RESPALDOS Y ELIMINACIÓN DE INFORMACIÓN

TIPO DE DOCUMENTO: Procedimiento

CÓDIGO: PRO GSI 032

I. AUTORIZACIONES

Elaboró:	*Revisó:*	*Autorizó:*
Ing. Salvador Santiago Araujo *Gerente Administrativo*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*

Última revisión: octubre 2025

No. de versión: 11

Fecha de emisión: Agosto 2015

Revisó: DGE

Aprobó: DGE

ÍNDICE

CONTENIDO **PÁGINA**

II. OBJETIVO

Garantizar que la información almacenada en equipos y soportes sea respaldada de forma segura y en su caso, borrada o eliminada de forma también segura.

III. ALCANCE

Aplica a todas las áreas, procesos y activos de la Organización, involucradas en el Sistema de Gestión de Seguridad de la Información.

IV. HISTORIAL DE CAMBIOS

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
1	Versión inicial.	MBS	Agosto 2015
2	Cambio de Formato	LBR	Octubre 2016
3	Adecuaciones en las referencias; cambios en el punto 1.2; eliminación del punto 1.3 y cambios en la numeración; cambios en el punto 5.1. Adecuaciones generales.	LBR	Mayo 2017
4	Eliminación de apartados no aplicables, adecuación de actividades	RML	Febrero 2018
5	Inclusión de proceso y tiempos de eliminación de información electrónica	MAH	Abril 2019
6	Se actualiza el mecanismo para la realización de las copias de seguridad.	LBR	Junio 2019
7	Se actualiza el mecanismo para la realización de las copias de seguridad v2	RFML	Junio 2021
8	Se actualiza el mecanismo para la realización de las copias de seguridad v3	RFML	Mayo 2022

9	Se adecua el tiempo de eliminación de información, de acuerdo a lo solicitado por el cliente.	CST	Septiembre 2023
10	Se actualiza el punto 7.1, se especifica que la información de CitiBanamex que se encuentra en el sistema ERP de la organización, también debe ser eliminada, cada 6 meses.	CST	Mayo 2024
11	Actualización del documento para reforzar políticas generales de seguridad de la información y alinearlas a los requisitos de la norma ISO/IEC 27001:2022.	SSA	Septiembre 2025

V. REFERENCIAS

- MAN GSI 001 Manual de gestión de seguridad de la información
- POL GSI 001 Políticas generales de seguridad de la información
- LIS GSI 023 Inventario y clasificación de activos
- LIS CAL 001 Lista de información documentada controlada
- PRO GSI 015 Gestión de activos, clasificación y control de la información
- FOR CAL 007 Destrucción de información documentada

VI. ABREVIACIONES Y DEFINICIONES

Abreviaciones:

DGE	Director General / Director General Adjunto
GAD	Gerente Administrativo
CSG	Coordinador de Sistemas de Gestión
CST	Coordinador de Sistemas TI
N/A	No Aplica
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información

Definiciones:

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

VII. DESARROLLO DE ACTIVIDADES

No.	Descripción	Responsable(s)
1	Respaldo de la información	
1.1	**Alcance de respaldos** Se realizan **respaldos automáticos de toda la información crítica y no crítica** de la organización, utilizando los medios seleccionados y controlados por el área de Sistemas, previamente aprobados por la Dirección General. • Los respaldos cubren: bases de datos de sistemas críticos, servidores de archivos, configuraciones de red, documentación administrativa y carpetas compartidas de cada área. • Se programan **copias de seguridad automáticas cada 60 minutos** y, adicionalmente, se ejecutan copias **completas y diferenciales de manera diaria** mediante la herramienta **Robocopy**. • Toda incidencia o error en la ejecución del respaldo debe documentarse en **CIA-Desk** para su análisis y resolución.	Sistemas
1.2	**Infraestructura y soportes de respaldo (versión actualizada)** La organización cuenta con una infraestructura tecnológica diseñada bajo el principio de **segregación de aplicativos**, lo que significa que cada sistema crítico (ERP CIASC, SICOB, FileMaker, Aspel, OPTI-RISKS, Servidor Web, etc.) opera en un **servidor dedicado**. Este modelo de segregación permite: • **Independencia de respaldos:** cada servidor genera sus propias copias de seguridad, reduciendo el riesgo de que un fallo afecte a múltiples aplicativos al mismo tiempo. • **Mayor frecuencia:** al estar distribuidos en servidores separados, los respaldos se realizan con intervalos más cortos (cada **60 minutos**) sin afectar el rendimiento de la red ni la operación. • **Mayor velocidad:** los respaldos individuales son más rápidos, pues cada tarea se concentra en un volumen de información optimizado y no en cargas combinadas de varios aplicativos. • **Mejor control y trazabilidad:** cada respaldo queda registrado en **CIA-Desk** y vinculado al servidor correspondiente en **GLPI**, lo que facilita auditorías, conciliaciones y pruebas de restauración. Infraestructura de soportes implementada: • **NAS dedicados en cada sede (Nezahualcóyotl, Insurgentes y Toluca)** para resguardo local. • **Arreglos RAID 1 y RAID 5** configurados en servidores para tolerancia a fallos.	Sistemas

