CONTINUIDAD DEL NEGOCIO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaboró:	Revisó:	Aprobó:
_____	_____	_____
Contratista Seguridad de la Información	Asesor TIC	Rector(a)

1. OBJETIVO

Definir la forma como la Institución Universitaria Colegio Mayor del Cauca - IUCMC gestionara su infraestructura y servicios de TI para mantener la seguridad de la información en caso de un desastre o de otro incidente disruptivo.

2. ALCANCE

El procedimiento aplica para todos los desastres e incidentes disruptivos que se presenten en la institución e involucre las actividades críticas dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI). Este documento debe ser conocido y aplicado por todos los funcionarios y contratistas de la institución.

El presente documento complementa el procedimiento de gestión de incidentes de seguridad de la información.

3. DEFINICIONES

Disrupción o interrupción: Evento o circunstancia que puede afectar significativamente las operaciones críticas de la organización. Esto incluye cualquier ocurrencia inesperada de causa natural, técnica o humana. [ISO/IEC 22301: 2012].

Continuidad del Negocio: Capacidad de la organización para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial. [22301: 2012].

Análisis de Impacto al Negocio - BIA (por sus siglas en inglés, Business Impact Analisys): Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas.

Pérdida: Recursos irrecuperables del negocio que son re-direccionados o removidos como resultado de un desastre. Dichas pérdidas pueden incluir pérdida de vidas, utilidades, participación en el mercado, ventaja competitiva, imagen pública, facilidades o capacidad operacional

Criterios de decisión: Umbrales, objetivos o patrones utilizados para determinar la necesidad de una acción o de una mayor investigación, o para describir el nivel de confianza en un resultado determinado. [ISO/IEC 27000: 2016].

Evento: Aparición o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000: 2016].

Ejercicio: Proceso para entrenar, evaluar, practicar y mejorar el desempeño en una organización. [ISO 22300].

Infraestructura TI: Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización.

Procesos críticos: Procesos de negocio relevantes para la viabilidad y operación de la organización. La no disponibilidad de éstos puede afectar gravemente los intereses tanto reputaciones como de cumplimiento normativo.

Interrupción máxima aceptable (MAO, por sus siglas en inglés): El tiempo que tomaría para que los efectos adversos que pudieran ocurrir como resultado de no proporcionar un producto/servicio o realizar una actividad, se convierta en inaceptable [NTC 5722].

Punto Objetivo de Recuperación (RPO por sus siglas en inglés): Punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación.

Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés). Periodo de tiempo después de un incidente en el que:

- El producto o servicio debe ser reanudado
- La actividad debe reanudarse, o
- Los recursos deben ser recuperados. [NTC 5722]

4. DOCUMENTOS Y REGISTROS

DOCUMENTOS Y REGISTROS	CÓDIGO
Formato Incidentes de Seguridad de la Información.	104.03.01.02.02.R.19

5. DESARROLLO

5.1 PREPARACIÓN, CONTEXTO, CONTROL Y APRENDIZAJE

La preparación y contexto para la gestión de continuidad de seguridad de la información, contiene las actividades previas requeridas para enfrentar o dar un adecuado manejo a los eventos de interrupción. Estas actividades se describen a continuación:

5.2 REALIZAR EL ANÁLISIS DE IMPACTO AL NEGOCIO - BIA

Una vez al año o por cambios considerables en la infraestructura de la IUCMC El Profesional asignado por la oficina de Tecnologías de la Información realiza entrevistas a los diferentes procesos de la Institución, con el fin de identificar los procesos críticos para la operación de la misma y los recursos mínimos que esta necesita para recuperar la operación tras la ocurrencia de un incidente perjudicial.

Con el insumo de las entrevistas y el apoyo del grupo de trabajo de la Oficina de TI, se establecerán los recursos para la recuperación de procesos y el plan de recuperación de TI.

El análisis debe identificar los tiempos de interrupción: Interrupción Máxima Aceptable (MAO), el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación de Información (RPO)

5.3 IDENTIFICAR LOS RIESGOS DE INTERRUPCIÓN

El líder o responsable de seguridad de la información, realiza una identificación de los factores de riesgo de interrupción sobre los procesos que hacen parte del alcance del SGSI, usando la matriz de riesgos de activos de información, con código (documento sin código asignado aún), con el fin de conocer las causas que afectan la operación normal de los servicios.

