CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Eduar Enrique Navarro Morales Cargo: Coordinador Informática Forense y Seguridad Digital.	Nombre: Oscar Javier Asprilla Cargo: Jefe Oficina de Tecnología e Informática.	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad. Fecha: 2019-01-18

1 OBJETIVO

Presentar los criterios, formas, orientaciones y recomendaciones que deben ser utilizados por los propietarios y responsables de los activos de información de la Oficina de Tecnología e Informática (OTI) de la Superintendencia de Industria y Comercio (SIC), para garantizar la confidencialidad de la información.

2 DESTINATARIOS

Servidores públicos y contratistas de la SIC.

3 GLOSARIO

ACTIVO DE INFORMACIÓN: Conforme con la norma ISO 27001[1], un activo de información es "cualquier cosa que tiene valor para la organización".

AES (Advanced Encryption Standard): Algoritmo de encriptación para datos electrónicos establecido por el NIST (National Institute of Standards and Technology) como un estándar federal del gobierno de los Estados Unidos en estado vigente. AES es un algoritmo de llave simétrica, por lo tanto utiliza la misma llave para cifrar y descifrar información. AES también es definido dentro del estándar ISO/IEC 18033 que especifica sistemas de cifrado para la confidencialidad de datos.

ALMACENAMIENTO: Se refiere a la acción y efecto de almacenar[2]. En el contexto de almacenamiento de activos de información se refiere a la forma en la que se conserva o guarda un activo, como medios magnéticos, cajas, PC's, servidores, CD's, DVD's, USBs, cintas magnéticas, etc., para el caso de información digital o depósitos, cajas, armarios, bodegas para el caso de información física.

CIFRAR: Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar.

CIFRADO: Se refiere al procedimiento de cifrar (ver cifrar) un activo de información. En caso de que se requiera un procedimiento de cifrado para la información de tipo digital, se consideran un conjunto de características técnicas mínimas a tener en cuenta para garantizar un correcto cifrado.

---

[1] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), NTC-ISO/IEC 27005 Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información, Colombia, 2008.

[2] Diccionario de la Lengua Española, Vigésimo segunda edición. Real Academia Española (RAE).

CÓDIGO HASH: Código generado por medio de una función hash, el cual representa un texto cifrado usado para proveer integridad en un archivo de tipo digital. Un cambio en el archivo provoca un cambio en el código Hash e indica por lo tanto una afectación a la integridad del archivo. Cuando dos elementos de información provocan el mismo código hash se dice que existe una colisión.

CREACIÓN: Se refiere a la concepción de documentos (con información física o digital), el momento en el cual se origina el contenido de un medio de información.

DESTRUCCIÓN: Acción y efecto de destruir[3]. En el contexto de destrucción de activos de información se refiere a la dinámica para la inutilización total o desaparición de la información que maneja el activo en el momento en el que éste finaliza su ciclo de vida:

- Incineración: desaparición de información exponiéndola a altas temperaturas para destruirla por medio del fuego.
- Borrado Seguro: aplica solo para información de tipo digital, es un procedimiento de destrucción que asegura la no recuperación de la información almacenada en un medio de almacenamiento (Revisar documento GS01-P09 Procedimiento de Borrado Seguro).
- Trituración: aplica a la destrucción de papel por medio de máquinas trituradoras.

IETF (Internet Engineering Task Force)[4]: Grupo de Trabajo de Ingeniería de Internet. Es una entidad internacional de normalización que regula las propuestas y los estándares de internet, incluyendo análisis de seguridad a un nivel de arquitectura y protocolos de red.

NIST (National Institute of Standards and Technology)[5]: Instituto Nacional de Estándares y Tecnología. Es la agencia de tecnología federal del Departamento de Comercio de los Estados Unidos que brinda a la industria, la academia, los gobiernos y otros usuarios materiales de referencia (estándares, recomendaciones y guías) en los ámbitos de biotecnología, nanotecnología, tecnologías de la información y fabricación avanzada. Los estándares relacionados con tecnologías de cifrado son elaborados por la División de Seguridad Informática (CSD, Computer Security Division).

---

[3] Diccionario de la Lengua Española, Vigésimo segunda edición. Real Academia Española (RAE).

[4] http://www.ietf.org/

[5] http://www.nist.gov/index.html

SHA (Secure Hashing Algorithm): Familia de funciones para la creación de códigos hash, publicada por el NIST y definido como un estándar federal para el procesamiento de información por el gobierno de Estados Unidos. Las familias vigentes actualmente corresponden a SHA2 (SHA-256 y SHA-512) y SHA3.

TLS/SSL (Transport Layer Security/Secure Sockets Layer): Protocolos criptográficos para establecer una comunicación segura a través de internet. Mediante estos protocolos se garantiza la autenticación de las partes de la comunicación y la confidencialidad e integridad de la información transmitida.

TRANSPORTE: Sistema de medios para conducir cosas de un lugar a otro[2]. En el contexto de transporte de activos se refiere a las diferentes formas en la que se conduce la información de un lugar a otro y los cuidados que se deben tener en este proceso, según el nivel de clasificación del activo.

UNIDAD ORGANIZACIONAL: Corresponde a un segmento de la organización, la cual tiene sus propios planes, métricas, ingresos y costos. Cada unidad organizacional posee activos y los usa para crear valor para los clientes en la forma de bienes o servicios.