	• **Instantáneas (snapshots)** programadas en cada servidor para recuperación rápida frente a borrados accidentales o corrupción de discos. • **Capacidad de respaldo disponible:** servidores de almacenamiento con discos de 6 **TB** y enlaces de red de **1 Gbps**. Con esta estrategia, los respaldos son **más frecuentes, rápidos y eficientes**, manteniendo un balance entre **continuidad operativa** y **resiliencia de la información**.	
1.3	**Respaldos de bases de datos y sistemas críticos** El área de Sistemas ejecuta respaldos de las principales bases de datos y aplicaciones de la organización de la siguiente forma: • SICOB • FileMaker • Aspel • ERP CIASC • CIA - Desk • OPTI – Risk • Intranet SGC • Servidor de Archivos • Directorio Activo • VPN Printunl	Sistemas
1.4	**Concentración y resguardo** El área de Sistemas es responsable de concentrar y custodiar las copias de seguridad, asegurando que se conserven durante el tiempo definido por las políticas de la organización y conforme a los requisitos legales y contractuales. • Los respaldos almacenados en NAS y RAID se encuentran **cifrados** para mantener la confidencialidad de la información. • Los registros de ejecución de respaldos son revisados **diariamente** por el Coordinador de TI.	Sistemas
1.5	Carpetas de intercambio de información entre áreas. Para facilitar la entrega de información de un área a otra, y mantener los principios de rendición de cuentas y correcta disposición de los activos de información, así como su cancelación y borrado cuando ya no son necesarios, se designarán carpetas compartidas con las restricciones indicadas posteriormente.	Sistemas
1.6		Personal

	Las áreas que requieran recibir información de otra deberán solicitar autorización para que se asigne una carpeta de entrega de información, distinta y separada de la carpeta compartida por el área para su trabajo cotidiano.	
1.7	No deberán tener permisos para la misma carpeta más de dos áreas a la vez, a excepción hecha para dirección que cuenta con acceso a todas las carpetas (solo lectura).	Sistemas
1.8	Para mantener la rendición de cuentas sobre el uso de los activos, una vez recibida la información, el área receptora deberá guardar los archivos en su propia carpeta compartida, a la que solo su personal tiene acceso.	Personal
1.9	Se eliminará rutinariamente la información en dicha carpeta de intercambio, de acuerdo con los tiempos aprobados por dirección en la autorización recibida por el área.	Sistemas
2	**Monitoreo y verificación de respaldos**	
2.1	Los respaldos de todos los **sistemas críticos** de la organización (**SICOB, Opti-Risks, FileMaker, Aspel, SGC, SGCI, CIADESK y ERP**), así como de las carpetas compartidas en los servidores, son **monitoreados y verificados de manera continua** por el área de Sistemas. • Gracias al principio de **segregación de aplicativos**, cada sistema cuenta con su propio servidor dedicado, lo que permite que los respaldos se ejecuten de manera independiente, aumentando la frecuencia de copias y reduciendo el tiempo de ejecución. • Los **respaldos automáticos se realizan cada 60 minutos**, complementados con respaldos completos/diferenciales diarios en cada servidor. • El **Coordinador de Sistemas TI** valida diariamente en los registros de respaldo que los procesos se hayan completado sin errores. • En caso de detectarse fallas en la ejecución o inconsistencias en la validación de archivos respaldados. 1. El incidente se documenta de inmediato en el **portal CIA-Desk**, con detalle del servidor afectado, hora y descripción del error. 2. Se inicia el procedimiento de corrección, priorizando los sistemas críticos y notificando a la Gerencia Administrativa en caso de retraso en la ejecución del respaldo.	Sistemas
3	Eliminación y/o destrucción de información contenida soportes y equipos móviles	
3.1	• Antes de la destrucción, baja o reutilización de cualquier **equipo móvil** (laptops, teléfonos, tabletas u otros dispositivos portátiles), todos los **datos, configuraciones y software con licencia** deberán ser eliminados de manera segura.	Sistemas

