

	CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C.		
	CLAVE DEL PROCESO CYR-OYP-012		
	No. REVISION 3	FECHA DE EMISIÓN: 01/08/2022	PAGINA: 1 de 6
PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN			

1 OBJETIVO.

Definir el procedimiento de seguridad lógica mediante el desarrollo de un plan adecuado de trabajo que permita:

- Garantizar el correcto funcionamiento de los sistemas de información.
- Proteger la información contenida en la Infraestructura de TI que se ubica en el centro de datos con el fin de garantizar su integridad, confidencialidad y disponibilidad.

2 CAMPO DE APLICACIÓN.


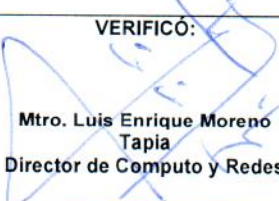
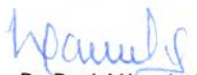
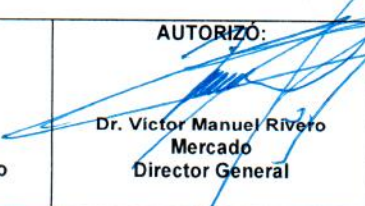
Al ser una actividad constante, se aplica en todo momento haciendo uso de herramientas de protección y monitoreo sobre los servicios de TI.


3 RESPONSABILIDADES.

- 3.1 El responsable del dominio tecnológico tiene la tarea/actividad de monitorear que los servicios estén funcionando de forma correcta.
- 3.2 El responsable del dominio tecnológico tiene la tarea/actividad instalar y configurar herramientas de seguridad en los sistemas que brindan los servicios de TI.
- 3.3 El responsable del dominio tecnológico tiene la tarea/actividad de reportar cualquier incidente de seguridad detectado.

4 DEFINICIONES.

Centro de datos. Espacio donde se concentran los recursos informáticos necesarios para ofrecer los servicios de una organización.

ELABORÓ:  TSU. Ulises Andrés Martínez Rodríguez Cómputo y Redes OyP	VERIFICÓ:  Mtro. Luis Enrique Moreno Tapia Director de Computo y Redes	REVISÓ:  Dr. Daniel Hernández Hernández Coordinador Académico	AUTORIZÓ:  Dr. Víctor Manuel Rivero Mercado Director General
---	--	--	--

	CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C.		
	CLAVE DEL PROCESO CYR-OYP-012		
	No. REVISIÓN 3	FECHA DE EMISIÓN: 01/08/2022	PAGINA: 2 de 6
PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN			

Dominio tecnológico. Las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo.

Escaneo de vulnerabilidades. Análisis, identificación y reporte de las vulnerabilidades en cuestión de seguridad que se tienen en una infraestructura de TI.

Herramientas de monitoreo. Software utilizado en los servicios de TI que permiten el acceso a los sistemas de monitoreo, por ejemplo: SNMP, ICMP, Agentes, Firewall, Scripts, etc.

Herramientas de protección. Software diseñado para proteger uno o más sistemas de información como, por ejemplo: Fail2Ban, Denyhosts, Logwatch, Firewall, Scripts, etc.

Infraestructura de TI. Conjunto de componentes de tecnología de la información que son la base de un servicio de TI; normalmente componentes físicos, pero también varios componentes de software y de red.


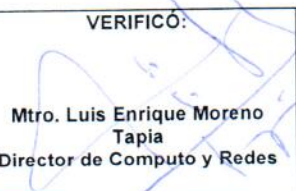


OyP. Área de Operaciones y Proyectos adscrito al departamento de Cómputo y Redes.

Sistema de monitoreo. Es el proceso que ayuda con la supervisión de los recursos y el desempeño de la infraestructura de TI, tanto en software como en hardware.

Servicio de TI. Conjunto de actividades que buscan responder a las necesidades de un usuario por medio de un cambio de condición en la infraestructura de TI.

Técnico responsable del dominio tecnológico. Personal del área de Cómputo y Redes que se encarga de realizar trabajos técnicos y operativos dentro del centro.

Usuario. Persona que solicite el servicio al departamento de Cómputo y Redes del Cimat (alumnos, profesores, investigadores y administrativos).

