

ACUERDO N° 5808

El Consejo Superior de la FUNDACIÓN UNIVERSITARIA DE CIENCIAS DE LA SALUD, en uso de sus atribuciones legales y de acuerdo con el capítulo VII de los Estatutos de la FUNDACIÓN UNIVERSITARIA DE CIENCIAS DE LA SALUD, ratificados mediante Resolución No. 021948 de 24 de noviembre de 2020 del Ministerio de Educación Nacional, en sesión ordinaria No. 603 del dieciocho (18) de abril del año 2023, y

CONSIDERANDO

Que: La información es uno de los principales activos para el desarrollo de las operaciones y cumplimiento de los objetivos misionales y estratégicos de la FUCS. En consecuencia, la información debe ser protegida de los riesgos que afecten su confidencialidad, integridad y disponibilidad.

Que: Mediante la evolución de nuevas tecnologías de la información y la puesta a producción de servicios (Herramientas/productos y software) para el cubrimiento de las necesidades de la FUCS y la optimización de procesos misionales, se incorpora el requerimiento de protección de información tratada; de igual forma todo aquello que contemple en proporcionar seguridad a sistemas, redes, dispositivos, software y servicios que son utilizados en la FUCS.

Que: Es potestad del Consejo Superior estudiar, establecer y modificar Políticas de la Universidad,

ACUERDA

ARTÍCULO PRIMERO: Aprobar modificar el nombre del documento denominado "Manual de Políticas de Seguridad de la Información" a "Política de Seguridad de la Información".

ARTÍCULO SEGUNDO: Aprobar actualizar la introducción, las generalidades, el alcance y el marco normativo de las políticas.

ARTÍCULO TERCERO: Aprobar actualizar los objetivos específicos de la siguiente manera:

Objetivos Específicos
Generar cultura de uso seguro de los sistemas de información.
Fortalecer la Seguridad de la Información, mediante la implementación de mecanismos de control que permitan mitigar los riesgos.
Gestionar a la mayor brevedad los eventos o incidentes de seguridad de la información, identificados y originados por el incumplimiento de las políticas de seguridad de la información.

ARTÍCULO CUARTO: Aprobar modificar la redacción del numeral “Roles, Responsabilidades y Autoridades”, y los controles asociados, de la siguiente manera:

Controles

Responsable	Actividades
Comité de Seguridad de la Información	<p>Se adicionan las siguientes actividades:</p> <ul style="list-style-type: none"> • Aprobar roles relacionados con la seguridad de la información en los diferentes niveles jerárquicos. • Definir planes de acción para subsanar debilidades en controles.
Seguridad de la Información	<p>Se incluyen las siguientes actividades:</p> <ul style="list-style-type: none"> • Gestionar en conjunto con la División de Desarrollo Tecnológico los controles para mitigar los riesgos asociados a la Seguridad de la Información. • Monitorear la aplicación y cumplimiento de los controles definidos e informar al Comité de Seguridad de la Información los resultados correspondientes.
División de Desarrollo Tecnológico	<p>Se incluye la siguiente actividad:</p> <ul style="list-style-type: none"> • Gestionar en conjunto con Seguridad de la Información los controles para mitigar los riesgos asociados a la Seguridad de la Información.
División de Gestión del Talento Humano	<p>Se actualiza la siguiente actividad:</p> <ul style="list-style-type: none"> • Notificar a los nuevos colaboradores sobre la obligación de cumplir con las Políticas de Seguridad de la Información descritas en el presente documento. <p>Se incluye la siguiente actividad:</p> <ul style="list-style-type: none"> • Definir y aplicar los procesos disciplinarios a que haya lugar por las faltas identificadas a la Política de Seguridad de la Información.
División de Auditoría.	<p>Se adiciona la siguiente actividad:</p> <ul style="list-style-type: none"> • Auditar la política de Protección de Datos Personales.

