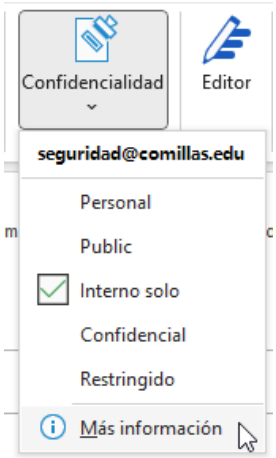
PR.005 - Política de Clasificación de las Informaciones

CONTROL DE REVISIONES

Versión	Fecha	Autor	Descripción
1.0	24/04/2025	Unidad Ciberseguridad	Documento inicial
1.1	01/09/2025	Unidad Ciberseguridad	Actualización de las clasificaciones

CONTENIDO



*Con el fin de utilizar el módulo de clasificación, **es necesario disponer de Office 365**, ya que el botón no está disponible en las versiones de Office 2019 o 2021.
Si necesitáis solicitar una actualización de Office, podéis hacerlo desde: Jira CAU.
La funcionalidad aparecerá en vuestros documentos y correos de manera automática.

Para comprobar la versión de Office, seguid estos pasos:

1. Abrir cualquier aplicación de Office (por ejemplo, Outlook, Word, Excel o PowerPoint).
2. Ir al menú **Archivo** en la esquina superior izquierda.
3. Hacer clic en **Cuenta** en la parte inferior del panel de la izquierda (o en **Ayuda**, dependiendo de vuestra versión).
4. En la sección **Información del producto**, podréis ver el nombre de vuestra versión de Office (por ejemplo, Microsoft 365, Office 2021, Office 2019, etc.)..

Funcionalidad adicional:

Para asignar una etiqueta a una carpeta completa sin necesidad de abrir cada archivo para seleccionar el nivel de confidencialidad, podéis instalar la extensión **Microsoft Purview Information Protection** desde el enlace de Microsoft.

1 OBJETIVO

El objetivo de esta política es establecer un marco para clasificar los datos en función de su sensibilidad, valor e importancia para la organización, de modo que los datos sensibles de la universidad y de los clientes puedan protegerse adecuadamente.

En función de la clasificación que se aplique a la información, es fundamental aplicar las medidas de seguridad adecuadas, como el cifrado y la identificación visual, para reducir los errores en el tratamiento de los datos.

Esta política describe la clasificación de la información electrónica, las medidas de seguridad y las responsabilidades para asegurar la información universitaria, evitando su destrucción (disponibilidad), modificación (integridad), divulgación (confidencialidad), uso no autorizado y acceso (confidencialidad). También sirve como punto de referencia para la clasificación de la seguridad de la información con respecto a otros reglamentos, métodos, normas, reglamentos escolares y reglamentos en las sedes de la Universidad Pontificia Comillas.

2 ÁMBITO DE APLICACIÓN

Esta política se aplica a todas las formas de datos, incluidos los documentos en papel y los datos digitales almacenados en cualquier tipo de soporte. Se aplica a todos los empleados de la universidad, así como a los agentes de terceros autorizados a acceder a los datos.

3 FUNCIONES Y RESPONSABILIDADES

El responsable de los Datos:

El responsable de los datos, de la información recogida y del seguimiento de los datos es el productor de información, apoyado por su manager. El propietario de los datos debe realizar las siguientes tareas:

- **Revisar y categorizar** - Revisar y categorizar los datos y la información recogida por su departamento o división. Asignación de etiquetas de clasificación según el impacto potencial de los datos.
- **Compilación de datos** - Garantizar que los datos compilados a partir de múltiples fuentes se clasifican como mínimo al nivel más seguro de clasificación de cualquier dato clasificado individualmente.
- **Coordinación de la clasificación de datos** - Garantizar que los datos compartidos entre los departamentos estén sistemáticamente clasificados **y protegidos**.
- **Cumplimiento de la clasificación de datos** - Comprobar la protección de la información de impacto alto y moderado de acuerdo con las normativas y directrices nacionales.
- **Protección** - Aplique el cifrado y derechos de acceso limitados necesario para que los datos sólo sean accesibles a las personas seleccionadas.

