



Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)

ACTIVIDAD	RESPONSABLE	NOMBRE Y APELLIDO	FIRMA	FECHA
Elaborado por:	Ing. Especialista	Brayan Navarrete		26-01-2021
Revisado por:	Ing. Especialista Senior	Giovanni Diaz		03-03-2021
Aprobado por:	Encargado CIP COMASA Spa	Ricardo Vallejos	 Ricardo Vallejos ENCARGADO CIP COMASA SpA	30-03-2021

"Documentos impresos o fotocopiados son Copias No Controladas. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"

 COMASA Bioenergía Lautaro	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
---	--	--

ÍNDICE

1	OBJETIVO	3
2	ALCANCES	3
3	REFERENCIAS	3
4	DEFINICIONES	3
5	POLÍTICA	4
5.1	Encargado CIP	5
6	PLAN DE CIBERSEGURIDAD	5
6.1	Conciencia de Ciberseguridad	5
6.2	Controles de Seguridad Física	6
6.3	Control de Acceso Electrónico	7
6.4	Respuesta a Incidentes de Ciberseguridad	8
6.5	Mitigación de Riesgos de Código Malicioso en Ciber Activos Transitorios y Medios Removibles	12
6.5.1	Ciber Activos Transitorios	13
6.5.2	Medios Removibles	13
6.6	Declaración y respuesta a circunstancias excepcionales CIP	14
7	VALIDEZ Y GESTIÓN DEL DOCUMENTO	14
8	CONFIDENCIALIDAD	14
9	ANEXOS	15
10	REVISIONES	15

"Documentos impresos o fotocopiados son **Copias No Controladas**. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"



 COMASA <small>Bioenergía Lautaro</small>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

1 OBJETIVO

Especificar controles de gestión de la seguridad consistentes y sostenibles en la operación de COMASA que establezcan la responsabilidad para proteger Ciber Sistemas SEN contra eventos que afecten o comprometan instalaciones pudiendo conducir una mala operación o inestabilidad del SEN.

2 ALCANCES

Los Ciber Sistemas SEN que sean definidos en el documento “COM-PL-001_CIP-002 - Ciber Seguridad - Categorización de Ciber Sistemas SEN”

Todo personal de COMASA y externos deberán dar cumplimientos a los puntos establecidos en el conjunto de políticas y procedimientos de Ciberseguridad.

3 REFERENCIAS

- Estándar de Ciberseguridad SEN Final 20-07-2020.

4 DEFINICIONES

ARI	Administración de Acceso Remoto Interactivo
CEE	Conectividad Enrutable Externa
HTTPS	Hypertext Transfer Protocol Secure
PAE	Punto de Acceso Electrónico
PSE	Perímetro de seguridad electrónica
SEN	Sistema de Energía Nacional
SSH	Secure SHell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network

Ciber Activo SEN: Ciber Activo que, en caso de fallar, ser degradado, mal utilizado o quedar indisponible, dentro de un intervalo de 15 minutos medidos desde el momento de ser requerido en tiempo real, desde tener que cumplir el programa operacional, desde su falla o desde su indisponibilidad, pudiese impactar adversamente una o más instalaciones, sistemas, o equipos los cuales, de ser

“Documentos impresos o fotocopiados son Copias No Controladas. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información”



 COMASA <i>Bioenergía Lautaro</i>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

destruidos, degradados, o volverse indisponibles cuando se requieran, afectaría la operación segura y confiable del SEN. La redundancia de las instalaciones, sistemas o equipos afectados, no se deberá considerar al momento de determinar el impacto adverso. Cada Ciber Activo SEN debe estar incluido en uno o más Ciber Sistemas SEN.

Ciber Sistema SEN: Uno o más Ciber Activos SEN agrupados lógicamente por una Entidad Responsable.

Circunstancias Excepcionales CIP: Situación que involucra, o amenaza involucrar, una o más de las siguientes condiciones que impactan la seguridad o confiabilidad del SEN, entre las que destacan:

- i) Riesgo de accidente o muerte
- ii) Desastre natural
- iii) Disturbios civiles
- iv) Una falla inminente de equipos, software o hardware
- v) Un incidente de ciberseguridad que requiera apoyo de emergencia
- vi) La firma de un acuerdo de asistencia mutua
- vii) Una indisponibilidad de fuerza laboral de gran escala.