	• La eliminación se realizará utilizando el software **Privacy Eraser**, el cual garantiza la sobrescritura segura de la información, imposibilitando su recuperación por terceros. • Adicionalmente, se verificará que los controles de seguridad (BitLocker, SentinelOne, certificados SSL Fortinet) hayan sido revocados o desactivados antes de la entrega o destrucción del activo. • Cada proceso de borrado debe documentarse en **CIA-Desk** y actualizarse en **GLPI**, cambiando el estado del activo a "En baja" o "En destrucción".	
4	Eliminación y/o destrucción en equipos PC y Servidores	

4.1	• El área de Sistemas es responsable de verificar y borrar de forma segura la información contenida en **PCs y servidores**, siguiendo los criterios de **clasificación de la información** definidos en el **PRO-GSI-015 – Gestión de activos, clasificación y control de la información**.
	• El borrado se ejecuta mediante **Privacy Eraser**, asegurando la sobrescritura y eliminación definitiva de los datos antes de la reasignación, reciclaje o baja de equipos.
	• Este proceso es **obligatorio** cuando:
	  ○ Lo solicite un cliente como requisito contractual.
	  ○ El equipo vaya a ser reasignado a otro usuario.
	  ○ El servidor o equipo sea retirado definitivamente de la operación.
		Sistemas

5	Termino de relación comercial con clientes	
5.1	**Notificación y arranque del proceso** • Cuando finalice la relación comercial con un cliente, la Dirección General notificará al área de Sistemas por correo electrónico para iniciar el proceso de eliminación total de la información asociada a dicho cliente. • Antes de ejecutar cualquier borrado, el área de Sistemas valida si existen obligaciones de retención contractual, regulatorias o legales vigentes. En caso de existir, se coordina con Dirección/Legal el alcance y los plazos (legal hold). Si no existen restricciones, se continúa con la eliminación.	Dirección

5.2	El área de Sistemas ejecutará la **destrucción lógica** de toda la información almacenada y procesada durante la vigencia del servicio, incluyendo pero no limitada a los siguientes servidores: • SICOB • ERP CIASC • OPTI – Risk • Servidor de Archivos • Directorio Activo La eliminación se realiza utilizando **Privacy Eraser** configurado con el **algoritmo Zero Fill**, ejecutando **tres (3) pasadas completas de sobrescritura** en todos los sectores del disco: 1. Primera pasada con valores binarios “0”. 2. Segunda pasada con valores binarios “1”. 3. Tercera pasada con patrones aleatorios. Este proceso garantiza que los datos no puedan ser recuperados por herramientas de recuperación ni mediante análisis forense avanzado, cumpliendo con los estándares internacionales **DoD 5220.22-M** y **NIST SP 800-88 Rev. 1** de eliminación segura. Al finalizar la ejecución, **Privacy Eraser genera un log de proceso exitoso**, el cual se adjunta como evidencia en **CIA-Desk** y en el **FOR-CAL-007 – Destrucción de Información Documentada**, asegurando trazabilidad y respaldo documental del proceso.	Sistemas

5.3	**Evidencia previa y verificación posterior**
	
	• Antes del borrado, el área de Sistemas captura evidencias técnicas del estado inicial:
	  ○ Peso total de la información a eliminar.
	  ○ Cantidad de archivos y directorios.
	  ○ Tipos/extensiones predominantes.
	  ○ Rutas y servidores involucrados.
	
	• Después del borrado, se ejecuta una búsqueda indexada en:
	  ○ Los servidores intervenidos.
	  ○ Volúmenes compartidos relevantes.
	  ○ Segmentos de red LAN que pudieran albergar copias residuales.
	