Rol del productor de información

El productor de una información utilizará el sistema de referencia existente para proponer el nivel de clasificación de dicha información. Si considera que el nivel indicado en el sistema de referencia no se aplica a la información que acaba de producir, puede apartarse de él de acuerdo con el proceso existente en su departamento.

Si el productor de los datos encuentra dificultades para identificar el nivel de clasificación de una información, puede recurrir a su línea de gestión o pedir consejo a la unidad de Ciberseguridad.

El productor de una información es responsable del seguimiento de la clasificación de dicha información. Si

Si la información se produce en el marco de un proyecto, los productores de la información y el director del proyecto serán corresponsables del control de la clasificación de la información. Siempre que sea posible, deberá indicarse la duración de la clasificación de la información. Deberá indicarse la duración de la clasificación de la información.

La persona responsable de supervisar la clasificación de un elemento de información es responsable de supervisar y desarrollar la clasificación de dicho elemento de información a lo largo de toda su vida.

La persona responsable de supervisar la clasificación de un elemento de información es responsable de supervisar y evolucionar la clasificación de dicho elemento de información a lo largo de su ciclo de vida de acuerdo con el proceso de la unidad.

Si el responsable del seguimiento de la clasificación de un elemento de información cambia de función, abandona su departamento o la universidad, corresponde a su jerarquía designar a un nuevo responsable de ese elemento de información.

Si los datos contienen datos personales y éstos ya no son indispensables para el tratamiento, los documentos deben ser anonimizados no permitiendo el cruce de información entre datos que puedan identificar a una persona.

Si el departamento desaparece, el responsable de la oficina o dirección a la que pertenecía se convierte en el nuevo responsable de la información.

El director de la oficina que es responsable en última instancia de los datos y la información recopilados y conservados por su departamento o división en los recursos de la universidad.

Rol del destinatario de la información

El destinatario de la información debe ser informado de las normas que debe seguir para garantizar la protección de la información que se le confía. información que se le ha confiado. En particular, los intercambios de información con terceros en el marco de una relación contractual o de asociación relación contractual o de asociación deben estar sujetos a cláusulas de seguridad para definir los requisitos que deben el nivel de clasificación de la información recibida; estas cláusulas garantizan una protección adecuada de la protección de la información por parte de su destinatario.

El destinatario de una información podrá decidir, si la necesidad lo justifica, retransmitir una información recibida, en cumplimiento de los compromisos a los que esté sujeto, aplicando el principio de "necesidad de conocer" y a condición de que respete las medidas de protección aplicables en razón de la clasificación de esta información y de las menciones específicas que puedan estar asociadas.

Para la información de nivel CONFIDENCIAL, destinada a una población nominalmente identificada, el destinatario deberá informar al emisor de la información en caso de difusión más allá del perímetro indicado por el aviso.

Para la información de nivel RESTRINGIDO, destinada a una población nominalmente identificada, el

destinatario deberá obtener previamente el acuerdo escrito del emisor de la información en caso de que sea necesario difundirla más allá del perímetro indicado por la declaración.

El hecho de que el emisor de una información no haya mencionado su carácter sensible no significa que el destinatario, que está sujeto a la obligación de discreción y debe respetar el principio de "necesidad de conocer", pueda difundirla. También puede preguntar al remitente de la información sobre las precauciones que debe tomar con respecto a la información que ha recibido de él. En particular, la difusión pública de la información debe ser el resultado de un proceso voluntario y controlado.

Cada persona sólo debe poseer la información necesaria para su actividad. En caso de cambio de puesto o de salida de la universidad, el usuario debe procurar borrar o destruir todas las copias de la información que posea y que ya no necesite disponer.

4 PROCEDIMIENTO DE CLASIFICACIÓN DE DATOS

El proceso de clasificación de la información se aplica a todas las versiones de un documento, incluidas las versiones en elaboración.