Los aspectos que se tendrán en cuenta son:

- **Procesos de negocio** – Actividades y procesos interrelacionados, entradas y salidas de cada proceso, claridad en roles y responsabilidades relacionadas con las operaciones críticas, Acuerdos de Niveles de Servicio (ANS) medibles.

- **Personas** - Gestión del conocimiento (Manuales, lecciones aprendidas, documentación de soluciones), segregación de funciones, salud ocupacional (manejo de epidemias, virus), políticas de retención de personal, motivación y compromiso.

- **Tecnología** – Control, gestión y mantenimiento de servidores, bases de datos, redes, almacenamiento, sistemas de información, archivos, sitios alternos de procesamiento, pruebas de recuperación y retorno respaldo de datos (tipo, frecuencia, software, políticas de respaldo de datos).

- **Infraestructura física** – Control de accesos en áreas críticas restringidas, controles de fallas relacionadas con aire acondicionado, suministro de energía; definición de planes de atención y evacuación ante incendio, terremoto, amenazas de terrorismo o situaciones similares que coloquen en riesgo vidas humanas

5.4 ESTABLECER LA ESTRATEGIA DE CONTINUIDAD TECNOLÓGICA

Una vez al año o por cambios considerables en la infraestructura de la IUCMC, el líder o responsable de seguridad de la información plantea las estrategias de recuperación de procesos y tecnología, las cuales deben dar cumplimiento a los requerimientos de seguridad de la información establecidos por la Institución. Una vez definidas, el sub proceso de Gestión de Recursos Tecnológicos selecciona y aprueba las que considera más adecuadas y realizará la gestión para disponer de los recursos necesarios para el desarrollo de las estrategias aprobadas, documentando el Plan de Continuidad de Negocio.

5.5 REALIZAR JORNADAS DE SENSIBILIZACIÓN Y CAPACITACIÓN

Dos veces al año o por cambios en el plan de continuidad de seguridad de la información, el líder de Gestión y Desarrollo de Talento Humano ejecutará capacitaciones de sensibilización a todas las áreas de la Institución con el fin de dar a conocer el Plan de Continuidad de Seguridad de la Información y sus aspectos generales.

5.6 REALIZAR EJERCICIOS Y PRUEBAS

Dos veces al año o por cambios en el plan de continuidad de seguridad de la información, el líder de seguridad de la información realizará pruebas de recuperación ante eventos simulados, acorde al alcance de SGSI, basándose en escenarios planificados, con objetivos predefinidos. Como resultado se obtendrán informes que contengan los resultados, recomendaciones y acciones a implementar.

Se debe evaluar los tiempos de respuesta de seguridad de la información de acuerdo con el nivel de prioridad definido en el procedimiento de gestión de incidentes:

- **Crítico: 0 - 8 horas**; Se debe restablecer en el menor tiempo posible para no generar problemas legales, económicos o de imagen a la institución.
- **Alto: 8 - 16 horas**; En caso de no restablecer las actividades en un tiempo menor a 12 horas, la institución empieza a tener problemas de imagen, financieros o legales.
- **Medio: 16 - 48 horas**; El incidente tiene una prioridad Media debido a que afecta en forma parcial la continuidad en la prestación del servicio de energía eléctrica por parte de la institución en caso de llegar a las 36 horas sin solución.
- **Bajo: >=48 horas**; El nivel de prioridad es bajo debido a que el incidente no afecta la continuidad de la prestación del servicio por parte de la institución.

5.7 RESPUESTA: CONTENCIÓN, Y RECUPERACIÓN

Las opciones o estrategias para la solución de los eventos de seguridad de la información son:

5.7.1. ASPECTOS EN LAS ESTRATEGIAS DE CONTENCIÓN

- ✓ Daño potencial de recursos a causa del incidente de seguridad de la información.
- ✓ Necesidad de preservación de la evidencia.
- ✓ Tiempo y recursos necesarios para poner en práctica la estrategia.
- ✓ Efectividad de la estrategia.
- ✓ Duración de las medidas a tomar.
- ✓ Criticidad de los sistemas afectados.
- ✓ Características de los posibles atacantes.
- ✓ Si el evento es de conocimiento público.
- ✓ Pérdida económica.

- ✓ Posibles implicaciones legales.

El líder de seguridad de la información junto con el responsable de los activos de información define la estrategia de contención.