5 POLÍTICA

Esta política define los parámetros de gestión de la seguridad que aplican a los Ciber Sistemas SEN, la cual deberá ser revisada y aprobada por el encargado CIP al menos cada 12 meses.

Esta política cubre los siguientes puntos:

- Conciencia de Ciberseguridad.
- Controles de seguridad física.
- Controles de acceso eléctrico.
- Respuesta a incidentes de Ciberseguridad.
- Mitigación de riesgos de código malicioso en Ciber Activos Transitorios y medios removibles.
- Declaración y respuesta a Circunstancias Excepcionales CIP.

"Documentos impresos o fotocopiados son **Copias No Controladas**. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"



 COMASA <i>Bioenergía Lautaro</i>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

Para los puntos declarados anteriormente se deben generar medidas de control o evidencia aceptable que incluyen, pero no están limitadas a, plan Ciberseguridad, revisión histórica, registros de revisión, o evidencia de workflow de un sistema de gestión de documentos que demuestre revisión de cada política de ciberseguridad al menos una vez cada 12 meses calendario; documentación de aprobación de cada política de ciberseguridad por parte del Encargado CIP.

COMASA mantendrá registros de evidencias y medidas de control por un periodo de al menos 3 años, plazo que se podría extender según lo requiera la SEC por existir una investigación en curso como resultado de una auditoría.

5.1 Encargado CIP

Se establece que el encargado CIP para los Ciber sistemas SEN de COMASA será definido en el documento “**COM-REG-001_Acta de asignación Encargado CIP**”, donde también se definirán sus actividades y responsabilidades.

Se deberá identificar el Encargado CIP por su nombre y documentar por escrito cualquier modificación al respecto dentro de 30 días calendario de ocurrido el cambio. Lo cual deberá quedar registrado en el documento “**COM-REG-001_Acta de asignación Encargado CIP**”.

6 PLAN DE CIBERSEGURIDAD

Se incluyen a continuación puntos para el desarrollo de la política y planes de ciberseguridad para los elementos que son parte de los sistemas de ciberseguridad SEN.

6.1 Conciencia de Ciberseguridad

COMASA realizará un plan de concientización de ciberseguridad continuo en donde se aborden los siguientes puntos:

- a) Conocimiento general de ciberseguridad
- b) Ciberseguridad en COMASA
- c) Ciber sistemas SEN
- d) Conocimiento de las políticas de Ciberseguridad SEN

“Documentos impresos o fotocopiados son Copias No Controladas. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información”



 COMASA Bioenergía Lautaro	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
---	--	--

- e) Conocimiento de los procedimientos de Ciberseguridad SEN
- f) Incidentes y Respuestas
- g) Consecuencias de incumplimiento de políticas y procedimientos

El plan de concientización de ciberseguridad se realizará en las siguientes modalidades.

Metodología	Registro y Documentación
E-mails hacia personal de COMASA.	Evidencia de correo enviado a personal.
Capacitaciones E-learning	Presentación y “COM-REG-003_REGISTRO - Capacitación”
Capacitación presencial y remota	Presentación y “COM-REG-003_REGISTRO - Capacitación”
Afiches Informativos	Afiche digital

Las metodologías indicadas deberán ser gestionadas por el encargado CIP de COMASA, pero así mismo, tendrá la facultad de asignar y delegar la ejecución de estas metodologías a otro personal que tenga las competencias adecuadas. Si esto último fuese el caso, deberá verse reflejado en el documento “COM-REG-005_REGISTRO - Delegaciones Encargado CIP”.

Este plan tendrá que ser revisado al menos cada 15 meses, donde se deberá evaluar el éxito del plan y si se continúa con la misma metodología, el método de evaluación será mediante encuestas, medición de cumplimiento, auditorías, pruebas, etc.