4 DESCRIPCIÓN DE ACTIVIDADES Y RESPONSABILIDADES

4.1 Niveles de clasificación

La rotulación de los activos de información tiene como objetivo asegurar que se tienen acuerdos en la OTI para compartir la información entre dependencias y terceros, de esta forma asegurar que la información recibe los niveles de protección adecuados. La información con base en su valor y de acuerdo a los requisitos de confidencialidad tiene diferentes grados de rotulación o manejo especial que se definen en la clasificación de activos de información.

En este documento se define el esquema de rotulación y se estipulan los niveles de protección para los activos de información.

Todo activo de información debe contar con una etiqueta que describe su clasificación a nivel de Confidencialidad de manera correspondiente.

La confidencialidad es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados[6].

[6] Tomado de NTC ISO/IEC 27002:2013

Los niveles de clasificación de los activos de información de la OTI son: Pública, uso Interno, Confidencial y Reservada como se muestra en la Tabla 1.

Tabla 1. Niveles de Clasificación

NIVEL	DESCRIPCIÓN	EJEMPLOS
Pública	Información que puede ser distribuida abiertamente al público, si la información está en manos del público no causará ningún daño a la OTI, a sus funcionarios, otras áreas o a otras entidades. Para que la información sea pública debe ser clasificada como tal por el área que la elaboró. Los documentos públicos pueden ser distribuidos libremente a las demás dependencias entidades o ciudadanos.	Material publicitario, información de la página web o carteleras en áreas abiertas al público.
Uso Interno	Información que NO se debe distribuir al público en general. Información que tiene un destinatario especifico. Información que es propia de la SIC y no se debe distribuir al público. Información que requiere autorización para distribuirla a una persona o entidad diferente a la SIC.	Prácticamente toda la información de trabajo de la SIC es de uso interno. Ejemplos de esta información son: cartas, memorandos, boletines internos, manuales, guías de entrenamiento, documentos de trabajo de las áreas, correos electrónicos, información misional o publicitaria que no ha sido autorizada para su distribución al público, reportes para entidades de control, documentos contables y financieros que solo se pueden suministrar con autorización, acuerdos de niveles de servicio, contratos, reportes de vacaciones. La mayoría de la información procesada en la entidad es de uso interno a menos que alguien con autoridad en la SIC permita su distribución al público o a las partes interesadas en dicha información.

Confidencial	Documentos clasificados como altamente sensitivos, esta información solo puede ser vista por un grupo de personas, o un área en particular. La divulgación solo se realiza a terceros bajo autorización del nivel directivo o bajo orden de autoridad competente.	Contraseñas de usuarios, números de cuentas corrientes o de ahorros de funcionarios, evaluaciones de propuestas antes de su publicación, información personal de funcionarios (dirección, teléfono, cargo, salario), configuración de equipos de cómputo, protocolos de seguridad, resultados de evaluaciones de riesgos, información de procesos legales, información de procesos disciplinaros en curso o información amparada por la ley de habeas data (artículos 15 y 20 de la Constitución Política Colombiana, ley 1266 de 2008 y ley 1581 de 2012).
Reservada	Información que está catalogada como reservada por LEY o MANDATO. Toda información catalogada como reservada también es de carácter CONFIDENCIAL.	Información de investigación a empresas intervinientes. Toda información que por ley se defina como reservada. De acuerdo a la ley 1581 de 2012, pueden caber dentro de esta categoría aquellos datos sensibles los cuales afecten la intimidad del titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

La clasificación de los activos de información se realiza en el momento en el que se realiza la valoración de éstos en términos de confidencialidad, en caso tal de presentarse dudas al momento de rotular un documento, por favor referirse al inventario de los activos de información y verificar el nivel de clasificación asignado.

4.2 Responsabilidad y propiedad de los activos de información

Tabla 2. Responsabilidad y Propiedad de los Activos de Información

RESPONSABILIDAD	FUNCIÓN
Propietario	Es la Unidad Organizacional donde se genera o produce la información. Sus responsabilidades son: • Identificar los activos de información. • Encargarse de la clasificación de sus activos.
Responsable	Es un funcionario perteneciente a la Unidad Organizacional propietaria de un grupo de activos de información y que toma decisiones sobre el manejo, protección, disposición y demás atribuciones del activo. Tiene bajo su cargo: • Definir las apropiadas medidas de protección que garanticen la Confidencialidad, Integridad y Disponibilidad del(los) activo(s) de información. • Monitorear que las medidas de protección implementadas sean las adecuadas. • Supervisar el cumplimiento de la política de clasificación de la información. • Autorizar y revocar el acceso a aquellas personas que tengan una necesidad de utilizar la información.
Custodio	Es un funcionario, grupo de funcionarios o una Unidad Organizacional, designados por el responsable, los cuales se encargan de mantener las medidas de protección sobre los activos de información. Los custodios de la información son responsables de: • Implantar controles de acceso a la información autorizada por los propietarios. • Utilizar las mejores prácticas con el fin de mantener la confidencialidad, la integridad, y la disponibilidad de las fuentes de información.
Usuarios	Son los colaboradores de la organización, quienes están autorizados por el responsable a acceder y manejar los activos de información, adicional a ello deben cumplir con todos los requerimientos de control especificados por el custodio de la información. Las responsabilidades de los usuarios son: • Acatar las políticas y procedimientos de clasificación y

	acceso a la información establecidos por los propietarios. • Acceder solamente a la información para la cual se encuentran autorizados. • Divulgar las violaciones de las políticas y procedimientos de clasificación y acceso a la información establecidos por los propietarios. • Obrar con el debido cuidado en el uso de información confidencial y reservada.

