NOMBRE DEL PROCESO O SUBPROCESO: **SEGURIDAD INFORMÁTICA**	Campus Bucaramanga - Líder Nacional del Proceso o subproceso: **JEFE DE SEGURIDAD INFORMÁTICA.**
	Campus Cúcuta y Valledupar - Líder del Proceso o subproceso: **N/A.**

PROPÓSITO DEL PROCESO O SUBPROCESO: garantizar la seguridad de todo el sistema informático, minimizando la vulnerabilidad del mismo y detectando tanto riesgos como violaciones, de manera que se logre un servicio de prevención y seguridad informática seguro, transparente, confiable.

ALCANCE DEL PROCESO O SUBPROCESO: desde el establecimiento de planes de acción de seguridad informática hasta el desarrollo y seguimiento de los mismos en los campus de Bucaramanga, Cúcuta y Valledupar.

PROVEEDORES	ENTRADAS	CICLO	ACTIVIDADES	SALIDAS	CLIENTE
Dirección de TIC Procesos y/o Subprocesos académicos y administrativos	Lineamientos Institucionales Necesidades Informáticas	P	Establecer la propuesta, políticas, normas y buen uso de recursos informáticos Realizar la planeación de las diferentes actividades del subproceso	Propuesta, políticas, normas y buen uso de recursos informáticos por medio de flash informativos o capacitaciones al usuario final Registro en la planeación estratégica anual del aplicativo de administración SGC -VAF	Dirección Tic Procesos y/o Subprocesos académico administrativos
Dirección Tic Procesos y/o Subprocesos académico administrativos	Planeación estratégica registrada en el aplicativo de administración SGC - VAF	H	Ejecución de la planeación estratégica	Registro en la planeación estratégica del aplicativo de administración SGC- VAF	Procesos y/o subprocesos UDES

COPIA NO CONTROLADA

Subproceso IFT Seguridad Informática	Información general de los equipos activos de la red de datos Institucional. Solicitud del Usuario en mesa de servicio y/o notificación de la plataforma de monitoreo y logs de firewall Backups de usuario final y servidores		Revisión de la plataforma de monitoreo y logs de firewall y retroalimentación frente al servicio. Respaldo y restauración de la información. Escaneos de vulnerabilidades a sistemas de información y servidores	Ticket Mesa de servicio Registro de falla o incidentes e información, problemas con los servicios, equipos activos o componentes de la infraestructura tecnológica en el formato SEI-FT-002-UDES Registro en el servidor de respaldo. Registro de las solicitudes de restauración de la información en la aplicación de mesa de servicio Plan de programación y seguimiento de respaldo de la información institucional SEI-FT-006-UDES Tabla de control SEI SEI-FT-005-UDES.	Equipo de Trabajo de Gestión de Tic

Jefe de Seguridad Informática SGC-VAF	Sensores presentados con error de caída o tráfico inusual en la herramientas de monitoreo y escaneos de vulnerabilidades Planeación estratégica registrada en el Aplicativo de administración SGC-VAF. Reporte de resultados de auditorías.	V	Supervisión y monitoreo de tráfico inusual de la red institucional Seguimiento de las vulnerabilidades a sistemas de información y servidores Verificación Del cumplimiento de la planeación estratégica Hacer seguimiento y evaluar el cumplimiento de los lineamientos establecidos dentro del SGC-VAF.	Envió de novedad por correo electrónico a los administradores de las plataformas tecnológicas o sistemas de información Cronograma de Seguimiento de Vulnerabilidades y Tabla de control SEI-FT-004-UDES, SEI-FT-005-UDES Reporte de R2 de la planeación estratégica en el kawak Envío de correo administradores de aplicaciones y servidores	Dirección de TIC Administradores de los sistemas de Información Infraestructura Tecnológica Dirección de TIC Administradores de plataformas o sistemas

COPIA NO CONTROLADA

Jefe de Seguridad Informática Dirección de TIC	Reporte de resultados de auditoría. Retroalimentación planeación anual Estado de cumplimiento de la planeación anual	A	Analizar las causas para determinar acciones de mejora.	Plan de Acción	Seguridad Informática SGC – VAF Dirección de TIC

RECURSOS				
Talento humano: Jefe de Seguridad Informática. Auxiliar de Seguridad Informática. Formación del equipo de trabajo: Tecnólogos y profesionales.	**Infraestructura física:** área administrativa, área para los elementos activos de la red de datos, mobiliario.	**Infraestructura tecnológica:** equipos de cómputo, equipos periféricos, telefonía, biométricos, TV LCD.	**Ambiente de trabajo:** condiciones de humedad, temperatura, iluminación y ruido.	**Recursos económicos:** Presupuesto.