El propietario de los datos asigna una etiqueta de clasificación a cada dato en función del nivel de impacto global por la Universidad:

Nivel de impacto	**Nivel de clasificación**
Critico (~1% de los datos)	*Restringido*
Alta	*Confidencial*
Moderado	*Interno Solo*
Bajo	*Público*
Zero	*Personal*

El propietario de los datos registra la etiqueta de clasificación y el nivel de impacto global de cada dato en la tabla oficial de clasificación de datos, ya sea en una base de datos o en papel.

Los custodios de los datos aplicarán los controles de seguridad adecuados para proteger cada dato según la etiqueta de clasificación y el nivel de impacto global registrados en el cuadro oficial de clasificación de datos.

La sensibilidad de un documento evoluciona con el tiempo, muy generalmente hacia una reducción de las necesidades de confidencialidad. Por ejemplo, una vez patentada, una invención ya no necesita ser confidencial. Cualquier documento acaban convirtiéndose en un archivo de clasificación interna o desaparecen.

Siempre que sea posible, debe indicarse en el documento la fecha o el acontecimiento a partir del cual puede revisarse el nivel de clasificación. Si no se especifica la duración de la clasificación, el nivel de clasificación se modifica a la baja cada 2 años.

5 NORMAS ESTABLECIDAS

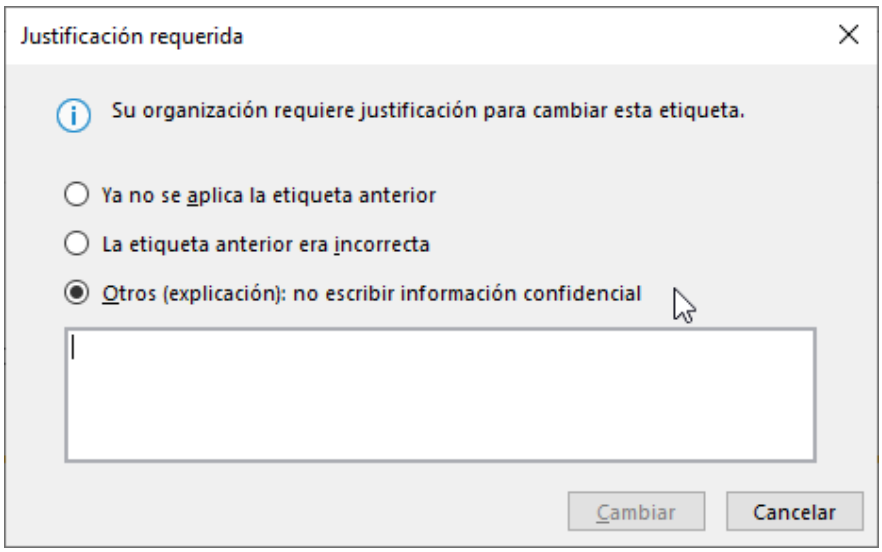
Medidas de seguridad relacionadas con las clasificaciones:

Nivel de clasificación	Medidas relacionadas
Restringido (Secreto)	**Cifrado automatico del documento o del email** Marcado que la información está al nivel "Restringido" en la parte superior y abajo del email en color Rojo oscuro. **No se comparte con grupos; No se reenvia.**
Confidencial - Cifrado	**Cifrado automatico del documento o del email.** Marcado que la información está al nivel "Confidencial" en la parte superior del email en color Rojo
Confidencial - Básico	Clasificación seleccionada por defecto. Sin marcado visible en los documentos ni en los correos. **Sin uso de protección mediante encriptación.**
Interno solo	Marcado que la información contenida es "sólo para uso interno" en la parte superior del email en color Azul.
Público	Simple marca que la información es "Pública" en la parte superior del email en color Verde.
Personal	Marca que la información es "Personal" en la parte superior del email en color Negro.

- Los usuarios tendrán que aplicar etiquetas para poder guardar documentos, enviar correos y crear grupos o sitios (siempre que estos elementos no tengan ya una etiqueta aplicada).
  La compatibilidad y el comportamiento de esta configuración varían según las aplicaciones y las plataformas.

- También, es posible enviar un correo electrónico a un interlocutor externo utilizando la clasificación "Confidencial", el correo electrónico se enviará utilizando un cifrado fuerte - El contacto podrá acceder al contenido iniciando sesión con su cuenta de Microsoft y, si es necesario, podrá solicitar un código único que recibirá por correo electrónico para acceder al contenido.