4.3 Manejo de la información

A continuación se definen los controles a aplicar para el manejo de la información en los diferentes niveles de clasificación:

Tabla 3. Manejo de la Información

NIVEL \ MANEJO	CREACIÓN	DISTRIBUCIÓN	ALMACENAMIENTO	TRANSPORTE	DESTRUCCIÓN
Público	No hay acción específica para este nivel.	Se puede distribuir libremente.	Al ser público no se requiere una acción específica más allá de la determinada en las tablas de retención documental.	Se puede transportar libremente.	No se requiere una acción específica más allá de la indicada en las tablas de retención documental.
Uso Interno	Rotular el activo con la etiqueta "Uso Interno"	El activo no puede enviarse a personal externo de la SIC, salvo que exista una autorización formal (por ejemplo en el caso de un derecho de petición).	Se debe almacenar según lo estipulado en las tablas de retención documental.	Se debe manejar correspondencia interna. En caso de ser necesaria la salida del activo, es necesario que vaya en un sobre sellado.	Si es información digital, debe realizarse un borrado seguro.
Confidencial	Rotular el activo con la etiqueta "Confidencial"	El activo debe definir el grupo de personas que pueden acceder a la información. Para la distribución de información digital, esta debe ser cifrada (1) antes de ser distribuida o se debe establecer un canal seguro antes de distribuirse (2). 1. El cifrado debe realizarse utilizando un algoritmo de cifrado que garantice la completa confidencialidad de la información y el acceso a la misma utilizando una única llave de cifrado. Para la selección del algoritmo de cifrado se recomienda revisar los algoritmos de cifrado en bloque aprobados por el NIST (ver definición en el glosario) en su publicación regular	Si es información digital, se debe almacenar cifrada utilizando un algoritmo de cifrado que garantice la completa confidencialidad de la información y el acceso a la misma utilizando una única llave de cifrado. Para la selección del algoritmo de cifrado se recomienda revisar los algoritmos de cifrado en bloque aprobados por el NIST (ver definición en el glosario) en su publicación regular de herramientas criptográficas aprobadas (En el momento de elaboración de esta guía, AES es uno de los algoritmos aprobados). Se debe verificar la integridad de la información utilizando una función Hash para la cual no exista un método computacional	Para el transporte de información digital, esta debe ser cifrada (1) antes de ser transportada o se debe establecer un canal seguro antes de transportarse (2). 1. El cifrado debe realizarse utilizando un algoritmo de cifrado que garantice la completa confidencialidad de la información y el acceso a la misma utilizando una única llave de cifrado. Para la selección del algoritmo de cifrado se recomienda revisar los algoritmos de cifrado en bloque aprobados por	Si es información digital, debe realizarse un procedimiento de borrado seguro que garantice la no recuperación de la información (Revisar documento GS01-P09 Procedimiento de Borrado Seguro de Información) y en lo posible realizar la destrucción del medio magnético por incineración. Si es información física, debe ser pasada por la trituradora de papel y separarla lo mejor posible de tal forma que no pueda ser reconstruida, antes de ir a la basura.

NIVEL \ MANEJO	CREACIÓN	DISTRIBUCIÓN	ALMACENAMIENTO	TRANSPORTE	DESTRUCCIÓN
		de herramientas criptográficas[7] (En el momento de elaboración de esta guía, AES es uno de los algoritmos aprobados). 2. Un canal seguro se debe establecer utilizando una suite de cifrado de gestión de claves (para algoritmos asimétricos o técnicas híbridas simétrica/asimétrica) que garantice la confidencialidad e integridad de la información transportada. Para la selección de la suite de cifrado de gestión de claves se recomienda revisar las suites aprobadas por el NIST en su publicación regular de herramientas criptográficas[7] (En el momento de elaboración de esta guía, TLS es una técnica híbrida aprobada por el NIST). Para su acceso debe solicitarse usuario y contraseña. Si es información física, esta debe permanecer en un sobre sellado antes de ser distribuida. Para distribuir este tipo de información	conocido para la generación de colisiones. Para la selección de la función hash se recomienda revisar las funciones de hash aprobadas por el NIST en su publicación regular de herramientas criptográficas (En el momento de elaboración de esta guía, SHA-256 y SHA-512 son funciones aprobadas). Para su acceso debe solicitarse usuario y contraseña. Se debe contar con una contraseña para acceder a la información digital, adicionalmente si esta información se almacena en un servidor, base de datos o repositorio digital, es necesario generar un mensaje de alerta al ingreso del software que lo controla, para advertir al usuario que está accediendo a información CONFIDENCIAL. Si es información física, se debe almacenar según lo dispuesto por las tablas de retención documental, en sobre sellado, bajo un control de registros de consulta.	el NIST (ver definición en el glosario) en su publicación regular de herramientas criptográficas[8] aprobadas (En el momento de elaboración de esta guía, AES es uno de los algoritmos aprobados). 2. Un canal seguro se debe establecer utilizando una suite de cifrado de gestión de claves (para algoritmos asimétricos o técnicas híbridas simétrica/asimétrica) que garantice la confidencialidad e integridad de la información transportada. Para la selección de la suite de cifrado de gestión de claves se recomienda revisar las suites aprobadas por el NIST en su publicación regular de herramientas criptográficas[7] (En el momento de elaboración de esta guía, TLS es una técnica híbrida aprobada por el	

[7] http://csrc.nist.gov/groups/ST/toolkit/index.html (Enlace web consultado en la fecha: 02-Diciembre-2014)

NIVEL \ MANEJO	CREACIÓN	DISTRIBUCIÓN	ALMACENAMIENTO	TRANSPORTE	DESTRUCCIÓN
		a personal externo a la SIC, se debe contar con una autorización formal (por ejemplo el caso de un derecho de petición).	Adicionalmente, como buena práctica se recomienda disponer de un circuito cerrado de video que brinde vigilancia al sitio donde se almacena la información (sala de almacenamiento).	NIST). Para su acceso debe solicitarse usuario y contraseña. Si es información física, esta debe transportarse en un sobre sellado y se debe llevar un registro de la hora de salida y la hora de entrega, al igual que los datos de la persona que realizó el transporte.	
Reservada	Rotular el activo con la etiqueta "Reservada"	Aplica lo mismo que en el nivel confidencial.	Aplica lo mismo que en el nivel confidencial.	Aplica lo mismo que en el nivel confidencial.	Aplica lo mismo que en el nivel confidencial.