SEGUIMIENTO Y MEDICIÓN	
Matrices de identificación y valoración de riesgos y oportunidades	**Indicadores registrados en el aplicativo de administración del SGC-VAF**

NORMATIVIDAD	
Normatividad legal y reglamentaria **Ley Estatutaria 1581 de 2012** y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: por la cual se dictan disposiciones general es para la protección de datos personales.	**Requisitos de la Norma ISO 9001:2015, aplicables al subproceso** 4 Contexto de la organización 4.1 Comprensión de la organización 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 4.4 Sistema de gestión de la calidad y sus procesos

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Ley 1273 DE 2009: por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 599 DE 2000: por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

CONPES 3854 de 2016 (Política Nacional de Ciberseguridad): Establece las directrices para la implementación de una política integral de ciberseguridad en el país, incluyendo la protección de infraestructuras críticas, regulación de delitos informáticos y promoción de la cultura de ciberseguridad.

Resolución 421 de 2018: Ministerio de Tecnologías de la Información y las Comunicaciones, Lineamientos sobre la Estrategia Nacional de Ciberseguridad. Proporciona directrices sobre cómo las organizaciones deben abordar la seguridad cibernética.

5 Liderazgo
5.1 Liderazgo y compromiso
5.1.1 Generalidades
5.1.2 Enfoque al cliente
5.3 Roles, responsabilidades y autoridades en la organización

6 Planificación
6.1 Acciones para abordar riesgos y oportunidades
6.2 Objetivos de la calidad y planificación para lograrlos
6.3 Planificación de los cambios

7 Apoyo
7.1 Recursos
7.1.1 Generalidades
7.1.2 Personas
7.1.3 Infraestructura
7.1.4 Ambiente para la operación de los procesos
7.1.6 Conocimientos de la organización

7.2 Competencia
7.3 Toma de conciencia
7.4 Comunicación

7.5 Información documentada
7.5.1 Generalidades
7.5.2 Creación y actualización
7.5.3 Control de la información documentada

8 Operación
8.1 Planificación y control operacional
8.2 Requisitos para los productos y servicios
8.2.1 Comunicación con el cliente

COPIA NO CONTROLADA

Ley 1266 de 2008 (Establece disposiciones generales sobre la protección de datos personales): Esta ley regula el manejo de la información personal y establece principios que las entidades deben seguir para garantizar la seguridad y confidencialidad de los datos.

Ley 527 de 1999 (Comercio Electrónico y Firma Digital) : Regula el uso de firmas electrónicas y la seguridad en documentos digitales.

Normatividad institucional aplicable al subproceso

Documentación SGSST.
Reglamento Interno de Trabajo UDES.
Política de tratamiento de protección de datos personales REG-PI-001-UDES.
Políticas Institucionales de los Procesos y subprocesos del SGC-VAF VAF-PI-001-UDES.
Manual de Funciones y Responsabilidades TAH-MN-001-UDES.
Procedimiento de Gestión del Cambio VAF-PR-006-UDES.
Procedimiento de la Gestión del Riesgo VAF-PR-007-UDES.
Procedimiento de Control de Salidas no Conforme VAF-PR-001-UDES.
Procedimiento Control Documentos y Registros GED-PR-004-UDES.
Acciones correctivas preventivas y de mejora VAF-PR-003-UDES.
Procedimiento de Peticiones, Quejas, Reclamos, Sugerencias o Felicitaciones VAF-PR-005-UDES.
Procedimiento supervisión y monitoreo de tráfico inusual de la red institucional SEI-PR-002-UDES.

8.2.2 Determinación de los requisitos para los productos y servicios
8.2.3 Revisión de los requisitos para los productos y servicios
8.2.4 Cambios en los requisitos para los productos y servicios

8.4 Control de los procesos, productos y servicios suministrados externamente
8.4.1 Generalidades
8.4.2 Tipo y alcance del control
8.4.3 Información para los proveedores externos

8.5 Producción y provisión del servicio
8.5.1 Control de la producción y de la provisión del servicio
8.5.2 Identificación y trazabilidad
8.5.3 Propiedad perteneciente a los clientes o proveedores externos
8.5.4 Preservación
8.5.5 Actividades posteriores a la entrega
8.5.6 Control de los cambios

8.6 Liberación de los productos y servicios

8.7 Control de las salidas no conformes

9 Evaluación del desempeño
9.1 Seguimiento, medición, análisis y evaluación
9.1.1 Generalidades
9.1.2 Satisfacción del cliente
9.1.3 Análisis y evaluación

