Ministerio de
Planificación Estratégica y Modernización

Gobierno de Jujuy
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Desinfección / Eliminación Segura

22
CAPÍTULO

Desinfección / Eliminación Segura

1.0 Propósito y Beneficios

Los sistemas de información capturan, procesan y almacenan información utilizando una amplia variedad de medios, incluido el papel. Esta información no sólo se encuentra en el medio de almacenamiento previsto, sino también en los dispositivos utilizados para crear, procesar o transmitir esta información. Estos medios pueden requerir una disposición especial para mitigar el riesgo de divulgación no autorizada de información y garantizar su confidencialidad.

2.0 Declaración de información

De acuerdo con la Política de Seguridad de la Información, la información debe ser adecuadamente gestionada desde su creación, pasando por el uso autorizado, hasta su adecuada disposición.

La Repartición debe garantizar que los usuarios y custodios de la información sean conscientes de su sensibilidad y de los requisitos básicos para la desinfección de los medios y su eliminación segura.

La Repartición debe garantizar que todos los agentes administrativos, profesionales y técnicos, incluidos los administradores, conozcan el proceso de desinfección de los medios y eliminación segura para establecer la responsabilidad adecuada de todos los datos.

La Repartición debe garantizar que el material confidencial sea destruido únicamente por personal autorizado y capacitado, ya sea interno o contratado, utilizando los métodos descritos en esta norma.

La Repartición podrá utilizar proveedores de servicios con fines de destrucción siempre que la información permanezca segura hasta que se complete la destrucción. Los proveedores de servicios deben seguir este estándar. La entidad debe asegurarse de que existan acuerdos contractuales o de mantenimiento que sean suficientes para proteger la confidencialidad de los medios y la información del sistema de manera acorde con los estándares de clasificación de la información.

Métodos de desinfección de medios

La siguiente tabla muestra los tres tipos de métodos de desinfección y el impacto de cada método.

Método de desinfección	Uso apropiado	Descripción
Borrar	Si los medios serán reutilizados y no saldrán del control de la entidad.	Protege la confidencialidad de la información contra un ataque reemplazando los datos escritos con datos aleatorios. La limpieza no debe permitir que las utilidades de recuperación de datos, discos o archivos recuperen información.
Purgar	Si los medios serán reutilizados y saldrán del control de la entidad.	Protege la confidencialidad de la información contra un ataque mediante desmagnetización o borrado seguro.
Destrucción física	Si los medios no se reutilizarán en absoluto.	La intención es destruir completamente los medios.

Proceso de decisión de desinfección

El proceso de decisión se basa en la confidencialidad de la información, no en el tipo de medio. Las Reparticiones eligen el tipo de sanitización a utilizar, y el tipo de sanitización es aprobado por el propietario de la Información. La técnica utilizada puede variar según el tipo de medio y la tecnología disponible para el custodio, siempre y cuando se cumplan los requisitos del tipo de sanitización. Las técnicas de desinfección recomendadas para tipos específicos de medios se describen en el Apéndice A de NIST 800-88, Rev. 1, Pautas para la desinfección de medios, Recomendaciones mínimas de desinfección.

La eliminación sin desinfección debe considerarse solo si la divulgación de información no tendría impacto en la misión gubernamental, no resultaría en daños a los activos del Gobierno de Jujuy y no resultaría en pérdidas financieras o daños a ningún individuo.

La categorización de seguridad de la información, junto con los factores ambientales internos, deberían impulsar las decisiones sobre cómo tratar con los medios. La clave es pensar primero en términos de confidencialidad de la información y luego aplicar consideraciones basadas en el tipo de medio.