4.4 Rotulación

4.4.1 Documentos Físicos

La rotulación se realizará mediante un sello donde se especifica el tipo de información que se está manejando, esto ayuda a que sea fácilmente identificable tanto por los funcionarios de la SIC como para los entes externos. Este sello se debe ubicar en la parte superior izquierda del documento a rotular. Una vez los documentos estén archivados y organizados en las carpetas de acuerdo a las series y sub - series de la tabla de Retención Documental, se deben clasificar tal como se haya relacionado en el inventario de Activos de la Información según su confidencialidad y utilizar el sello correspondiente. Todos los documentos físicos con un nivel de clasificación asignado deben ser rotulados, a excepción de aquellos documentos con el nivel de clasificación PÚBLICO los cuales no se rotularán.

Al utilizar el sello en cualquier documento físico, se debe especificar el tiempo de clasificación durante el cual se mantiene el nivel de clasificación asignado, por ejemplo si un archivo es clasificado como CONFIDENCIAL, se debe especificar cuanto tiempo tendrá ese nivel antes de pasar al inmediatamente inferior (ver Tabla 1. Niveles de Clasificación). Adicionalmente se debe indicar la fecha de

rotulación, el nombre del funcionario que esta asignando el nivel de clasificación y la dependencia a la cual pertenece. Los sellos a usarse con documentos físicos se ilustran a continuación:

USO INTERNO

Tiempo de Clasificación _____
Fecha de rotulación ___/___/____
Funcionario _____
Dependencia _____

CONFIDENCIAL

Tiempo de Clasificación _____
Fecha de rotulación ___/___/____
Funcionario _____
Dependencia _____

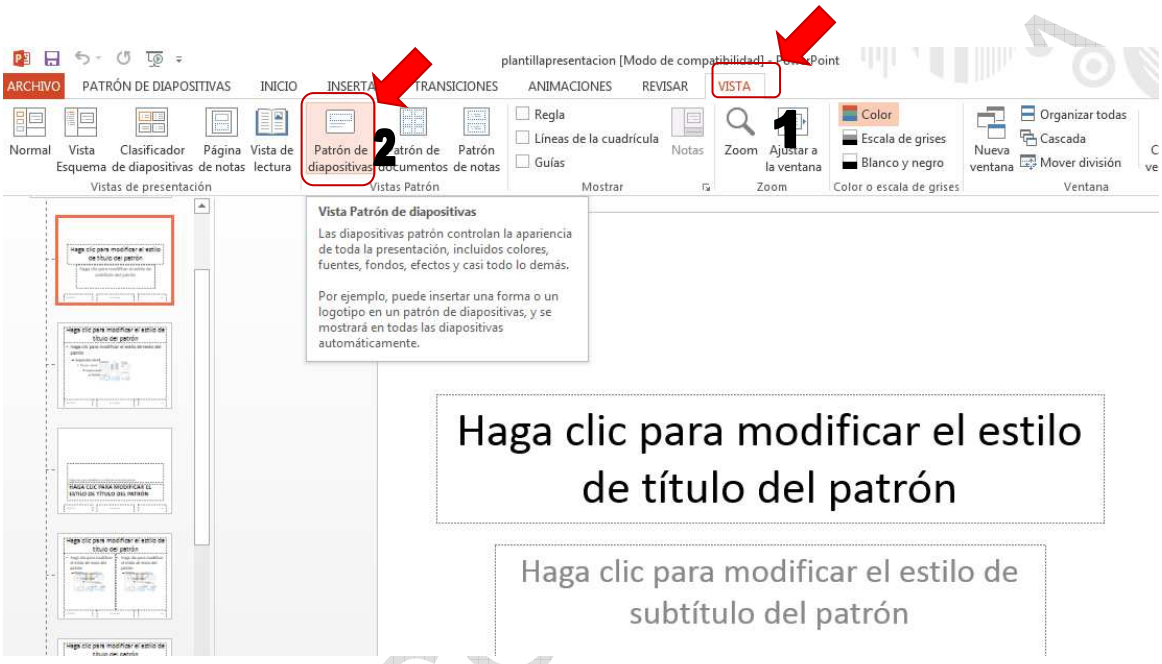
RESERVADO

Tiempo de Clasificación _____
Fecha de rotulación ___/___/____
Funcionario _____
Dependencia _____