ELABORÓ:	VERIFICÓ:	REVISÓ:	AUTORIZÓ:
 TSU. Ulises Andrés Martínez Rodríguez Cómputo y Redes OyP	 Mtro. Luis Enrique Moreno Tapia Director de Computo y Redes	 Dr. Daniel Hernández Hernández Coordinador Académico	 Dr. Víctor Manuel Rivero Mercado Director General

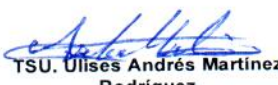



	CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C.		
	CLAVE DEL PROCESO CYR-OYP-012		
	No. REVISION 3	FECHA DE EMISIÓN: 01/08/2022	PAGINA 3 de 6
PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN			

5 DESARROLLO DEL PROCEDIMIENTO.

5.1. Procedimiento de seguridad de la información.


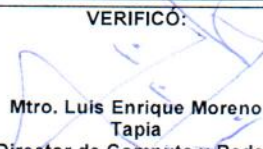
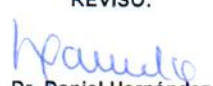

5.1.1 Descripción de actividades.

Paso	Responsable	Actividad	Documento de Trabajo, ayuda visual o referencia a sitio web.
1	<u>Usuario</u>	Solicitar nuevo servicio de TI a OyP.	Ticket de solicitud.
2	<u>Técnico de Cómputo y Redes</u>	Evaluar si es factible brindar el servicio solicitado.	
3	<u>Técnico de Cómputo y Redes</u>	¿Es factible brindar el servicio? SI: remitirse al paso 4. NO: remitirse al paso 19.	
4	<u>Técnico de Cómputo y Redes</u>	Instalar y configurar el servicio solicitado.	Servicio de TI.
5	<u>Técnico de Cómputo y Redes</u>	Instalar y configurar herramientas de protección y monitoreo en el servicio solicitado.	Guía de instalación de herramientas de protección y monitoreo.

ELABORÓ:  TSU. Ulises Andrés Martínez Rodríguez Cómputo y Redes OyP	VERIFICÓ:  Mtro. Luis Enrique Moreno Tapia Director de Compuo y Redes	REVISÓ:  Dr. Daniel Hernández Hernández Coordinador Académico	AUTORIZÓ:  Dr. Victor Manuel Rivero Mercado Director General
---	---	--	--

	CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C.		
	CLAVE DEL PROCESO CYR-OYP-012		
	No. REVISIÓN 3	FECHA DE EMISIÓN: 01/08/2022	PÁGINA: 4 de 6
PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN			

6	<u>Técnico de Cómputo y Redes</u>	Iniciar pruebas de funcionamiento del servicio	Reporte de pruebas de funcionamiento.
7	<u>Técnico de Cómputo y Redes</u>	¿Las pruebas fueron satisfactorias? SI: remitirse al paso 8. NO: remitirse al paso 4.	
8	<u>Técnico de Cómputo y Redes</u>	Instalar actualizaciones disponibles en el sistema. Consultar el procedimiento de actualizaciones.	Procedimiento de actualizaciones.
9	<u>Técnico de Cómputo y Redes</u>	Realizar escaneo de vulnerabilidades al servicio solicitado.	Reporte de vulnerabilidades.
10	<u>Técnico de Cómputo y Redes</u>	¿Se detectaron vulnerabilidades en el servicio? SI: remitirse al paso 11. NO: remitirse al paso 12.	
11	<u>Técnico de Cómputo y Redes</u>	Consultar documentación oficial del fabricante para solucionar las vulnerabilidades.	Sitio web del fabricante.
12	<u>Técnico de Cómputo y Redes</u>	Preguntar al usuario solicitante si requiere que el servicio se agregue al plan de respaldos.	Correo electrónico.