ARTÍCULO QUINTO: Aprobar modificar la redacción del numeral “Funciones del Comité de Seguridad de la Información”, de la siguiente manera:

Funciones del Comité de Seguridad de la Información
Estar atento a los riesgos en materia de seguridad de la información y protección de datos personales, sus cambios significativos y afectación de los recursos de información, frente a las principales amenazas.
Conocer los eventos, incidentes y/o riesgos relativos a la seguridad de la información y las acciones de mitigación establecidas, así como proponer y aprobar acciones de mejora que se consideren pertinentes frente a los mismos.
Solicitar a los responsables de los procesos de gestión que se alineen con la Política de Seguridad de la Información, cuando se detecten actividades o controles que no se ajusten a lo descrito en la política.
Coordinar, evaluar y promover la implementación de los controles específicos de seguridad de la información para nuevos servicios tecnológicos o sistemas, o procesos en los que se evidencie su necesidad de implementación.
Respaldar e impulsar la difusión de la Política de Seguridad de la Información y la Política de Protección de Datos personales, así como su importancia, dentro de la comunidad universitaria.
Se adicionan las siguientes funciones: <ul style="list-style-type: none">• Aprobar la matriz de roles y perfiles de los Sistemas de información.• Revisar las actualizaciones anuales y modificaciones necesarias que requiera la Política de tratamiento de datos personales de la Institución, para su aprobación por el Consejo Superior.• Las demás establecidas en la Política de Seguridad de la Información

ARTÍCULO SEXTO: Aprobar modificar la redacción del numeral “Organización Interna”, de la siguiente manera:

Organización Interna
Todos los colaboradores (directivos, administrativos, docentes, practicantes, aprendices), estudiantes y terceros (contratistas y/o proveedores), deben actuar de acuerdo con la Política de Seguridad de la Información y los controles aquí establecidos, participando en las revisiones de seguridad que se lleven a cabo. Adicionalmente, presentarse en las distintas capacitaciones y/o jornadas de sensibilización lideradas por la División de Desarrollo Tecnológico y Seguridad de la Información.
<ul style="list-style-type: none">• Aceptar y cumplir la Política de Seguridad de la Información y los controles que se establezcan en la FUCS.• Los colaboradores deben utilizar la información de la FUCS exclusivamente para fines laborales, quedando prohibido explícitamente el uso o divulgación para fines comerciales y/o privados no autorizado.

ARTÍCULO SÉPTIMO: Aprobar modificar el capítulo "Gestión de Activos de Información", de la siguiente manera:

- A. Se modifica la periodicidad de revisión de los activos de información, pasando de revisión anual a cada dos años.

Gestión de Activos de Información
<p>Tercer párrafo</p> <p>Los activos de información deben ser identificados y clasificados acordes con la criticidad del activo. El inventario de activos de información se revisará y actualizará cada dos años, identificando: responsable de los activos, custodios, ubicación, amenazas, vulnerabilidades, usuarios y los controles que se tienen implementados para garantizar la Confidencialidad, Integridad y Disponibilidad de la información.</p>

- B. Clasificación de la Información.

Se modifica la periodicidad de actualización de los activos de información por parte de los líderes de área, pasando de 12 a 24 meses.

Texto a actualizar
<p>Los líderes de las dependencias quienes para el efecto son los responsables de la información, deberán identificar los activos de información de las áreas a su cargo, con el fin de elaborar el inventario de activos de información y velar por mantenerlo actualizado con una periodicidad de 24 meses o cuando sea necesario.</p>

- C. Se modifican los siguientes controles:

Responsable	Actividades
Seguridad de la Información	<p>Se eliminan las siguientes actividades:</p> <ul style="list-style-type: none">• Proveer los métodos de cifrado de la información y gestionar la contratación y actualización de las herramientas tecnológicas usadas para este fin.• Debe garantizar la destrucción de información física, cuando se ha cumplido su ciclo de almacenamiento. <p>Se actualizan las siguientes actividades:</p> <ul style="list-style-type: none">• Monitorear que la depuración y la eliminación de la información se realice de una manera efectiva a través de los mecanismos necesarios.• Monitorear la supervisión sobre el cumplimiento de los ANS - Acuerdos de Niveles de Servicio y de intercambio de información establecidos con el proveedor de custodia externa de los documentos de la institución (en

	caso de presentarse la situación de almacenamiento externo).
División de Desarrollo Tecnológico	Se adiciona este responsable con la siguiente actividad: <ul style="list-style-type: none"> • Proveer los métodos de cifrado de la información y gestionar la contratación y actualización de las herramientas tecnológicas usadas para este fin.
Gestión Documental	Se adiciona este responsable con las siguientes actividades: <ul style="list-style-type: none"> • Velar por la destrucción de información física, cuando se ha cumplido su ciclo de almacenamiento. • Mantener actualizadas las tablas de retención documental y velar por su aplicación.