10 Mejora
10.1 Generalidades
10.2 No conformidad y acción correctiva

COPIA NO CONTROLADA

Procedimiento respaldo y restauración de la información SEI-PR-003-UDES. Procedimiento seguimiento de vulnerabilidades a los sistemas de información SEI-PR-004-UDES. Instructivo respaldo y restauración de la información SEI-IN-001-UDES. Instructivo de supervisión y monitoreo de tráfico inusual de la red institucional SEI-IN-002-UDES. Matriz de comunicación Seguridad Informática SEI-MT-001-UDES Matriz de identificación de posibles salidas no conformes Seguridad Informática SEI-MT-005-UDES	10.3 Mejora continua
DOCUMENTOS DE REFERENCIA	**REGISTROS**
Plan de desarrollo Institucional. Proyecto Educativo Institucional. Calendario Académico. Manual de calidad SGC-VAF VAF-MN-001-UDES. Programa de Auditorías VAF-PG-002-UDES. Programa de Capacitación VAF-PG-001-UDES. Programa gestión del conocimiento VAF-PG-004-UDES. Guía de requisitos de documentos para aprobación presupuestal y pagos VAF-GU-001-UDES. Aplicación de la Marca de Conformidad de la Certificación ICONTEC VAF-PC-001-UDES. Guía para el registro de la planeación anual de los procesos y subprocesos del SGC-VAF VAF-GU-002-UDES Guía de Salidas y/o Permisos TAH-GU-002-UDES. Protocolo de Atención al Público TAH-PC-003-UDES. Guía uso adecuado del papel GED-GU-001-UDES. Guía para el manejo de viáticos DIF-GU-002-UDES. Guía de activos fijos para el usuario ACF-GU-001-UDES. Reglamento Auditorios y Sala de Audiovisuales LOG-RG-001-UDES.	Registro de fallas o incidentes SEI-FT-002-UDES. Cronograma de Seguimiento de Vulnerabilidades SEI-FT-004-UDES. Tabla de control SEI-FT-005-UDES. Plan de programación y seguimiento de respaldo de la información institucional SEI-FT-006-UDES. Control de Llamadas VAF-FT-013-UDES. Informe de Gestión VAF-FT-032-UDES. Peticiones, Quejas, Reclamos, Sugerencias o Felicitaciones VAF-FT-003-UDES. Listado de Asistencia GED-FT-031-UDES. Actas GED-FT-032-UDES. Nota Interna GED-FT-015-UDES. Circular Interna GED-FT-016-UDES. Solicitud de Personal TAH-FT-001-UDES. Solicitudes TAH-FT-017-UDES. Solicitud de Salida y/o Permiso TAH-FT-007-UDES. Evaluación de actividades TAH-FT-022-UDES Requisición PRE-FT-004-UDES.

COPIA NO CONTROLADA

Instructivo de Logística LOG-IN-001-UDES. Norma ISO/IEC 27001. Consejo Nacional de Política Económica y Social CONPES 3995 ISO 27001 e ISO 27002. Plan Estratégico TIC DIT-PL-001-UDES. Servicios y Medios de Comunicación Institucionales COM-GU-001-UDES. Guía de Protocolo para Eventos Institucionales COM-GU-002-UDES. Guía de solicitud de servicios COM-GU-003-UDES. Manual de Marca UDES COM-MN-001-UDES. Guía de Presupuesto PRE-GU-001-UDES.	Inventario Único Documental GED-FT-005-UDES Solicitud de Desarrollo de Software SII-FT-001-UDES Autorización Uso de Imagen COM-FT-002-UDES Formato de Préstamo de Equipos e Insumos de la Dirección de Comunicaciones COM-FT-001-UDESCF-GU Ticket Mesa de Ayuda. Correo electrónico. Documento Equivalente a la Factura DIF-FT-006-UDES

COPIA NO CONTROLADA

CONTROL DE CAMBIOS

VERSIÓN 11	DESCRIPCIÓN DEL CAMBIO
FECHA DE APROBACIÓN 22/08/2023	En lineamientos institucionales se agrega en la salida "por medio de flash informativos o capacitaciones al usuario final" En el ciclo HACER en proveedor se incluyó "o seguridad informática", se agregó en la entrada "en mesa de servicio, de monitoreo y logs de firewall", en actividades se agregó "de monitoreo y logs de firewall" en la salida se agregó "en el formato" Se eliminó en el ciclo HACER la entrada "Los logs en tiempo real de los equipos activos de la red de datos y servidores entregados por el subproceso de IFT" Se agregó en el ciclo HACER una entrada "Backups de usuario final y servidores" se agregó en el ciclo HACER en la actividad "" Escaneos de vulnerabilidades a sistemas de información y servidores" En el ciclo VERIFICAR en proveedor jefe de seguridad informática en la parte de entrada se agregó "Sensores presentados con error de caia o tráfico inusual en la herramientas de monitoreo y escaneos de vulnerabilidades" en actividades se agregó "supervisión y monitoreo de tráfico inusual de la red institucional" "Seguimiento de las vulnerabilidades a sistemas de información y servidores" en la salida se agregó "Envío de novedad por correo electrónico a los administradores de las plataformas tecnológicas o sistemas de información" "y tabla de control" "SEI-FT-005-UDES" En el ciclo VERIFICAR se elimina la entrada "supervisión y Monitoreo de la red de datos institucional" y Seguimiento a las vulnerabilidades de los sistemas de información y de la red de datos institucional. En el ciclo VERIFICAR se elimina en la salida Correo electrónico de [reporte de seguimiento], Tabla de control SEI SEI-FT-005-UDES En el ciclo VERIFICAR en proveedor SGC-VAF se elimina "Informe de auditoría VAF-FT-005-UDES" en la actividad se elimina "del plan de trabajo"
RESPONSABLE Oscar Alfonso Larrota Roa Jefe de Seguridad Informática Gelmy Lorena Sánchez Baquero Directora de Gestión Documental	