ELABORÓ:  TSU. Ulises Andrés Martínez Rodríguez Cómputo y Redes OYP	VERIFICÓ:  Mtro. Luis Enrique Moreno Tapia Director de Cómputo y Redes	REVISÓ:  Dr. Daniel Hernández Hernández Coordinador Académico	AUTORIZÓ:  Dr. Víctor Manuel Rivero Mercado Director General
---	--	--	--

**CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C.**

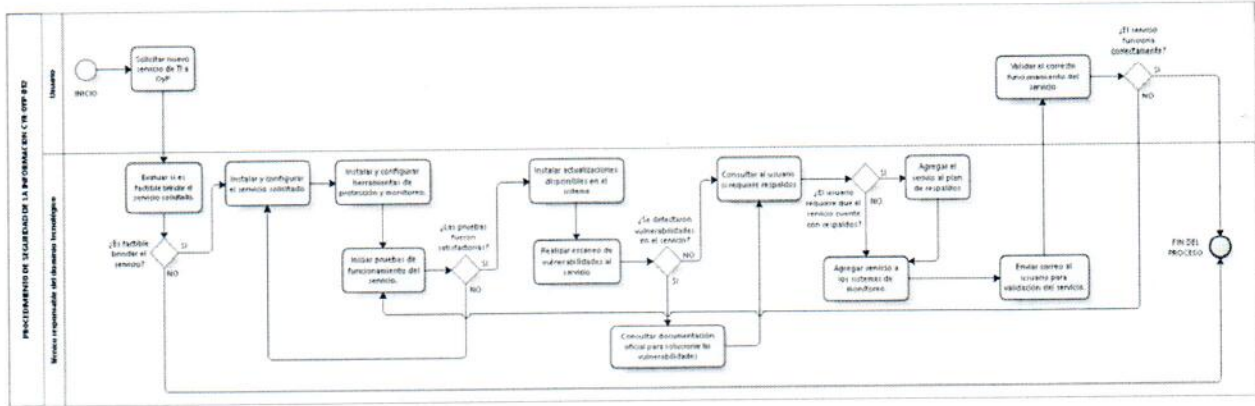
CLAVE DEL PROCESO CYR-OYP-012

No. REVISIÓN
3FECHA DE EMISIÓN:
01/08/2022PAGINA:
5 de 6**PROCEDIMIENTO DE SEGURIDAD DE LA INFORMACIÓN**

13	<u>Técnico de Cómputo y Redes</u>	¿El usuario requiere que el servicio cuente con respaldos? SI: remitirse al paso 14. NO: remitirse al paso 15.	
14	<u>Técnico de Cómputo y Redes</u>	Agregar el servicio al plan de respaldos. Consultar el procedimiento de respaldos.	Procedimiento de respaldos.
15	<u>Técnico de Cómputo y Redes</u>	Agregar el servicio a los sistemas de monitoreo. Consultar el procedimiento de monitoreo.	Procedimiento de monitoreo.
16	<u>Técnico de Cómputo y Redes</u>	Enviar correo al usuario para validación del servicio.	Correo electrónico.
17	<u>Usuario</u>	Validar el correcto funcionamiento del servicio.	
18	<u>Técnico de Cómputo y Redes</u>	¿El servicio funciona correctamente? SI: remitirse al paso 19. NO: remitirse al paso 6.	
19	<u>Técnico de Cómputo y Redes</u>	Finalizar el proceso documentando y cerrando ticket.	Ticket cerrado.

ELABORÓ: TSU. Ulises Andrés Martínez Rodríguez Cómputo y Redes OyP	VERIFICÓ: Mtro. Luis Enrique Moreno Tapia Director de Computo y Redes	REVISÓ: Dr. Daniel Hernández Hernández Coordinador Académico	AUTORIZÓ: Dr. Víctor Manuel Rivero Mercado Director General
---	--	---	--

5.1.2 Diagrama de flujo.



6 DOCUMENTOS GENERADOS.





- Sin documentos generados.

7 DOCUMENTOS DE REFERENCIA.

- Diagrama de seguridad lógica.
- Procedimientos del área de Operación y Proyectos.
- Guía de instalación de herramientas de protección y monitoreo.

8 ANEXOS.

- Sin anexos

ELABORÓ:	VERIFICÓ:	REVISÓ:	AUTORIZÓ:
 TSU. Ulises Andrés Martínez Rodríguez Cómputo y Redes OYP	 Mtro. Luis Enrique Moreno Tapia Director de Cómputo y Redes	 Dr. Daniel Hernández Hernández Coordinador Académico	 Dr. Victor Manuel Rivera Mercado Director General