ARTÍCULO OCTAVO: Aprobar modificar el capítulo “Seguridad del Talento Humano, lo siguiente:

A. “Vinculación de Colaboradores”

Responsable	Actividades
Gerencia – División de Gestión del Talento Humano	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Garantizar que los colaboradores de la institución conozcan, acepten y firmen los documentos de confidencialidad, seguridad de la información y tratamiento de datos personales; estos documentos deben estar anexos y hacer parte integral del proceso de contratación.

B. “Desvinculación, Licencias, Vacaciones, o Traslados de Colaboradores y Personal Provisto por Terceros”
 Controles

Responsable	Actividades
Oficina de Auditoría de Gestión	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Monitorear el cumplimiento de las políticas y controles establecidos.

ARTÍCULO NOVENO: Aprobar modificar el capítulo “Seguridad de las Operaciones”, los controles establecidos para el numeral “Asignación de Responsabilidades Operativas”, de la siguiente manera:

Controles

Responsable	Actividades
Seguridad de la Información	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Apoyar en las recomendaciones de seguridad sobre las soluciones para la infraestructura tecnológica de la FUCS.

ARTÍCULO DÉCIMO: Aprobar modificar en el capítulo “Seguridad de las Operaciones”, los controles establecidos para el numeral “Protección Frente a Software Malicioso”, de la siguiente manera:

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • Mantener instalado, actualizado y activo el software antivirus en todo el parque computacional de la FUCS.
Usuarios	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • No instalar ningún tipo de software o programa. Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Notificar de forma inmediata a Soporte Técnico y a Seguridad de la Información, cuando se detecte o sospeche alguna infección por software malicioso.
Seguridad de la Información	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • Monitorear mínimo una vez al mes la actualización de las bases de datos del software antivirus y su activación en todo el parque computacional de la FUCS.

ARTÍCULO UNDÉCIMO: Aprobar modificar en el capítulo “Copias de Respaldo de la Información”, lo siguiente:

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • Generar campañas que permitan conocer los procedimientos de respaldo de información.
Seguridad de la información.	Se adiciona este responsable con las siguientes actividades: <ul style="list-style-type: none"> • Generar campañas que permitan conocer los procedimientos de respaldo de información. • Monitorear la aplicación de los procedimientos para la generación, almacenamiento y restauración de las copias de respaldo de la información, garantizando su integridad,

	disponibilidad y confidencialidad.
--	------------------------------------

ARTÍCULO DUODÉCIMO: Aprobar modificar en el capítulo “Seguridad de las Operaciones”, lo siguiente:

A. “Eventos y Monitoreos a los Recursos Tecnológicos y Sistemas de Información”

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Debe establecer e implementar los tipos de eventos que deben registrar los logs o registros de auditoría, y garantizar la obtención de los mismos, tanto de recursos tecnológicos como de sistemas de información.
Desarrolladores, consultores, analistas entre otros (Internos y Externos)	Se complementan los responsables y se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Informar sobre eventos de los sistemas de información y/o plataforma tecnológica relacionados con interrupciones, acceso, modificación de acuerdo con los lineamientos establecidos por la División de Desarrollo Tecnológico.
Seguridad de la Información.	Se adiciona este responsable con las siguientes actividades: <ul style="list-style-type: none"> • Monitorear la gestión de usuarios en los Sistemas de Información. • Verificar el reporte de análisis de vulnerabilidades realizado por la División de Desarrollo Tecnológico y/o el tercero contratado; y verificar la ejecución de los planes de remediación.

B. “Seguridad para los Equipos Institucionales”

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Definir, implementar y asegurar el cumplimiento de los estándares de seguridad/configuración fiable para los equipos asignados a los empleados de la FUCS. Se adicionan las siguientes actividades: <ul style="list-style-type: none"> • Realizar la asignación de recursos tecnológicos. • Acompañar los movimientos de recursos tecnológicos.

Seguridad de la Información	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Monitorear periódicamente el cumplimiento de las configuraciones en los equipos de cómputo, con base en el estándar de seguridad definido.
Servicios administrativos	Se adiciona este responsable con la siguiente actividad: <ul style="list-style-type: none"> • Monitorear que la empresa de seguridad revise los accesos físicos en horas no hábiles a las áreas donde se procesa información.
Usuarios	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • No realizar movimientos de equipos tecnológicos.