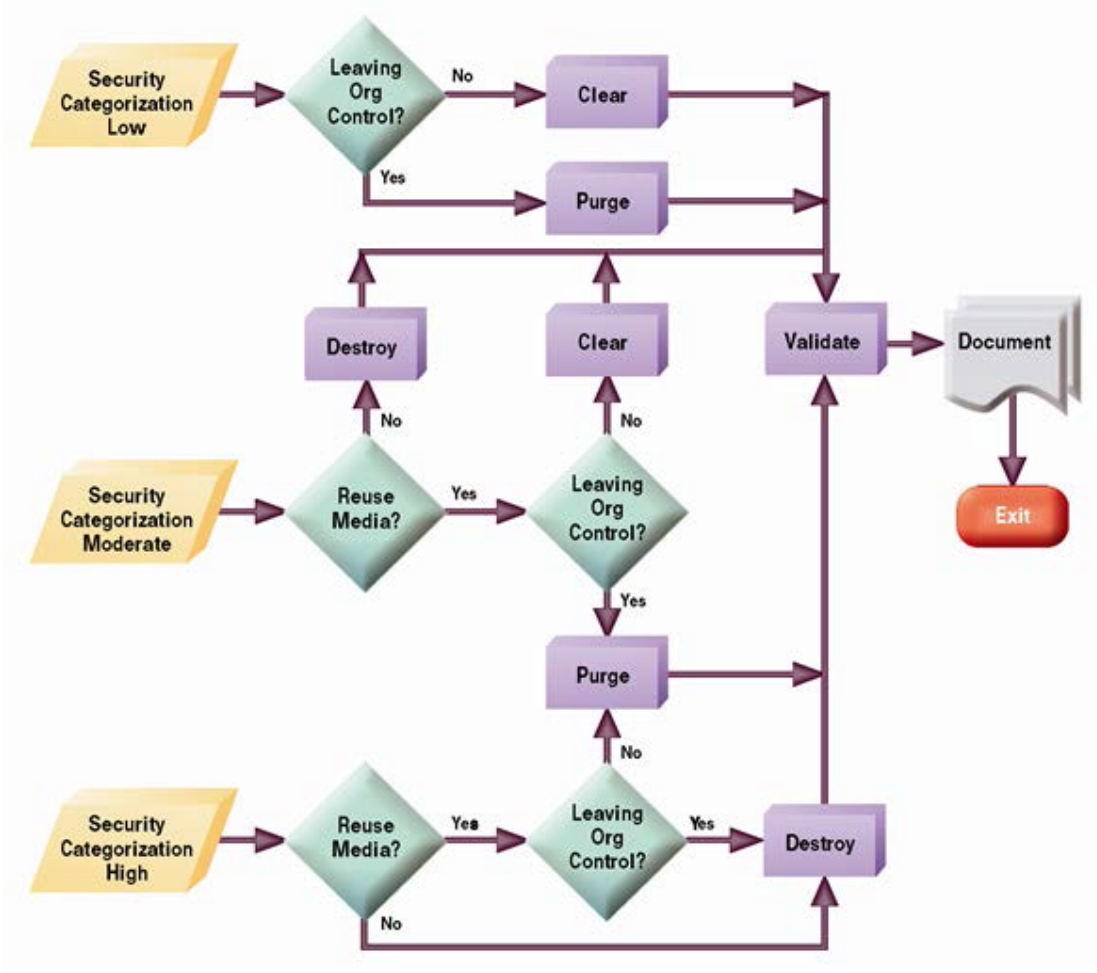

Figura 4.1- Flujo de decisiones de desinfección y disposición
(de NIST 800-88, Rev. 1, Directrices para la desinfección de medios)

Se debe comprender el costo versus el beneficio de un proceso de desinfección antes de tomar una decisión final. Las Reparticiones siempre pueden aumentar el nivel de saneamiento aplicado si ello es razonable y así lo indica una evaluación del riesgo existente. Por ejemplo, aunque Clear o Purge puede ser la solución recomendada, puede ser más rentable (teniendo en cuenta la capacitación, el seguimiento y la validación, etc.) destruir los medios en lugar de utilizar una de las otras opciones. Las Reparticiones no podrán disminuir el nivel de sanitización requerido.