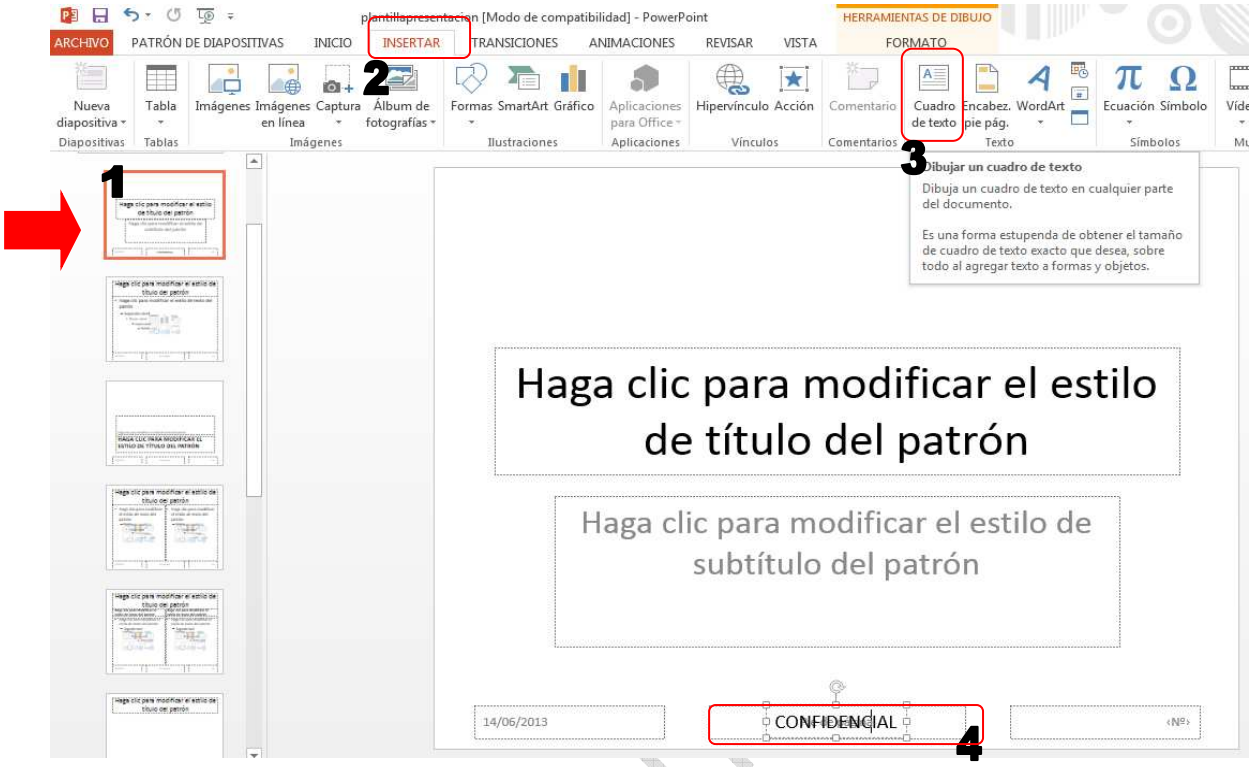
4.4.2 Información Digital

4.4.2.1 Power Point

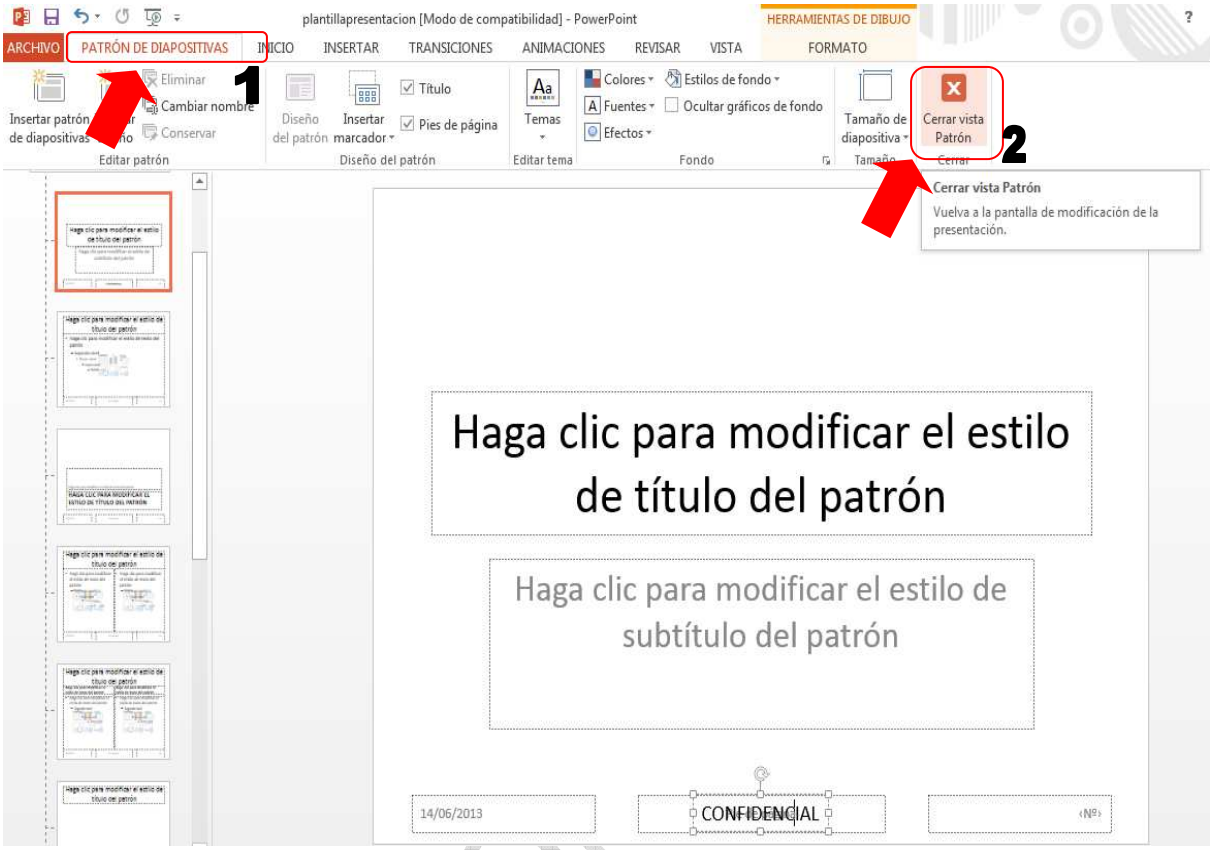
En la presentación a utilizar Ir al menú *vista* y seleccionar la opción "*Patrón de Diapositivas*"