ARTÍCULO DECIMO TERCERO: Aprobar modificar en el capítulo "Seguridad en las Comunicaciones", lo siguiente:

A. "Gestión y Aseguramiento de las Redes de Datos"

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se actualizan las siguientes actividades: <ul style="list-style-type: none"> • Definir y aplicar los controles necesarios para mitigar los riesgos de seguridad de la información que viajan a través de las redes de datos de la FUCS. • Documentar y mantener la configuración de los componentes de la plataforma tecnológica de la FUCS.

B. Uso del Correo Electrónico

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Diseñar e implementar la estrategia que proporcione un ambiente seguro y controlado que incluya los mecanismos de protección y detección para el buen funcionamiento de la plataforma de correo electrónico.
Seguridad de la Información	Se incluye la siguiente actividad: <ul style="list-style-type: none"> • Monitorear el uso del correo institucional para mitigar el riesgo de fuga de información y garantizar su uso exclusivo para labores institucionales.

Usuarios	<p>Se actualizan las siguientes actividades:</p> <ul style="list-style-type: none"> • No realizar el envío de cadenas de mensajes que contengan información no institucional (político, religioso, comercial, contenido discriminatorio, pornografía, etc.). • Reportar correos electrónicos de procedencia sospechosa, a las cuentas de correo de Soporte Técnico y Seguridad de la Información.
----------	---

C. Uso Adecuado de Internet

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	<p>Se actualiza la siguiente actividad:</p> <ul style="list-style-type: none"> • Establecer e implementar controles que garanticen el óptimo funcionamiento del servicio de internet (red interna), que restrinja el acceso y/o descarga de software, malware o sitios que representen una amenaza para la Seguridad de la Información.
Seguridad de la Información	<p>Se incluye la siguiente actividad:</p> <ul style="list-style-type: none"> • Realizar monitoreo sobre el uso de internet y verificar las configuraciones de restricciones definidas.
Usuarios	<p>Se actualizan las siguientes actividades:</p> <ul style="list-style-type: none"> • Hacer uso adecuado del servicio de internet de acuerdo con las actividades que se desarrollan. Está prohibido la descarga e instalación de software no autorizado en las estaciones de trabajo o dispositivos móviles institucionales.

D. Intercambio de Información

Controles

Responsable	Actividades
División Jurídica	<p>Se adicionan las siguientes actividades:</p> <ul style="list-style-type: none"> • Definir los procedimientos, servicios y herramientas para proteger con controles la información transmitida a los terceros que tienen relación con la FUCS. <p>Se actualiza la siguiente actividad:</p> <ul style="list-style-type: none"> • Elaborar y/o revisar aquellos contratos que se realicen con terceros y que incluyan acuerdos de confidencialidad o de intercambio de información, especificando las condiciones contractuales legales para los terceros en caso de divulgación no autorizada de la información entregada por la FUCS.

División Desarrollo Tecnológico	de	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> Definir e implementar los procedimientos, servicios y herramientas para proteger con controles la información transmitida a los terceros que tienen relación con la FUCS.
Gestión Documental		Se adiciona la siguiente actividad: <ul style="list-style-type: none"> Definir los procedimientos, servicios y herramientas para proteger con controles la información transmitida a los terceros que tienen relación con la FUCS. Se actualiza la siguiente actividad: <ul style="list-style-type: none"> Acoger los procedimientos de intercambio de información con terceros en medio físico o digital, así como garantizar la restricción de acceso al personal no autorizado, para evitar la divulgación no autorizada, destrucción, alteración y/o pérdida de la información.
Usuarios		Se actualiza la siguiente actividad: <ul style="list-style-type: none"> Hacer uso de medios adecuados para enviar o recibir información confidencial, no se debe compartir la información, sin previo contrato de transmisión de datos, no se debe utilizar el correo electrónico personal y/o medios no autorizados por la FUCS para enviar o recibir información confidencial de la FUCS.
Seguridad de la Información		Se adiciona este responsable con la siguiente actividad: <ul style="list-style-type: none"> Definir los procedimientos, servicios y herramientas para proteger con controles la información transmitida a los terceros que tienen relación con la FUCS.

