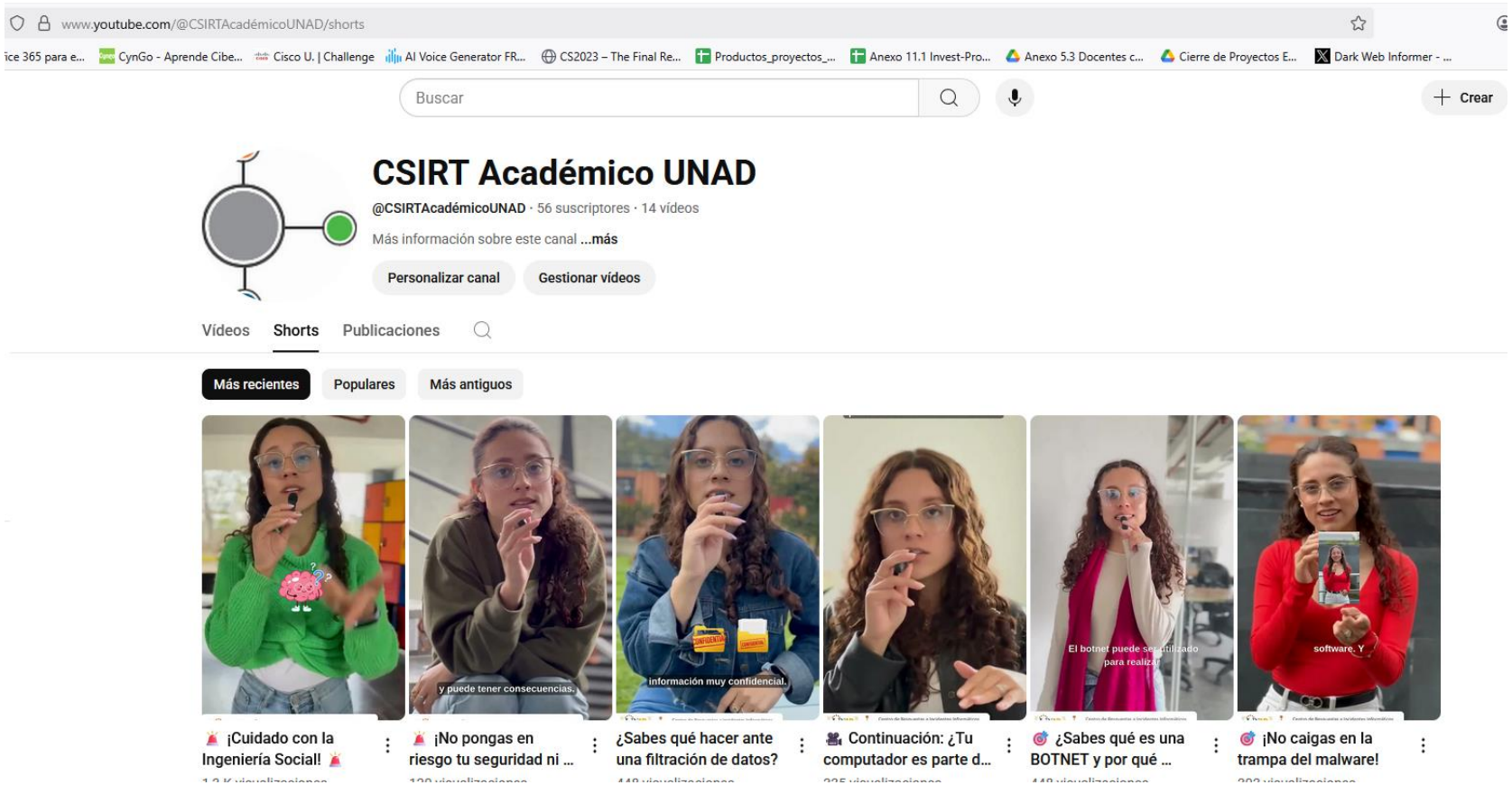
Fortalecimiento de Capacidades

OPEN CTI: Plataforma open-source diseñada para gestionar, analizar y compartir ciber-inteligencia

Función principal: Diseñar, gestionar y automatizar inteligencia de amenazas, ofreciendo a los responsables del riesgo en activos de información una visión profunda, contextualizada y confiable de los riesgos digitales

Estado: En construcción de la Base de datos documental

Educación y Cultura



https://www.youtube.com/@CSIRTAcad%C3%A9micoUNAD/shorts

Universidad Nacional Abierta y a Distancia

ACREDITADA EN ALTA CALIDAD

Gracias

www.unad.edu.co

Síguenos en