COPIA NO CONTROLADA

VERSIÓN 11	DESCRIPCIÓN DEL CAMBIO
FECHA DE APROBACIÓN 22/08/2023 RESPONSABLE Oscar Alfonso Larrota Roa Jefe de Seguridad Informática Gelmy Lorena Sánchez Baquero Directora de Gestión Documental	En el ciclo VERIFCAR se agrega en la salida ""envió de correo Administradores y aplicaciones y servidores y se agrega en cliente Dirección TIC y Administradores de plataformas o sistemas En recursos se elimina "número de personas 2;" Se agrega en formación del equipo de trabajo "Tecnólogos y" En requisitos se actualiza el nombre del procedimiento SEI-PR-002-UDES la palabra tráfico inusual, de datos, se actualiza el nombre del instructivo por SEI-IN-002-UDES Instructivo de supervisión y monitoreo de tráfico inusual de la red institucional. En documentos y referencia se agregó "DIT-PL-001-UDES PLAN Estratégico TIC" En registros se elimina "VAF-FT-003-UDES Peticiones, Quejas, Reclamos, Sugerencias o Felicitaciones " y "TAH-FT-022-UDES Evaluación de " Se actualiza imagen de sello IQNET, conforme al cambio que muestra el manual del uso de la marca de conformidad de la certificación ICONTEC para sistemas de gestión. Se ajustan entradas del control de cambios, según Procedimiento Control de Documentos y Registros.
VERSIÓN 12	DESCRIPCIÓN DEL CAMBIO
FECHA DE APROBACIÓN 18/06/2024 RESPONSABLE Oscar Alfonso Larrota Roa Jefe de Seguridad Informática	Se ajusta en normatividad institucional aplicable al subproceso incluyendo trazabilidad SEI-MT-001-UDES Matriz de comunicación Seguridad Informática SEI-MT-005-UDES Matriz de identificación de posibles salidas no conformes Seguridad Informática Se ajusta en documentos de referencia: VAF-PG-004-UDES Programa de gestión del conocimiento VAF-GU-002-UDES Guía para el registro de la planeación anual de los procesos y subprocesos del SGC-VAF Se incluye en la columna de registros: TAH-FT-022-UDES Evaluación de actividades Se ajustan entradas del control de cambios, según Procedimiento Control de Documentos y Registros.

COPIA NO CONTROLADA

VERSIÓN 13	DESCRIPCIÓN DEL CAMBIO
FECHA DE APROBACIÓN 29/04/2025 RESPONSABLE Oscar Alfonso Larrota Roa Jefe de Seguridad Informática Gelmy Lorena Sánchez Baquero Directora de Gestión Documental	Se realiza cambio de la palabra "mesa de ayuda" por "mesa de servicio" por todo el documento Se realiza los siguientes cambios en normatividad Se elimina el siguiente párrafo "Ley 1341 DE 2009: por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones." Se agrega el siguiente párrafo "CONPES 3854 de 2016 (Política Nacional de Ciberseguridad): Establece las directrices para la implementación de una política integral de ciberseguridad en el país, incluyendo la protección de infraestructuras críticas, regulación de delitos informáticos y promoción de la cultura de ciberseguridad." Se agrega el siguiente párrafo "Resolución 421 de 2018: Ministerio de Tecnologías de la Información y las Comunicaciones, Lineamientos sobre la Estrategia Nacional de Ciberseguridad. Proporciona directrices sobre cómo las organizaciones deben abordar la seguridad cibernética." Se agrega el siguiente párrafo "Ley 1266 de 2008 (Establece disposiciones generales sobre la protección de datos personales): Esta ley regula el manejo de la información personal y establece principios que las entidades deben seguir para garantizar la seguridad y confidencialidad de los datos." Se agrega el siguiente párrafo "Ley 527 de 1999 (Comercio Electrónico y Firma Digital) : Regula el uso de firmas electrónicas y la seguridad en documentos digitales." Se ajustan entradas del control de cambios, según Procedimiento Control de Documentos y Registros.

COPIA NO CONTROLADA