Después de esto, seleccionar la primera diapositiva que se muestra en las miniaturas de la izquierda, luego hacer clic en el menú "INSERTAR" y seleccionar "insertar cuadro de texto", y escribir el nombre del nivel de clasificación centrado en la parte inferior de la diapositiva (sobre el recuadro que dice "pie de página"). Repetir lo mismo con la diapositiva No. 2.



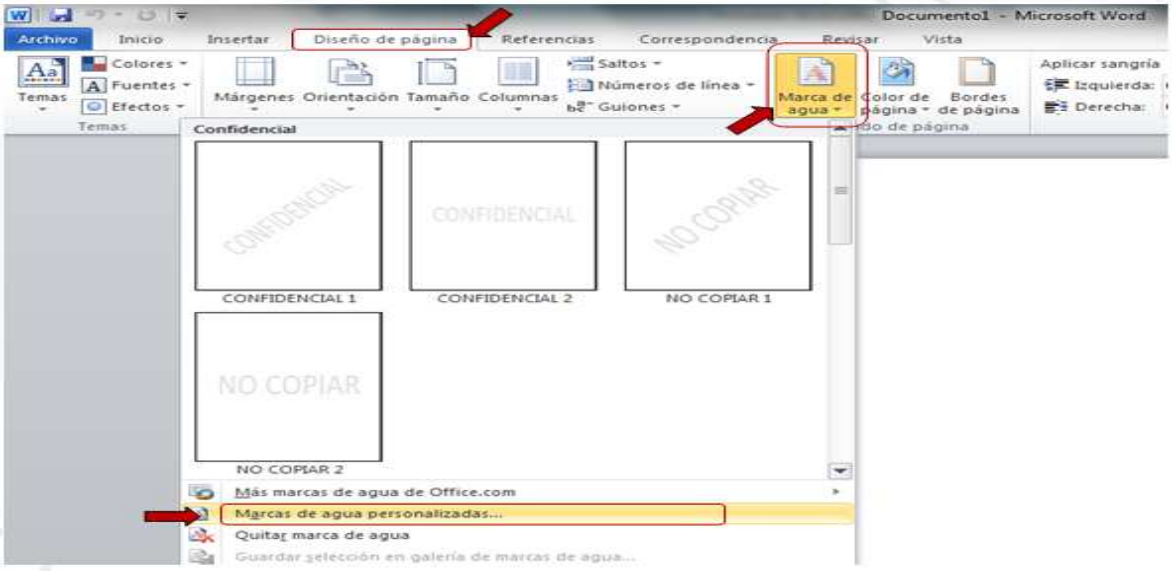
Después de esto hacer clic en el menú PATRON DE DIAPOSITIVAS y luego en Cerrar Vista Patrón.

