

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 1 de 10

UNAD © 2025

1) DATOS GENERALES DEL PROCESO	
1.1) Tipo de Proceso:	Apoyo
1.2) Nombre del Proceso:	Gestión de la seguridad de la información, ciberseguridad y continuidad operacional de la Organización
1.3) 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.
1.4) 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.

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 2 de 10

UNAD © 2025

2) ENTRADAS DEL PROCESO			
2.1) No. Entrada	2.2) Insumos que se Transforman	2.3) Proveedor	2.4) Controles Requeridos
1	Lineamientos y/o políticas definidas para la gestión de la ciberseguridad.	Estado Colombiano Estándares Internacionales relacionados con ciberseguridad	Requerimientos legales
2	Necesidades y expectativas de las partes interesadas en términos de ciberseguridad	Unidades del metasisistema	Matriz de Stakeholders (Partes Interesadas)
3	Resultados de la revisión por la alta dirección de los sistemas que componen el Sistema Integrado de Gestión	Alta Dirección	Acta del Comité de Gestión Integral SIG-MECI e informe de resultados de los sistemas.

asegúrese de consultar la versión vigente en <https://sig.unad.edu.co>

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 3 de 10

UNAD © 2025

4	Alertas sobre detección de patrones de acceso fuera de lo común en tiempo real detectados e identificados a través de los sistemas de información y monitoreo para la seguridad de la información y la ciberseguridad.	Sistemas de información y monitoreo	Reportes de alertas de ciberseguridad.
5	Registros de eventos de ciberseguridad.	Plataforma humana Unadista y partes interesadas	Registro del evento e incidente de ciberseguridad reportado a través de los canales definidos
6	Informe de identificación y evaluación de incidentes de ciberseguridad.	CSIRT Académico UNAD	Gestión de incidentes de ciberseguridad

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 4 de 10

UNAD © 2025

3) DESCRIPCIÓN DEL PROCESO					
3.1) No. Actividad	3.2) Actividades	3.3) PHVA	3.4) Entradas Relacionadas	3.5) Documentación y registros asociados al desarrollo de la actividad	3.6) Responsable
1	Identificar los activos de la información críticos para la universidad y analizar los riesgos asociados.	Planear	1, 3	Catalogación del Inventario de activos críticos de información de la UNAD	Oficial de seguridad / Propietario y responsable del activo
2	Establecer lineamientos de ciberseguridad para proteger los activos críticos de la universidad y responder ante un incidente de ciberseguridad	Planear	1, 2, 5	Lineamientos y procedimientos aprobados	Sistema de Alta Política GPIT - Oficial de seguridad CSIRT Académico UNAD
3	Ejecutar análisis de vulnerabilidades en los	Hacer	4	Reporte de análisis de vulnerabilidades	CSIRT Académico UNAD

“La impresión de este documento se considera COPIA NO CONTROLADA”.

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 5 de 10

UNAD © 2025

	activos críticos de la información de la UNAD, con el fin de detectar brechas y amenazas a los que puedan estar expuestos.				
4	Implementar controles de seguridad que permitan mitigar la ocurrencia de riesgos y amenazas en los activos críticos de la universidad	Hacer	2, 3	Documentación de controles implementados y socializados a partes interesadas.	Propietario responsable del activo crítico / GPIT - Oficial de seguridad/ CSIRT Académico UNAD
5	Fortalecer las capacidades de ciberseguridad, que permitan gestionar proactivamente el entorno digital de la universidad.	Hacer	3	Registro de herramientas tecnológicas	GPIT - Equipo funcional de seguridad / CSIRT Académico UNAD
6	Generar estrategias de comunicación y concientización para el	Hacer	2	Espacios de educación y entrenamiento.	CSIRT Académico UNAD GPIT - Equipo funcional de seguridad /

“La impresión de este documento se considera COPIA NO CONTROLADA”.

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 6 de 10

UNAD © 2025

	fortalecimiento de la ciberseguridad Unadista.			Boletines de ciberseguridad / Notificación de alertas de ciberseguridad /	
7	Recopilar y analizar registros de eventos de ciberseguridad, para correlacionar posibles incidentes	Verificar	3, 4, 5	Alertas de ciberseguridad	CSIRT Académico UNAD
8	Clasificar los incidentes de ciberseguridad según su criticidad.	Actuar	3, 4, 5	Casos relacionados a través del canal establecido para este fin	CSIRT Académico UNAD / GPIT - Oficial de Seguridad / Propietario responsable del activo crítico /
9	Reportar el incidente de ciberseguridad a los propietarios y responsables del activo, y según su criticidad al auditor	Actuar		Reporte del incidente a través de los mecanismos establecidos.	CSIRT Académico UNAD / Oficial de Seguridad / SGRAL / GCMK

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 7 de 10

UNAD © 2025

	metasistémico, a entes de control o partes interesadas.				
10	Atender los eventos o incidentes de ciberseguridad reportados	Actuar	2, 3, 4, 5	Solución a casos reportados a través de los canales establecidos.	Propietario responsable del activo crítico / GPIT - Equipo funcional de seguridad / CSIRT Académico UNAD /
11	Implementar planes de acción ante la recuperación de un incidente de ciberseguridad para garantizar la continuidad de los servicios	Actuar	3, 5	Documentación de controles implementados y pruebas de concepto.	Propietario responsable del activo crítico / GPIT - Equipo funcional de seguridad / CSIRT Académico UNAD /

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 8 de 10

UNAD © 2025

4) SALIDAS DEL PROCESO			
4.1) No. Salida	4.2) Salidas	4.3) Actividades Relacionadas	4.4) Usuario
1	Lineamientos, políticas de cumplimiento y procedimientos implementados por la universidad	2, 4	Comunidad Unadista y partes interesadas
2	Respuesta a las necesidades de las partes interesadas en términos de ciberseguridad.	2,3,4,5,6,10	Comunidad Unadista y partes interesadas
3	Plan de mejoramiento para atender las decisiones tomadas	4,5,6	Comunidad Unadista y partes interesadas

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 9 de 10

UNAD © 2025

	en la revisión por la alta dirección.		
4	Planes para el fortalecimiento de la seguridad de los activos de información	3,8	Propietario y responsable del activo crítico/ Equipo funcional de seguridad /
5	Informe de mitigación de vulnerabilidades y amenazas	3,8	Propietario y responsable del activo crítico/ Equipo funcional de seguridad /
6	Informe de mitigación, y/o recuperación de incidentes	8,9,10	Propietario y responsable del activo crítico/ Equipo funcional de seguridad / entes de control
Consultar Tratamiento a Salidas No Conformes asociadas al Proceso			

	CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	CÓDIGO: C-18
		VERSIÓN: 0-19-03-2025
		PÁGINA: Página 10 de 10

UNAD © 2025

5) NORMATIVIDAD Y DOCUMENTOS DE REFERENCIA	
5.1) Documento de consulta	5.2 Consulta en
Matriz de Marco Legal y Normatividad Aplicable	Ver enlace

6). DESEMPEÑO DEL PROCESO	
6.1) Instrumentos de Seguimiento	6.2) Consulta en
Indicadores	Ver enlace

7). MODIFICACIONES O ACTUALIZACIONES DE LA CARACTERIZACIÓN DE PROCESO		
VERSIÓN	FECHA	DESCRIPCIÓN RESUMIDA DEL CAMBIO
0	19-03-2025	Primera versión emitida