Universidad de Cundinamarca | 55 años de vida institucional

Tipos de proveedores que requieren validación por el SGSI

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Proveedor de servicios relacionados a **Talento Humano:**

Contratación y Selección

- (ISO/IEC 27001:2022 - Cláusula 7.1 Recursos)
- (ISO/IEC 27001:2022 - Cláusula 7.2 Competencia)
- (ISO/IEC 27001:2022 - A 6.1 Selección)
- (ISO/IEC 27001:2022 - A.6.2: Términos y Condiciones de Empleo)

Capacitación de personal

- (ISO/IEC 27001:2022 - Cláusula 7.3 Toma de conciencia)
- (ISO/IEC 27001:2022 - A. 6.3 Conciencia de seguridad de la información, educación y formación)

Gestión de nóminas (Tercerización)

- (ISO/IEC 27001:2022 - A. 5.22 Seguimiento, revisión y gestión de los servicios de los proveedores)

Procesos disciplinarios (Tercerización)

- (ISO/IEC 27001:2022 – A 6.4 Proceso Disciplinario)

Elaboración de políticas y programas de beneficios para los empleados

- (ISO/IEC 27001:2022 Cláusula 5.2 Política)
- (ISO/IEC 27001:2022 - A.5.4 Responsabilidades de la dirección)
- (ISO/IEC 27001:2022 - A.6.3 Toma de conciencia, educación y formación en la seguridad de la información)

Proveedores que suministran **Productos e Infraestructura Tecnológica:**

Venta y/o distribución de productos tecnológicos, como dispositivos electrónicos, software, sistemas y/o accesorios

- (ISO/IEC 27001:2022 Cláusula 8 – Operación)
- (ISO/IEC 27001:2022 - A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC)

Mantenimiento de equipos

- (ISO/IEC 27001:2022 – A.7.13 Mantenimiento de equipos)

Capacitación de personal

- (ISO/IEC 27001:2022 Cláusula 8 – Operación)
- (ISO/IEC 27001:2022 – A 8.21 Seguridad de los servicios de red)

Protección de transacciones de los servicios de las aplicaciones

- (ISO/IEC 27001:2022 Cláusula 8 – Operación)
- (ISO/IEC 27001:2022 – A 8.26 Requisitos de seguridad de las aplicaciones)

Proveedores para la tercerización **de Aplicativos:**

Desarrollo contratado externamente

- (ISO/IEC 27001:2022 Cláusula 6.1 Acciones para abordar los riesgos y las oportunidades)
- (ISO/IEC 27001:2022 – A 8.30 "Desarrollo contratado externamente")

Pruebas de seguridad de sistemas

- (ISO/IEC 27001:2022 Cláusula 6.1 Acciones para abordar los riesgos y las oportunidades)
- (ISO/IEC 27001:2022 – A 8.29 Pruebas de seguridad en desarrollo y aceptación)

Separación de los ambientes de desarrollo, pruebas, y operación

- (ISO/IEC 27001:2022 Cláusula 6.1 Acciones para abordar los riesgos y las oportunidades)
- (ISO/IEC 27001:2022 – A 8.31 Separación de entornos de desarrollo, evidencia y producción)

Respaldo de la información

- (ISO/IEC 27001:2022 Cláusula 6.1 Acciones para abordar los riesgos y las oportunidades)
- (ISO/IEC 27001:2022 – A 8.13 Respaldo de la información)
- (ISO/IEC 27001:2022 – A 8.6 Gestión Capacidad)

Proveedor de servicios que tengan **acceso a la información de la Universidad:**

Revisión de las políticas para la seguridad de la información

- (ISO/IEC 27001:2022 Cláusula 5.2 Política)
- (ISO/IEC 27001:2022 Cláusula 6.1 Acciones para abordar los riesgos y las oportunidades)
- (ISO/IEC 27001:2022 – A 5.1 Políticas de seguridad de la información)

Análisis y especificación de requisitos de seguridad de la información

- (ISO/IEC 27001:2022 – A 5.8 Seguridad de la información en la gestión de proyectos)

Gestión de Eventos

- (ISO/IEC 27001:2022 - Cláusula 6 Planificación)
- (ISO/IEC 27001:2022 - Cláusula 7 Apoyo)
- (ISO/IEC 27001:2022 - Cláusula 8 Operación)
- (ISO/IEC 27001:2022 – A 5.24 Planificación y preparación de la gestión de incidentes, de seguridad de la información)
- (ISO/IEC 27001:2022 – A 6.8: Reporte de eventos de seguridad de la información)

Servicios de Salud

- (ISO/IEC 27001:2022 – A 5.19 Seguridad de la información en las relaciones con los proveedores)
- (ISO/IEC 27001:2022 – A 5.20 Tratamiento de la seguridad de la información, en los acuerdos con los proveedores)

Servicios Contables

- (ISO/IEC 27001:2022 – A 5.19 Seguridad de la información en las relaciones con los proveedores)

Nota: Deben considerarse los documentos generados por el Sistema de Gestión de Seguridad de la Información (SGSI), tales como manuales, guías e instructivos, los cuales están disponibles en el Modelo de Operación Digital.