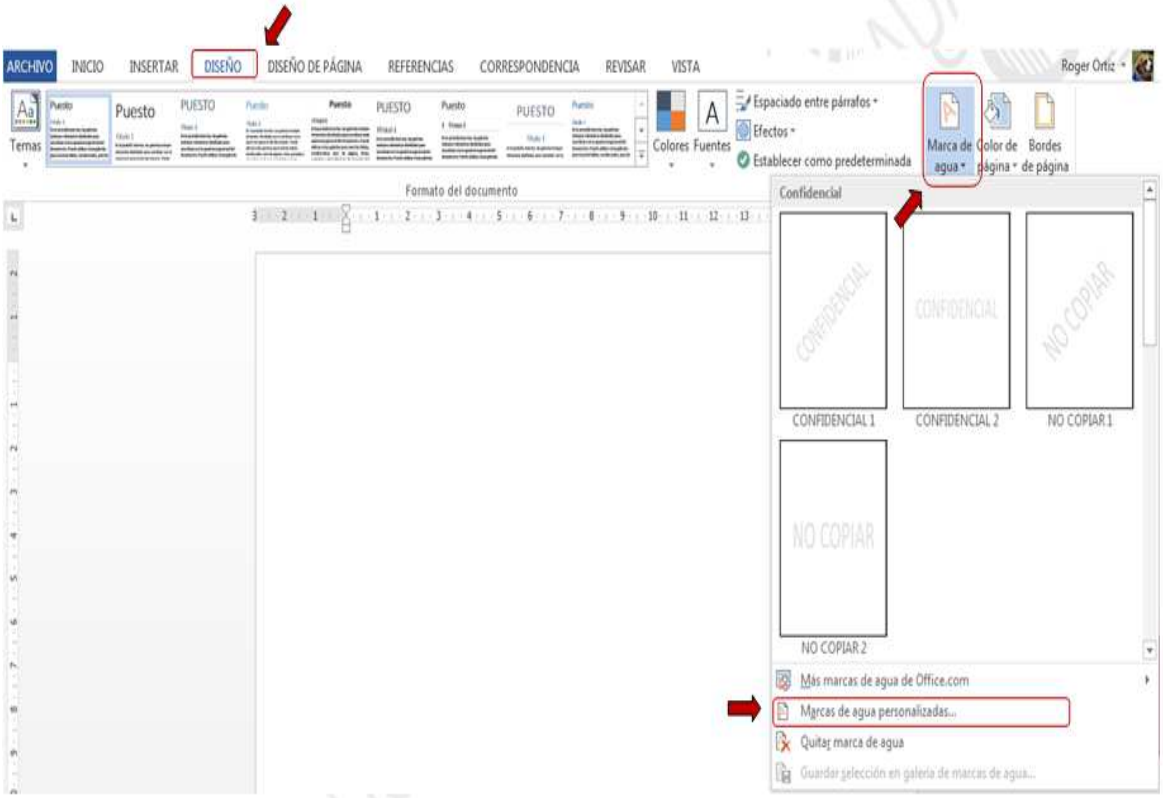


En caso de ser necesario, la persona que realiza la clasificación y rotulación de la información puede indicar el tiempo de clasificación asignado para cada nivel (Confidencial, Reservado, Uso interno), agregando un cuadro de texto en unidades de meses al lado derecho del nivel de clasificación.

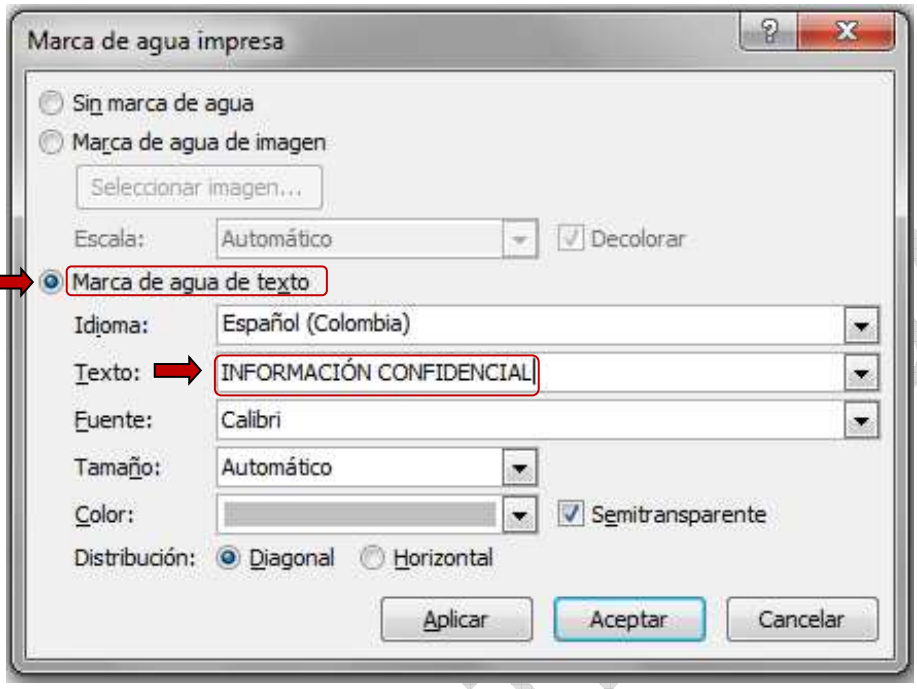
4.4.2.2 Word

En el menú "Diseño de Página en Word 2010" o en el menú "Diseño en Word 2013", seleccionar la opción "Marca de agua" y luego "Marcas de agua personalizadas", a continuación se muestra un ejemplo para Word 2010 y Word 2013 en este mismo orden.



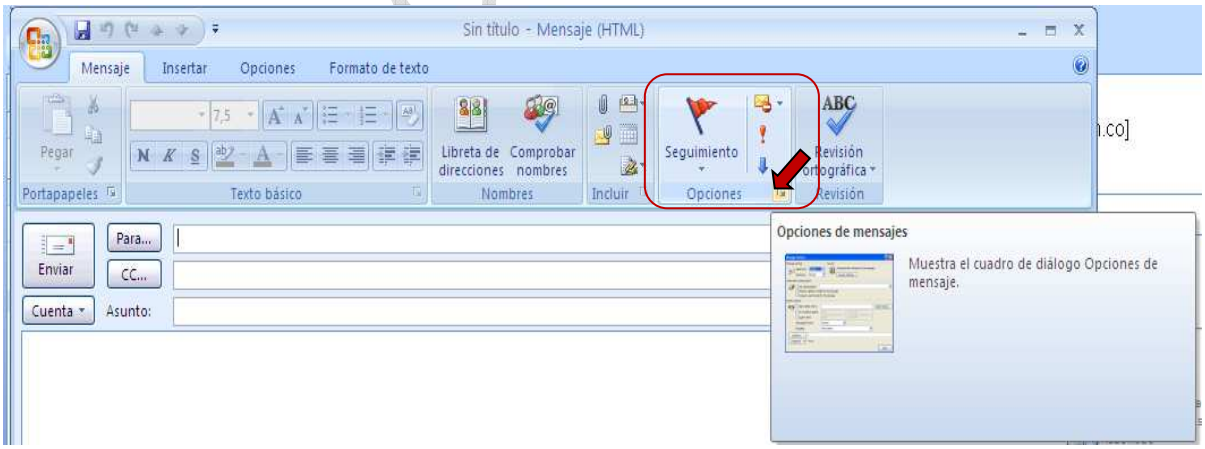


En la ventana que emerge (Marca de agua impresa) seleccionar la opción *Marca de agua de texto* y en el campo de *Texto* escribir Información Reservada, Información Confidencial, o Información de Uso Interno según corresponda y hacer clic en aplicar.