ARTÍCULO DECIMO CUARTO: Aprobar modificar en el capítulo "Control de Acceso", lo siguiente:

A. "Acceso a Redes y Recursos de Red"

Controles

Responsable	Actividades
División Desarrollo Tecnológico	de Se actualizan las siguientes actividades: <ul style="list-style-type: none"> Establecer e implementar el procedimiento de autorización y control de acceso a las redes y recursos tecnológicos de la FUCS, con el fin de proteger el ingreso indebido de terceros. Establecer e implementar controles de autenticación y autenticidad de los usuarios internos y externos a las redes y/o recursos de red de la FUCS. Se deben tratar las redes inalámbricas "WIFI" como redes externas y separarlas de las redes internas, para garantizar el cumplimiento de los principios de Seguridad de la Información de la FUCS.

B. "Administración de Accesos de Usuarios"

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se actualizan las siguientes actividades: <ul style="list-style-type: none"> • Establecer e implementar el procedimiento formal para la administración del acceso lógico de los usuarios en las redes de datos, sistemas de información de la institución y demás recursos tecnológicos. • Controlar la asignación de privilegios a roles y a usuarios, establecidos por el Comité de Seguridad de la Información.
Seguridad de la Información	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • Realizar monitoreo a los accesos lógicos, creación, modificación o bloqueo de cuentas de usuarios para validar que cuenten con la respectiva aprobación de los líderes de proceso. Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Establecer los perfiles de usuario (roles, funcionalidades y permisos), junto con los líderes de los activos de información y el Comité de Seguridad de la Información.
Comité de Seguridad de la Información.	Se incluye la siguiente actividad: <ul style="list-style-type: none"> • Definir las actividades pertinentes para la administración de roles y perfiles.
División de Gestión del Talento Humano	Se actualiza y traslada la siguiente actividad: <ul style="list-style-type: none"> • Deberá mediante procedimiento informar a la División de Desarrollo Tecnológico y a Seguridad de la Información las novedades del personal, en las que se requiera modificación de cuentas, accesos y privilegios de usuarios.

C. Uso de Altos Privilegios y Utilitarios de Administración

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se incluye la siguiente actividad: <ul style="list-style-type: none"> • Restringir el acceso a programas utilitarios solo a los perfiles administradores en los equipos de cómputo.

D. Control de Accesos a Sistemas y Aplicativos

Controles

Responsable	Actividades
<ul style="list-style-type: none"> • División de Desarrollo Tecnológico 	<p>Se adiciona este responsable con las siguientes actividades:</p> <ul style="list-style-type: none"> • Debe establecer los controles de acceso a los ambientes productivos de los aplicativos, así mismo, debe garantizar que los desarrolladores internos o externos cuenten con acceso limitado y controlado tanto a los datos como a toda información que se encuentre en los ambientes de producción. • Suministrar el repositorio de archivos con acceso controlado y definición de privilegios para almacenar el código fuente de los Sistemas de información propios.
<ul style="list-style-type: none"> • Seguridad de la Información 	<p>Se actualiza la siguiente actividad:</p> <ul style="list-style-type: none"> • Monitorear periódicamente la definición de perfiles y asignación de privilegios a los usuarios que acceden en los sistemas de información, así mismo, notificar al Comité de Seguridad de la Información. <p>Se adiciona la siguiente actividad:</p> <ul style="list-style-type: none"> • Realizar verificaciones periódicas y aleatorias a las actividades ejecutadas con el usuario administrador de los sistemas de información críticos de la FUCS.
<ul style="list-style-type: none"> • Usuarios 	<p>Se actualiza la siguiente actividad:</p> <ul style="list-style-type: none"> • Para los distintos aplicativos, sistemas de información y medios, los propietarios deben definir qué información sensible puede ser eliminada y tener soporte de la eliminación de dicha información, como es el caso de los datos personales, datos sensibles o financieros, cuando estos ya no son requeridos. Para lo anterior, es necesario contar con el acompañamiento de la División Jurídica y Seguridad de la Información.