Control de medios

Un factor que influye en una decisión de desinfección es quién tiene control y acceso a los medios. Este aspecto debe ser considerado cuando los medios

abandonan el control gubernamental. El control de los medios puede transferirse cuando los medios se devuelven de un contrato de locación o se donan o revenden para ser reutilizados fuera de la gobernación. Los siguientes son ejemplos de control de medios:

Bajo control:

- Los medios que se entregan para mantenimiento todavía se consideran bajo el control de la Repartición si existen acuerdos contractuales y el proveedor de mantenimiento prevé específicamente la confidencialidad de la información.
- El mantenimiento realizado en el sitio de una Repartición, bajo la supervisión de la Repartición, por un proveedor de mantenimiento también se considera bajo el control de la Repartición.

No bajo control de la Repartición:

- Los medios que se intercambian por garantía, reembolso de costos u otros fines y donde los medios específicos no serán devueltos a la Repartición se consideran fuera del control de la Repartición.

Reutilización de medios

Las Reparticiones deben considerar el costo versus el beneficio de la reutilización. Puede ser más rentable (teniendo en cuenta la capacitación, el seguimiento y la validación, etc.) destruir los medios en lugar de utilizar una de las otras opciones.

Limpiar / Purgar / Destruir

Método	Descripción
Borrar	Un método para desinfectar los medios es utilizar productos de software o hardware para sobrescribir el espacio de almacenamiento direccionable por el usuario en los medios con datos no confidenciales, utilizando los comandos estándar de lectura y escritura para el dispositivo. Este proceso puede incluir sobrescribir no sólo la ubicación de almacenamiento lógico de un archivo (por ejemplo, tabla de asignación de archivos), sino que también debe incluir todas las ubicaciones direccionables por el usuario. El objetivo de seguridad del proceso de sobrescritura es reemplazar los datos de destino con datos no confidenciales. La sobrescritura no se puede utilizar para medios dañados o que no se pueden reescribir y es posible que no aborde todas las áreas del dispositivo donde se pueden conservar datos confidenciales. El tipo y tamaño del medio también pueden influir en si la sobrescritura es un método de desinfección adecuado. Por ejemplo, los dispositivos de almacenamiento basados en memoria flash pueden contener celdas de repuesto y realizar una nivelación de desgaste, lo que hace que sea inviable para un usuario desinfecte todos los datos anteriores usando este enfoque porque es posible que el dispositivo no admita abordar directamente todas las áreas donde se han almacenado datos confidenciales usando el Interfaz nativa de lectura y escritura. La operación Borrar puede variar contextualmente para medios que no sean dispositivos de almacenamiento dedicados, donde el dispositivo (como un teléfono celular básico o un equipo de oficina) solo brinde la capacidad de devolver el dispositivo al estado de fábrica (generalmente simplemente eliminando los punteros del archivo) y no admite directamente la capacidad de reescribir o aplicar técnicas específicas de medios a los contenidos de almacenamiento no volátiles. Cuando no se admite la reescritura, los restablecimientos del fabricante y los procedimientos que no incluyen la reescritura pueden ser la única opción para borrar el dispositivo y los medios asociados. Estos aún cumplen con la definición de Borrado siempre que la interfaz del dispositivo disponible para el usuario no facilite la recuperación de los datos borrados.