Este plan está registrado en el documento “COM-PC-001_PLAN DE CONCIENTIZACION”

6.2 Controles de Seguridad Física

COMASA establece un control físico de acceso a la o las salas donde se ubican los Ciber Sistemas SEN, estableciendo a lo menos 2 controles que sean de distinto

“Documentos impresos o fotocopiados son Copias No Controladas. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información”



 COMASA Bioenergía Lautaro	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
---	--	--

ámbito, uno administrativo y uno técnico. Los controles mencionados se declaran en el documento “**Política de control de acceso físico COMASA SpA**”.

Se definen zonas con distintos niveles de autorización, acorde con la criticidad de los equipos para la operación de los cibersistemas SEN. Las zonas deberán estar identificadas en el instructivo de acceso publicado en cada sitio o lugar. Los niveles de autorización son descritos en el documento “**Política de control de acceso físico COMASA SpA**”.

El personal autorizado para este acceso deberá estar documentado en el “**COM-REG-007_REGISTRO - Personal Autorizado**”, indicando el nivel de acceso o zona a la cual tiene autorización.

6.3 Control de Acceso Electrónico

Para poder establecer comunicaciones mediante el PSE, se deben generar políticas o listas de control de acceso (de ahora en adelante ACL), dependiendo de las capacidades de cada PSE. Las políticas o ACL deben ser lo más específicas posibles, definiendo dirección IP origen y destino, como también puertos. Esto aplica únicamente para protocolos enrutables (IP), otros protocolos quedarán contenidos dentro del perímetro de seguridad. Los permisos idealmente deben ser nombrados o comentados con la función que cumple, o a su vez, declarando un número de incidencia o requerimiento que lo relacione.

Si se hace referencia a un número de incidencia o requerimiento, se debe mantener el registro correspondiente, que a lo menos contenga: quien solicita, quién aprueba, el motivo, fecha de solicitud y de ejecución.

La documentación o evidencia para este proceso se obtendrá directamente del sistema que actúa como PSE y del sistema que registra los requerimientos.

Se debe tener en consideración el control de acceso a sistemas que está ligado al documento “**Política de Control de acceso a sistemas COMASA SpA**.” Por lo tanto, cualquier acceso a un sistema deberá estar de acuerdo con lo que dicta la política y su registro de acceso “**Listado de Usuarios y permisos de Sistemas COMASA SpA**.” Cualquier desviación de estos puntos será considerada una violación de la política y de los accesos electrónicos, lo que será clasificado como un incidente de Ciberseguridad.

“Documentos impresos o fotocopiados son **Copias No Controladas**. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información”



 COMASA <i>Bioenergía Lautaro</i>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

6.4 Respuesta a Incidentes de Ciberseguridad

Para dar atención a un incidente de Ciberseguridad es importante tener definido lo que es, y poder detectarlo. Si no hay detección, se puede estar frente a un incidente e ignorarlo.

Se definen los siguientes puntos como incidentes en COMASA.

- Cuentas de usuario inusuales en sistemas o especialmente privilegiadas.
- Ficheros ocultos o de tamaño, nombre y ubicación sospechosa.
- Infección por Malware que realiza cambios en los ficheros o registros de los sistemas.
- Procesos o servicios inusuales, a la escucha o con conexiones hacia el exterior (internet).
- Cargas excesivas de disco o memoria que pueden estar causadas por malware o denegación de servicio.
- Configuraciones en equipos de perímetro que incumplen los parámetros mínimos de seguridad.
- Controles de seguridad físico o lógicos vulnerables. (Puertas de acceso abiertas a zonas restringidas, permisos incorrectos a usuarios).
- Cualquier punto que vulnere o viole las definiciones de esta política o de las políticas anexas.

Las formas para detectar los incidentes pueden ser complemento de uno o varios métodos, en COMASA se utilizan las siguientes formas de detección.

- Consolas de antivirus.
- Sistemas de Detección / Prevención de Intrusión (IDS/IPS).
- Alertas de sistemas de correlación de eventos de seguridad o SIEM.
- Registros de auditoría para detectar intentos de acceso no autorizados.
- Registro de conexiones bloqueadas en los cortafuegos.
- Registro de conexiones realizadas a través de proxys corporativos.
- Registros en herramientas DLP (Data Loss Prevention).
- Bloqueo de cuentas de usuario u otras anomalías reportadas en masa a la mesa de ayuda o que impliquen algún riesgo como pérdidas de USBs o equipos portátiles.
- Consumos excesivos y repentinos de memoria o disco en servidores.