ARTÍCULO DÉCIMO QUINTO: Aprobar modificar en el capítulo “Adquisición, Desarrollo y Mantenimiento de Sistemas de Información”, lo siguiente:

A. “Establecimiento de Requisitos de Seguridad”

Controles

Responsable	Actividades
<p>División de desarrollo tecnológico</p>	<p>Se eliminan las siguientes actividades:</p> <ul style="list-style-type: none"> • Definir un área física designada y con las medidas de protección dentro de la FUCS para el desarrollo de sistemas de información o software. • Las áreas propietarias de los sistemas de información deben apoyar a la División de Desarrollo Tecnológico con los requerimientos para la adquisición, desarrollo de software o sistemas de información, teniendo en cuenta los controles como; autenticación, acceso y diseño de aplicaciones que garanticen la seguridad de la información.

Propietarios de los Sistemas de Información.	<p>Se incluye la siguiente actividad:</p> <ul style="list-style-type: none"> • Establecer los requerimientos que incluyan las necesidades propias de los sistemas de información.
--	--

B. "Desarrollo Seguro, Realización de Pruebas y Soporte de Sistemas"

Controles

Responsable	Actividades
Propietarios de los Sistemas de Información	<p>Se actualizan las siguientes actividades:</p> <ul style="list-style-type: none"> • Realizar metódicamente las pruebas de funcionalidad que aseguren el cumplimiento de los requerimientos y realizar la documentación de las pruebas. • Aprobar el paso a producción de los desarrollos/ajustes/cambios de versiones, luego de la revisión del cumplimiento de los requerimientos.
División de Desarrollo Tecnológico	<p>Se adicionan las siguientes actividades:</p> <ul style="list-style-type: none"> • Realizar metódicamente las pruebas que aseguren el cumplimiento de los requerimientos de seguridad, realizar la documentación de las pruebas y correcciones realizadas necesarias antes del paso a producción. • Llevar un control de cambios de las migraciones/ajustes/versiones entre los diferentes ambientes de desarrollo, pruebas, calidad y producción de los productos entregados.
Desarrolladores (Internos o Externos)	<p>Se adiciona la siguiente actividad:</p> <ul style="list-style-type: none"> • Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados.

C. Gestión de la Prestación de Servicios de Terceras Partes

Controles

Responsable	Actividades
Supervisores de Contratos Terceros	<p>Se actualiza la siguiente actividad:</p> <ul style="list-style-type: none"> • Monitorear periódicamente el cumplimiento de acuerdos de niveles de servicio. <p>Se elimina la siguiente actividad:</p> <ul style="list-style-type: none"> • Administrar y controlar las novedades y monitorear la aparición de nuevos riesgos en el suministro de servicios, de los proveedores. <p>Se adiciona la siguiente actividad:</p> <ul style="list-style-type: none"> • Identificar posibles situaciones anómalas que representen riesgo para la institución en la ejecución del contrato y reportarlas a la Gerencia y a la División Jurídica.

ARTÍCULO DÉCIMO SÉXTO: Aprobar modificar el capítulo "Relación con los Proveedores", de la siguiente manera:

Controles

Responsable	Actividades
Proveedores y/o Terceros	Se actualizan las siguientes actividades: <ul style="list-style-type: none">• Todos los proveedores y terceros que vayan a tener acceso a información confidencial de la FUCS, deberán firmar acuerdos de confidencialidad y/o acuerdos de transmisión de datos personales.• Deben cumplir con los controles y políticas establecidas en la Política de Seguridad de la Información de la FUCS.

ARTÍCULO DÉCIMO SÉPTIMO: Aprobar modificar en el capítulo "Gestión de Incidentes de Seguridad", lo siguiente:

A. "Reporte y Tratamiento de Eventos o Incidentes de Seguridad"

Controles

Responsable	Actividades
Propietarios de los Activos de Información	Se actualiza la siguiente actividad: <ul style="list-style-type: none">• Reportar los eventos o incidentes de seguridad a Seguridad de la Información y a la División de Desarrollo Tecnológico.
División de Desarrollo Tecnológico	Se adicionan las siguientes actividades: <ul style="list-style-type: none">• Asignar personal calificado para realizar las revisiones necesarias de los eventos o incidentes de seguridad reportados, con el fin de identificar sus causas y que permita proporcionar soluciones, así como prevenir su recurrencia.• Establecer en conjunto con Seguridad de la Información, responsabilidades y procedimientos que permitan una respuesta rápida y efectiva a los eventos o incidentes de seguridad de la información.• Implementar un sistema de gestión de conocimiento que permita tener respuesta rápida a eventos o incidentes conocidos, así como la documentación de los nuevos incidentes.
Comité de Seguridad de la Información	Se eliminan las 5 actividades vigentes y se deja la siguiente: <ul style="list-style-type: none">• Apoyar las iniciativas de comunicación y sensibilización frente a los eventos de seguridad de la información.
Seguridad de la Información	Se elimina la siguiente actividad: <ul style="list-style-type: none">• Documentar procedimientos, donde se establezcan responsables y actividades que permiten brindar respuestas oportunas a los eventos reportados. Se adiciona la siguiente actividad:

	<ul style="list-style-type: none"> • Evaluar los eventos o incidentes de Seguridad de la Información, así como realizar el escalamiento al Comité de Seguridad de la Información para los casos que requieran evaluación conjunta.
Usuarios	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Reportar oportunamente cualquier evento que pueda ser clasificado como incidente para la seguridad de la información, así como la pérdida o divulgación no autorizada de información, comunicando lo correspondiente a Seguridad de la Información y a la División de Desarrollo Tecnológico para la gestión respectiva.

B. Desarrollo Gestión de Vulnerabilidades

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Coordinar y realizar directamente o a través de un tercero especializado, una vez al año, el análisis de vulnerabilidades técnicas a la infraestructura tecnológica de la FUCS.

ARTÍCULO DÉCIMO OCTAVO: Aprobar modificar en el capítulo “Inclusión de Seguridad de la Información en la Gestión de la Continuidad del Negocio”, los controles definidos para el numeral “Continuidad, Contingencia, Recuperación y Retorno a la Normalidad con Consideraciones de Seguridad de la Información”, lo siguiente:

Controles

Responsable	Actividades
Consejo Superior	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • Identificar y formalizar los procesos críticos en la Institución, como eje y punto de partida para orientar los recursos en caso de eventos que afectan la continuidad del servicio.

ARTÍCULO DÉCIMO NOVENO: Aprobar modificar en el capítulo “Cumplimiento”, lo siguiente:

A. “Cumplimiento con Requisitos Legales y Contractuales”

Controles

Responsable	Actividades
-------------	-------------

División Jurídica	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • Identificar normatividad de cumplimiento frente a propiedad intelectual y derechos de autor, con el fin de establecer de manera adecuada en los contratos que se realicen con proveedores.
Seguridad de la Información	Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • Identificar normatividad de cumplimiento frente a Seguridad de la Información.

B. Privacidad y Protección de Datos Personales

Controles

Responsable	Actividades
Áreas/Dependencias /Oficinas/Divisiones que Procesan Datos Personales	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Para el procesamiento de datos personales de los titulares identificados en la Política de Protección de Datos Personales de la FUCS, se debe contar con la respectiva autorización del titular de la información para poder tratarla en el desarrollo de las acciones que se lleven a cabo por la FUCS.
Seguridad de la Información	Se adicionan las siguientes actividades: <ul style="list-style-type: none"> • Supervisar y monitorear el cumplimiento de los controles establecidos en la Política de Protección de Datos Personales de la FUCS. • Realizar seguimiento al programa integral de Gestión de Datos Personales. • Atender las solicitudes judiciales y/o de entes de control que requieren datos personales de conformidad con la ley.
Todos los Usuarios	Se actualiza la siguiente actividad: <ul style="list-style-type: none"> • Guardar la reserva absoluta de la información y bases de datos a cargo de la FUCS que por cualquier motivo conozcan. Se adiciona la siguiente actividad: <ul style="list-style-type: none"> • Atender las solicitudes judiciales y/o de entes de control que requieren datos personales de conformidad con la ley.

ARTÍCULO VIGÉSIMO: Aprobar incluir y actualizar definiciones y referencias, en el capítulo de "TÉRMINOS Y DEFINICIONES".

ARTICULO VIGÉSIMO PRIMERO: El presente acuerdo rige a partir de su fecha de expedición.

NOTIFIQUESE Y CÚMPLASE

Dado en Bogotá D.C., a los dieciocho (18) días del mes de abril del año 2023.



JORGE GÓMEZ CUSNIR
Presidente
Consejo Superior



JORGE LUIS HERRERA
Secretario
Consejo Superior