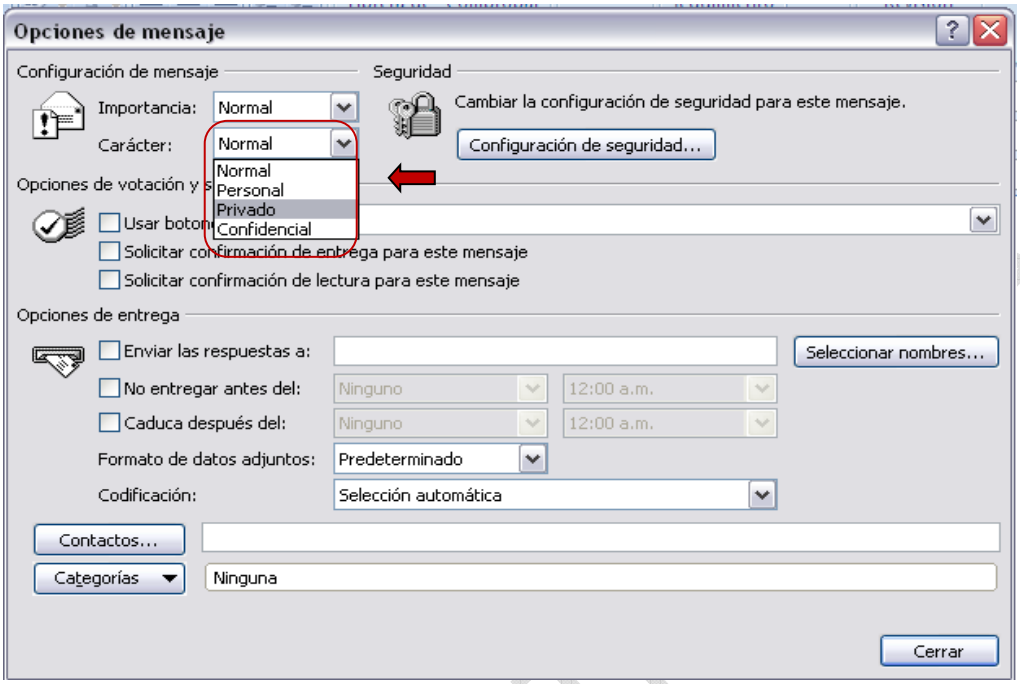


4.4.2.3 Outlook

En el menú "Mensajes", ítem "Opciones" en Outlook 2010 o ítem "Etiquetas" en Outlook 2013, hacer clic.

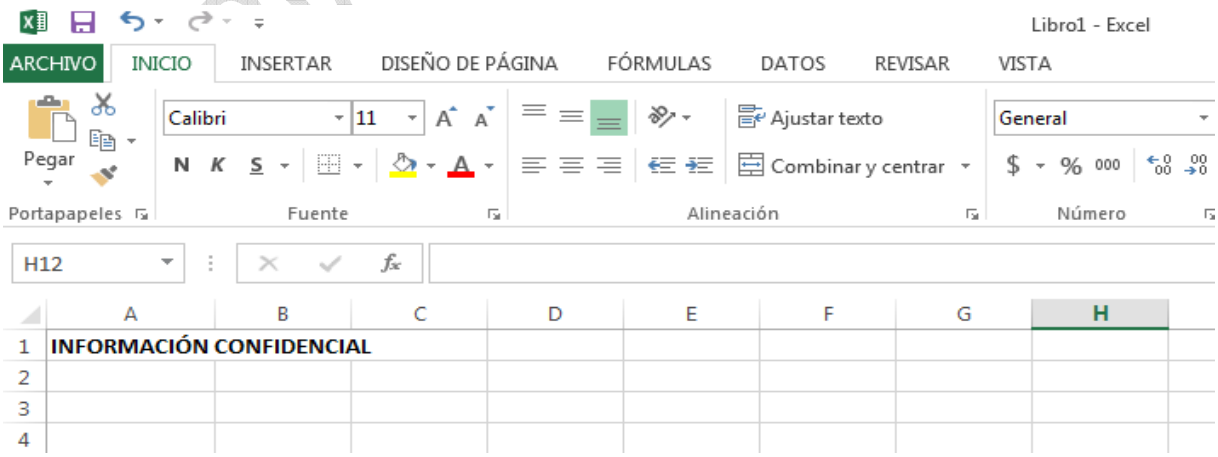


En el menú despegable "Opciones de mensajes" seleccionar la opción "Privado" si la información es Reservada o seleccionar la opción "Confidencial" si la información es Confidencial. Para correo electrónico NO SE MANEJARÁ el rotulo USO INTERNO.



4.4.2.4 Excel

En una celda ubicada en la parte superior izquierda se debe incluir el mensaje Información Reservada, Información Confidencial, o Información de Uso Interno según corresponda. En caso de ser necesario, la persona que realiza la clasificación y rotulación de la información puede indicar el tiempo de clasificación asignado para cada nivel (Confidencial, Reservado, Uso interno), agregando un cuadro de texto en unidades de meses al lado derecho del nivel de clasificación.



5 DOCUMENTOS RELACIONADOS

SC05-I01	Sistema de Gestión de Seguridad de la Información Política del SGSI.
GS01-P09	Procedimiento de Borrado Seguro de Información.

6 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se migra al proceso SC05 Gestión de la Seguridad de la Información, siendo el código documental anterior GS02-I02.

_____

Fin documento