"Documentos impresos o fotocopiados son Copias No Controladas. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"



 COMASA <i>Bioenergía Lautaro</i>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

- Anomalías de tráfico como picos de consumo a horas no habituales.
- Volcados de red, mediante port mirroring por ejemplo, que permitan confirmar alguna sospecha de incidente.
- En el caso de equipos de trabajo, pueden indicar algún tipo de infección en el sistema, entre otros: comportamiento anómalo de alguna aplicación, ventanas emergentes del navegador, conexiones muy lentas, reinicios o aplicaciones que se cierran sin motivo.
- Detección por usuarios y reporte a la mesa de ayuda.

Una vez que se ha detectado un incidente se debe pasar a la clasificación de este, lo que indicará la criticidad de atención. Esto se establecerá acorde al impacto y urgencia del incidente. Se definen 5 niveles de prioridad que son codificados en base a la siguiente tabla.

Urgencia\Impacto	Alto	Medio	Bajo
Alta	1	2	3
Media	2	3	4
Baja	3	4	5

Impacto: Impacto en los Ciber sistemas SEN de COMASA que genera un incidente de ciberseguridad.

Alto	Medio	Bajo
Existe caída o degradación sobre el 35% de los servicios.	Existe degradación o afectación hasta en 35% de los servicios.	No hay degradación o caída de servicios.

Urgencia: que tan rápido debe ser necesaria la resolución del incidente de ciberseguridad.

"Documentos impresos o fotocopiados son **Copias No Controladas**. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"



 COMASA Bioenergía Lautaro	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

Alto	Medio	Bajo
Inmediatamente: sin solución temporal disponible	A mediano plazo: existe solución temporal parcial	A largo plazo: existe solución temporal satisfactoriamente

El tiempo de resolución de un incidente de ciberseguridad depende de su código de prioridad y se calcula de la siguiente forma:

Código de Prioridad	Descripción	Tiempo de Atención
1	Crítico	1 Hora
2	Alto	3 horas
3	Medio	5 Horas
4	Normal	8 Horas
5	Planificado	24 Horas

Estos tiempos de resolución no son aplicables cuando existe una circunstancia excepcional CIP.

Para lograr clasificar e identificar los incidentes de ciberseguridad, se debe consultar el documento "**COM-REG-008_REGISTRO - Clasificación de incidentes de Ciberseguridad**", en donde se muestra las categorías de los incidentes. Este registro tiene la finalidad de enmarcar los incidentes en una categoría preestablecida, de esta forma se puede tener un registro sobre los tipos de incidentes que han existido para un análisis posterior. El sistema de ticket debe estar sincronizado con esta tabla para hacer una correcta clasificación en el sistema.

Todos los incidentes deberán ser reportados a la mesa de ayuda, mediante el sistema de ticket o un correo, la mesa se encargará de clasificar el incidente y gestionar su atención con los responsables de cada área o especialidad de acuerdo con el siguiente cuadro de Roles y responsabilidades. Debe quedar registrado en el documento "**COM-REG-009_REGISTRO Incidentes de Ciberseguridad**".

"Documentos impresos o fotocopiados son **Copias No Controladas**. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"



 COMASA Bioenergía Lautaro	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

Rol	Responsabilidad
Encargado CIP	Asegurar el cumplimiento de las políticas y la atención de los incidentes para una expedita solución. Reporte de incidentes cuando se requiera. Administrar, operar y resolver incidentes de ciberseguridad que contemplen servidores o sistemas. Administrar, operar y resolver incidentes de Ciberseguridad que contemplen dispositivos de control y automatización.
Mesa de ayuda	Registrar, identificar y gestionar incidentes de ciberseguridad. Resolver incidentes de Ciberseguridad en dispositivos de trabajo (PC, Notebook, otros.)
Gestor de Comunicaciones	Administrar, operar y resolver incidentes de ciberseguridad que contemplen dispositivos de comunicación y seguridad.