Purgar	Algunos métodos de purga (que varían según el medio y deben aplicarse teniendo en cuenta las consideraciones que se describen más adelante a lo largo de este documento) incluyen la sobrescritura, el borrado de bloques y el borrado criptográfico, mediante el uso de comandos de desinfección de dispositivos estandarizados y dedicados que aplican técnicas específicas de los medios para evitar la abstracción inherente a los comandos típicos de lectura y escritura. Las técnicas destructivas también hacen que el dispositivo se purgue cuando se aplican eficazmente al tipo de medio apropiado, incluida la incineración, trituración, desintegración, desmagnetización y pulverización. El beneficio común de todos estos enfoques es la garantía de que no es posible recuperar los datos utilizando técnicas de laboratorio de última generación. Sin embargo, doblar, cortar y el uso de algunos procedimientos de emergencia (como usar un arma de fuego para perforar un dispositivo de almacenamiento) solo pueden dañar el medio, ya que algunas partes del medio pueden permanecer intactas y, por lo tanto, ser accesibles mediante técnicas de laboratorio avanzadas. La desmagnetización hace que un dispositivo magnético heredado se purgue cuando la fuerza del desmagnetizador se adapta cuidadosamente a la coercitividad del medio. Puede ser difícil determinar la coercitividad basándose únicamente en la información proporcionada en la etiqueta. Por lo tanto, consulte al fabricante del dispositivo para obtener detalles sobre la coercitividad. Nunca se debe confiar únicamente en la desmagnetización para dispositivos de almacenamiento basados en memoria flash o para dispositivos de almacenamiento magnéticos que también contienen almacenamiento no volátil y no magnético. La desmagnetización inutiliza muchos tipos de dispositivos (y en esos casos, la desmagnetización también es una técnica de destrucción).

Destruir	Existen muchos tipos, técnicas y procedimientos diferentes para la destrucción de medios. Si bien algunas técnicas pueden hacer que no sea factible recuperar los datos de destino a través de la interfaz del dispositivo y no se puedan usar para el almacenamiento posterior de datos, el dispositivo no se considera destruido a menos que la recuperación de los datos de destino no sea factible utilizando técnicas de laboratorio de última generación. • *Desintegrar, pulverizar, fundir e incinerar*. Estos métodos de desinfección están diseñados para destruir completamente los medios. Por lo general, se llevan a cabo en una instalación de destrucción de metales subcontratada o en una instalación de incineración autorizada con las capacidades específicas para realizar estas actividades de manera efectiva y segura. • *Desgarrar*. Las trituradoras de papel se pueden utilizar para destruir medios flexibles, como disquetes, una vez que los medios se retiran físicamente de sus contenedores exteriores. El tamaño de los fragmentos de basura debe ser lo suficientemente pequeño como para que exista una seguridad razonable, en proporción a la confidencialidad de los datos, de que no se pueden reconstruir. Para dificultar aún más la reconstrucción de los datos, el material triturado se puede mezclar con material no sensible del mismo tipo (por ejemplo, papel triturado o soporte flexible triturado). La aplicación de técnicas destructivas puede ser la única opción cuando los medios fallan y otras técnicas de limpieza o purga no se pueden aplicar de manera efectiva a los medios, o cuando la verificación de los métodos de limpieza o purga falla (por razones conocidas o desconocidas).

Tabla 5-1 – Métodos de desinfección
(de NIST 800-88, Rev. 1, Directrices para la desinfección de medios)

Validación

Las reparticiones deben probar una muestra representativa de los medios para una desinfección adecuada y garantizar que se mantenga la protección adecuada.

Verificación de equipos

Si la Repartición está utilizando herramientas de desinfección (por ejemplo, un desmagnetizador), la entidad debe tener procedimientos para garantizar que las herramientas estén funcionando de manera efectiva.

Verificación de Competencias del Personal

Las Reparticiones deben garantizar que los operadores de equipos estén adecuadamente capacitados y sean competentes para realizar funciones de desinfección.

Documento

Las Reparticiones deben mantener un registro de su desinfección para documentar qué medios se desinfectaron, cuándo, cómo se desinfectaron y la disposición final de los medios.

3.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

4.0 Historial de revisiones

Fecha	Descripción de Cambio	Participantes
07/08/2024	Revision inicial	Alejandro Castro, Pablo Zalazar
08/08/2024	Visado, y corrección de errores	Alejandro Castro.

5.0 Documentos relacionados

NIST 800-88, Rev. 1, Directrices para la desinfección de medios.