5.7.2. ESTRATEGIAS DE RECUPERACIÓN

Para decidir y/o definir las estrategias de recuperación es necesario tener en cuenta:

- ✓ Cargar la copia de respaldo actualizada del sistema de información, configuración y/o base de datos.
- ✓ Creación nuevamente de la información digital o física, configuración de sistemas operativos, sistemas de información y carga manual de la información.
- ✓ Actualización o instalación de parches de seguridad a los sistemas que se vieron comprometidos.

6. RESPONSABILIDADES

6.1 LÍDER DE SEGURIDAD DE LA INFORMACIÓN

- ✓ Mantener actualizada la política y los procedimientos para su implementación
- ✓ Velar por la divulgación y mantenimiento de las políticas y procedimientos
- ✓ Elaborar y mantener el plan de continuidad de Negocio.
- ✓ Verificar el cumplimiento del presente procedimiento al interior de la institución.

6.2 LÍDER DE GESTIÓN DE RECURSOS TECNOLÓGICOS

- ✓ Adelantar las gestiones operativas necesarias para dar cumplimiento al presente procedimiento.
- ✓ Escalar al líder de seguridad de la información cualquier circunstancia que se salga del presente lineamiento.

6.3 LÍDER DE GESTIÓN Y DESARROLLO DEL TALENTO HUMANO

- ✓ Incluir en el plan de capacitación anual de la institución la aplicación del procedimiento de continuidad de seguridad de la información.
- ✓ Velar por que se haga la ejecución completa del plan de capacitación.

- ✓ Garantizar que todos los funcionarios, contratistas y terceros vinculados reciban la capacitación en continuidad de seguridad de la información.

6.4 FUNCIONARIOS, DOCENTES Y CONTRATISTAS

- ✓ Reportar cualquier evento o incidente de seguridad de la información que se presenten en la institución.

7. GESTIÓN DE ACTIVIDADES

ACTIVIDADES	RESPONSABLE	REGISTRO
Realizar análisis de impacto al negocio.	Líder de Seguridad de la Información	Listado de asistencia de entrevistas de levantamiento de información.
Documentar estrategias de continuidad tecnológica.	Líder de Gestión TIC	Documento y listados de asistencias de reuniones.
Realizar Jornadas de sensibilización y capacitación.	Líder de Gestión Humana	Listado de asistencia a capacitaciones.
Realizar ejercicios y prueba.	Líder de Seguridad de la Información /responsable de activos de información.	Informe de resultados de pruebas.
Realizar actividades de contención y recuperación.	Líder de Seguridad de la Información / Líderes de proceso afectado.	Documento con estrategias de contención y recuperación.

8. DOCUMENTOS DE REFERENCIA

Norma ISO/IEC 27001:2013
Normas ISO/IEC 22301:2012
Norma NTC 5722
104.03.01.02.02. P.04 Procedimiento Gestión de incidentes Seguridad y Privacidad de la Información.
104.03.01.02.02. R.20 Matriz Tratamiento De Riesgos En Seguridad Y Privacidad De La Información.

9. DISPOSICIONES FINALES

9.2 DIFUSIÓN

El personal autorizado por el subproceso Gestión de Recursos Tecnológicos realizará la socialización y/o difusión de esta política a la comunidad universitaria y grupos de interés, de acuerdo a las directrices del documento 104.03.01.02.02.D.09 plan de sensibilización de seguridad de la información.

9.3 ACTUALIZACIÓN

Para garantizar la vigencia, mejora continua y actualización de este procedimiento, deberá ser revisada por lo menos una vez por año por personal competente y autorizado del subproceso Gestión de Recursos Tecnológicos y será el comité integral de planeación y gestión quien avale las mejoras a implementar.

Durante la actualización se deberá tener en cuenta la normatividad vigente, lineamientos institucionales y resultado de auditorías de seguridad y privacidad de la información.

9.4 SANCIONES

El incumplimiento de esta política se aplicará la normativa vigente en la Institución Universitaria Colegio Mayor del Cauca, además de las normas emitidas a nivel Nacional y Regional a través del proceso Gestión y Desarrollo del Talento Humano.

10. ANEXOS

No aplica.

11. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIOS REALIZADOS
2 de diciembre de 2019	Se realizó ajustes en el nombre del procedimiento, adición de numeral 9. Disposiciones finales y el código de los documentos internos de referencia, en el numeral 8.