Para la gestión de incidentes, se crea el siguiente modelo de atención:

- 1.- Preparación: Consiste en preparar los sistemas para prevenir la ocurrencia de un incidente, básicamente cumplir con las normas mínimas que establecen las políticas.
- 2.- Recursos para análisis de incidentes: COMASA debe contar con la información de todos los sistemas, inventarios, diagramas, y cualquier otro elemento que apoye la expedita gestión de un incidente.
- 3.- Recursos para la mitigación y remediación: Se consideran los elementos básicos para realizar una restauración del o los sistemas. Backup de configuración, imágenes de sistemas, respaldos de base de datos, etc.
- 4.- Detección y evaluación: Los medios de detección están declarados en este documento al inicio de este punto. Luego de detectado y notificado a la mesa de ayuda ésta realizará la evaluación del incidente y lo clasificará de acuerdo con la categoría que corresponda.
- 5.- Contención y recuperación: En este punto el incidente debe ser atendido por el personal idóneo, para lo cual se han establecido los roles y responsabilidades. Cada Rol es responsable por la contención y recuperación del incidente en su área de especialidad. La gestión y escalamiento cuando corresponda será realizada por la mesa de ayuda, y el encargado CIP si el incidente es de nivel crítico.
El rol responsable deberá realizar la contención del incidente evitando que pueda propagarse y afectar otros activos. Luego se deberá realizar la recuperación del

"Documentos impresos o fotocopiados son Copias No Controladas. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"



 COMASA <i>Bioenergía Lautaro</i>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

sistema o activo utilizando la información disponible, el conocimiento de su especialidad y los procedimientos de respuesta a incidentes, cuando existan.

6.- Análisis e investigación: Se debe realizar un análisis de los eventos y logs que permitan establecer la causa raíz del incidente. Esto se debe documentar como parte de la gestión del incidente, y la investigación deberá ser utilizada como fuente de información para la revisión y mejora de las políticas.

COMASA realizará pruebas de los planes de respuesta a incidentes de ciberseguridad al menos una vez cada 36 meses. Estos podrán ser:

- I. respondiendo a un Incidente de Ciberseguridad Reportable real.
- II. usando un ejercicio o ensayo (drill) de un Incidente Ciberseguridad Reportable.
- III. Usando un ejercicio operacional de un Incidente de Ciberseguridad Reportable.

Al finalizar este ejercicio, se deberá actualizar o ajustar los planes de respuesta para ser más eficiente o efectivo el proceso, de acuerdo con la experiencia obtenida. Esto deberá realizarse dentro de los siguientes 180 días calendario luego de las pruebas u ocurrido un incidente de Ciberseguridad Reportable real.

En el caso que el incidente de seguridad comprometa o interrumpa el funcionamiento del ciber sistema SEN o en consecuencia tenga un nivel de impacto alto, el encargado CIP deberá realizar la notificación correspondiente vía correo electrónico al CEN y la SEC.

6.5 Mitigación de Riesgos de Código Malicioso en Ciber Activos Transitorios y Medios Removibles

Se implementa un plan para lograr los objetivos de mitigación de riesgos de introducción de código malicioso a Ciber Sistemas SEN a través del uso de Ciber Activos Transitorios y medios Removibles. Excepto bajo condiciones excepcionales CIP. El plan incluye:

"Documentos impresos o fotocopiados son Copias No Controladas. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"



 COMASA <i>Bioenergía Lautaro</i>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

6.5.1 Ciber Activos Transitorios

Para Ciber Activos Transitorios gestionados por COMASA, si existen, deben hacer uso de uno o una combinación de los siguientes métodos, de manera continua o por demanda (según capacidad del Ciber Activo Transitorio):

- Software antivirus, incluyendo actualización manual o administrada de firmas o patrones.
- Aplicación de lista blanca.
- Otro método(s) para mitigar la introducción de código malicioso.

Para Ciber Activos Transitorios gestionados por terceros distintos a COMASA, si existen, deben cumplir los siguientes puntos:

- Uso de uno o una combinación de los siguientes métodos previo a conectar Ciber Activos Transitorios a un Ciber Sistema SEN (según capacidad del Ciber Activo Transitorio).

Revisión del nivel de actualización del antivirus:

- Revisión del proceso de actualización del antivirus utilizado por terceros.
- Revisión de la aplicación de lista blanca utilizada por terceros.
- Revisión del uso de sistemas operativos vivos (Live OS) y software ejecutable solo desde medios de lectura (read-only).
- Revisión del reforzamiento (Hardening) de sistemas utilizado por terceros.
- Otros métodos para mitigar la introducción de código malicioso.