	El objetivo es corroborar la inexistencia de archivos, cachés, índices o huellas residuales que involucren al cliente. Se anexan capturas y reportes de estas validaciones como evidencia técnica.
		Sistemas

5.4	El área de sistemas levantará un ticket en CIA Desk, documentando la actividad y enviará por correo electrónico a la dirección general la evidencia previa al borrado de información, también la evidencia posterior al borrado de información y por último se documentará en el formato **Destrucción de información documentada FOR CAL 007** donde se asentarán las rutas, carpetas, cantidades, peso de los archivos destruidos y así como las firmas de las áreas involucradas. Con esta información daremos garantía al cliente que nuestros servidores, computadoras y correos electrónicos ya no cuentan con información de su representada. En caso de ser necesario, nuestra organización puede extender una invitación para que personal de nuestro cliente acuda a las instalaciones a testificar la destrucción y también pueda ser documentada por ellos mismos.	Sistemas
6	Soportes en papel	
6.1	Los empleados de la organización que manejan documentos individuales son responsables de entregar los documentos obsoletos al archivo muerto para su resguardo y posterior destrucción. Los soportes en papel se destruyen a través de un proveedor de destrucción de documentos y de acuerdo con el tiempo de resguardo estipulado en la **Lista de información documentada controlada LIS CAL 001**. Para los documentos controlados y confidenciales se solicitará el servicio de destrucción con el proveedor certificado para dicha tarea de acuerdo con la clasificación de la información. Las áreas deberán llenar el formato de **Destrucción de información documentada FOR CAL 007**, para tener una relación de lo destruido. Se invita a los clientes de Investigación de Crédito a presenciar la destrucción. Finalmente, se documenta y se conserva el certificado de destrucción como evidencia. Aquellos documentos que no son controlados podrán ser destruidos en la máquina trituradora del Corporativo, quedando bajo su total responsabilidad del usuario la información que ha sido eliminada y esta siempre será declarada en el **FOR CAL 007 Destrucción de Información Documentada**; en dicha destrucción debe estar presente el coordinador de sistemas de gestión para dar fe de la actividad.	Personal / Calidad
7	Soportes en electrónico	
7.1	Toda la información que se encuentra en la Organización está debidamente protegida para evitar la pérdida de **confidencialidad, integridad o disponibilidad**. Asimismo, se realizan **destrucciones periódicas** de acuerdo con los tiempos establecidos por nuestros clientes, eliminando la información directamente desde las carpetas de los servidores donde se encuentre y registrando la actividad en el formato **FOR-CAL-007 – Destrucción de Información**	Sistemas / Gerente Administrativo

Documentada, en apego a los tiempos de resguardo estipulados en la **LIS-CAL-001 – Lista de Información Documentada Controlada**.

Para el caso de **HDD y SSD**, se utiliza la herramienta **Privacy Eraser** configurada con el **algoritmo Zero Fill**, ejecutando **tres (3) pasadas completas de sobrescritura** en todos los sectores del disco: la primera con valores binarios "0", la segunda con valores binarios "1" y la tercera con patrones aleatorios. Este procedimiento asegura la eliminación definitiva de los datos, imposibilitando su recuperación mediante técnicas de recuperación forense, y cumple con los estándares internacionales **DoD 5220.22-M** y **NIST SP 800-88 Rev. 1** de eliminación segura de información.

Citibanamex

1. Para la ejecución del borrado seguro de la información que nuestra organización almacena y maneja de CitiBanamex, cada semestre el personal de CitiBanamex envía un correo electrónico al encargado de gestión domiciliaria y la dirección general; en dicho correo electrónico se solicita la eliminación de los documentos, correos electrónicos e información dentro del sistema interno ERP, también se indica el periodo de eliminación, así mismo se adjunta el formato, **registros electrónicos y medios magnéticos para destrucción F-GCB-OPS-CO-FC CGO-006**, para su correcto llenado y registro.

Nota: La solicitud puede ser de los siguientes correos electrónicos.