En cada revisión del documento o cuando se estime conveniente por nuevos métodos de infección se deberá analizar la necesidad de acciones adicionales previo a la conexión de Ciber Activos Transitorios al Ciber Sistema SEN.

6.5.2 Medios Removibles

Para Medios Removibles COMASA debe usar los siguientes métodos para detectar y prevenir código malicioso:

- Se debe usar un Ciber Activo distinto a un Ciber Sistema SEN para probar y detectar un posible código malicioso en medios removibles.

"Documentos impresos o fotocopiados son **Copias No Controladas**. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"



 COMASA <i>Bioenergía Lautaro</i>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

- Se debe mitigar la amenaza de código malicioso que sea detectada en medios removibles previo conectar dichos Medios en un Ciber Sistema SEN.

Para los puntos 6.5.1 y 6.5.2 se debe tomar en consideración lo establecido en la “**Política de administración de antivirus corporativo COMASA SpA**”.

Para ambos casos quien ejecute los métodos siempre deberá ser personal COMASA y deberá completar el registro “**COM-REG-006_REGISTRO - Mitigación de Riesgo de Código malicioso**” que identifique las acciones y los resultados obtenidos.

6.6 Declaración y respuesta a circunstancias excepcionales CIP.

Al inicio de este documento se indican las circunstancias excepcionales CIP, las cuales permiten incumplir momentáneamente las políticas. En caso de que eso suceda se deberá dar aviso al Encargado CIP para el registro del evento y acciones realizadas.

Esto deberá quedar documentado en el registro “**COM-REG-004_REGISTRO - Circunstancias Excepcionales CIP**”.

7 VALIDEZ Y GESTIÓN DEL DOCUMENTO

Este documento es válido desde el 16 de Abril de 2021.

El propietario de este documento es el encargado CIP de COMASA, que debe verificar y si es necesario actualizar el documento por lo menos una vez al año. Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes que surgen por fallas en los controles de políticas.
- Efectividad en la resolución de incidentes.

8 CONFIDENCIALIDAD

Este documento es para uso interno de COMASA, su distribución o publicación está prohibida. Es necesario que los proveedores con acceso a los sistemas tengan concientización de las políticas utilizadas en COMASA.

“Documentos impresos o fotocopiados son **Copias No Controladas**. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información”



 COMASA <small>Bioenergía Lautaro</small>	Política Ciber Seguridad – Controles de Gestión de la Seguridad (CIP-003)	Código: COM-PL-002 Revisión: E Fecha de Revisión: Noviembre 28, 2024
--	--	--

9 ANEXOS

A continuación, se indican todos los documentos de referencia que posee el presente documento.

- COM-REG-001_Acta de asignación Encargado CIP
- COM-REG-005_REGISTRO - Delegaciones Encargado CIP
- COM-REG-003_REGISTRO – Capacitación
- COM-PC-001_PLAN DE CONCIENCIACIÓN
- Política de control de acceso físico COMASA SpA
- COM-REG-008_REGISTRO - Clasificación de incidentes de Ciberseguridad
- COM-REG-007_REGISTRO - Personal Autorizado
- Política de administración de antivirus corporativo COMASA SpA
- COM-REG-006_REGISTRO - Mitigación de Riesgo de Código malicioso
- COM-REG-004_REGISTRO - Circunstancias Excepcionales CIP

10 REVISIONES

Revisión	Fecha	Descripción de la Modificación
A	06-02-2021	Creación y revisión del documento.
B	03-03-2021	Revisión del documento
C	29-03-2021	Actualización del documento
D	03-06-2022	Revisión del documento
E	30-09-2023	Revisión del documento
	28-11-2024	Revisión del documento



Ricardo Vallejos Ch.
ENCARGADO CIP
COMASA SPA
28/11/24

"Documentos impresos o fotocopiados son Copias No Controladas. Verificar su vigencia comparando el documento publicado en el servidor de archivos o solicitando documento actualizado al Jefe de departamento de Tecnología de la información"