- andrea.araceli.saynesortiz@citi.com
- eberth.perezgonzalez@citibanamex.com
- blanca1.guzman@citi.com

2. El encargado de gestión domiciliaria y el coordinador de sistemas TI toman captura de pantalla donde se muestren él antes, así como tomar el número de archivos a eliminar.

3. El Coordinador de Sistemas TI sobrescribe la información con la herramienta Privacy eraser con el algoritmo zero, a fin de poder destruir toda la información que contengan dichas carpetas o repositorios de Citbanamex.

4. El encargado de gestión domiciliaria reenvía el formato, **registros electrónicos y medios magnéticos para destrucción F-GCB-OPS-CO-FC CGO-006** al coordinador de sistemas TI vía correo electrónico para que este haga el llenado correcto de dicho formato, así como el adjuntar la evidencia de las capturas de pantalla del antes y después de las carpetas, así como capturas de la herramienta sobreescribiendo los sectores del disco duro.

5. El encargado de gestión domiciliaria escanea el formato, **registros electrónicos y medios magnéticos para destrucción F-GCB-OPS-CO-FC CGO-006** con firmas y lo envía con el archivo de capturas vía correo electrónico respondiendo el correo de solicitud y envía físicamente el formato **registros electrónicos y medios magnéticos para destrucción F-GCB-OPS-CO-FC CGO-006** a las instalaciones del cliente, para firma.

	BBVA Para toda la información que la organización almacena, trasmite y maneja de BBVA se sobrescribe el disco duro con la herramienta HDShredder con el algoritmo zero, a fin de poder destruir toda la información que contengan dichos discos duros con información de BBVA, esta actividad es realizada cada 12 meses.	
7.2	**Métodos de Destrucción de la Información que utiliza la organización dependiendo el tipo de uso que se dará al disco duro o soporte electrónico.** Los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son: la desmagnetización, la destrucción y la sobreescritura en la totalidad del área de almacenamiento de la información, por ello la organización utiliza los 3 medios para ejecutar la actividad de eliminación segura de la información. **Desmagnetización** La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo. Este método es válido para la destrucción de datos de los dispositivos magnéticos, como, por ejemplo, los discos duros, disquetes, cintas magnéticas de backup, etc.; Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas. **Destrucción física** El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento: • Desintegración, pulverización, fusión e incineración. • Trituración **Sobreescritura.** La sobreescritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento. La sobreescritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD.	Sistemas / Gerente Administrativo
7.3		Sistemas / Gerente Administrativo

DESTRUCCIÓN FÍSICA	DESMAGNETIZACIÓN	SOBRE-ESCRITURA
✓ Eliminación de forma segura de la información	✓ Eliminación de forma segura de la información	✓ Eliminación de forma segura de la información
✗ Un sistema de destrucción para cada soporte	✗ Una configuración del sistema para cada soporte	✓ Una única solución para todos los dispositivos
✗ Dificultad de certificación del proceso	✗ Dificultad de certificación del proceso	✓ Garantía documental de la operación
✗ Necesidad de transportar los equipos a una ubicación externa	✗ Necesidad de transportar los equipos a una ubicación externa	✓ Posibilidad de eliminación en las propias oficinas
✗ Medidas extraordinarias para garantizar la cadena de custodia	✗ Medidas extraordinarias para garantizar la cadena de custodia	✓ Garantía de la cadena de custodia
✓ Destrucción de dispositivos, no regrabables, ópticos	✗ Sólo válido para dispositivos de almacenamiento magnético	✗ No válido para dispositivos no regrabables ni ópticos
✗ Destrucción definitiva y dificultad de reciclaje de materiales	✗ Tras el proceso el dispositivo deja de funcionar correctamente	✓ Reutilización de los dispositivos con garantías de funcionamiento.

SOPORTE	TIPO	DESTRUCCIÓN FÍSICA	DESMAGNETIZACIÓN	SOBRE ESCRITURA
Discos Duros	Magnético	✓	✓	✓
Discos Flexibles	Magnético	✓	✓	✓
Cintas de *Backup*	Magnético	✓	✓	✓
CD	Óptico	✓	✗	✗
DVD	Óptico	✓	✗	✗
Blu-ray Disc	Óptico	✓	✗	✗
Pen Drive	Electrónico	✓	✗	✓ [3]
Discos Duros SSD	Electrónico	✓	✗	✓ [3]