- El enlace de la página web dedicada a la seguridad informática está disponible en la herramienta de privacidad desplegada para los usuarios: https://ciberseguridad.comillas.edu/
  También se incluye un artículo sobre clasificación de datos.
- Los usuarios deberán justificar la eliminación de una etiqueta o su sustitución por otra con un número de orden inferior. Puede utilizar el Explorador de Actividades para revisar los cambios en las etiquetas y el texto de justificación.



Sin la acción del creador de datos, los estados de confidencialidad se aplican por defecto en las herramientas de Microsoft.

Etiqueta configurada por defecto **para los documentos:**

- Confidencial - Básico

Los usuarios están obligados a aplicar un estado de confidencialidad a sus correos electrónicos.

Etiqueta configurada por defecto **para los emails:**

- Confidencial - Básico

Etiquetas configuradas por defecto **para el contenido de Power BI:**

- Sólo para uso interno

6 INSTRUCCIONES DE SEGURIDAD

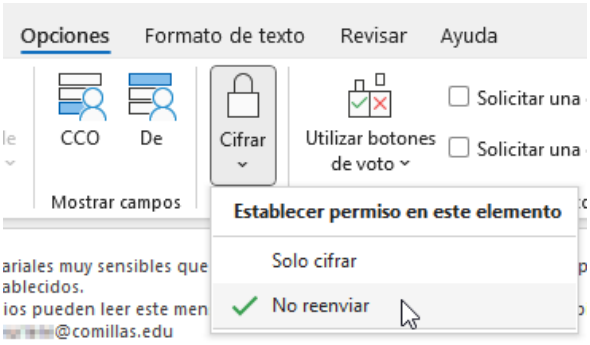
Las normas de seguridad se aplican tanto a los documentos institucionales digitales como a los de papel, según sean altamente confidenciales, confidenciales o no confidenciales.

Restringido:

Estos documentos contienen información personal sensible o de alto valor estratégico para la Universidad Pontificia Comillas.

- ✓ Almacenar **siempre en un servidor cifrado** o/y en un archivo 7zip cifrado.
- ✓ Si ya está impreso, destruya el documento con una máquina específica.
- ✗ Antes de compartir el documento en OneDrive, Teams u otras ubicaciones comprobar quién tiene acceso.
- ✗ No utilices mensajería instantánea ni redes sociales para compartir los datos.
- ✗ No imprimir este tipo de contenido.
- ✗ Cada destinatario de la información debe ser seleccionado manualmente.
- ✗ **No está permitida la transferencia de información sin el acuerdo del propietario de los datos.**

Cuando se utiliza la clasificación “Restringido”, se recomienda seleccionar la opción "No reenviar" para evitar transferencias erróneas y, por tanto, la fuga de información.



Ejemplos de documentos con fines de difusión Restringidos:

Documentos que contienen información personal sensible.

- ➢ Documentos relativos a la salud física y mental de una persona (estudiante, empleado, profesor, paciente u otro)
- ➢ Expediente de paciente de clínica médica, expediente de estudiante con información sanitaria, expediente de estudiante discapacitado, evaluación de salud o de aptitud física, documentos de permiso de maternidad, etc.

Documentos relativos a la situación financiera de una persona (estudiante, empleado, paciente u otro).

- Solicitud de ayuda financiera, expediente del becario, salario del empleado, profesor, etc...

Documentos relativos a las investigaciones en curso

- Casos de plagio, casos de disputa, quejas al defensor del pueblo, quejas de acoso, casos disciplinarios, solicitudes a los servicios jurídicos, quejas, medidas disciplinarias, etc.

Otros datos personales sensibles

- Número de la seguridad social, fecha de nacimiento, certificado de nacimiento, documento de inmigración, expediente de admisión, expediente de empleado, solicitud de honorarios profesionales que contengan un número de la seguridad social, DNI, Pasaporte, etc.

Documentos de alto valor estratégico para la Universidad Pontificia Comillas.

- Negociación de acuerdos con otras instituciones, negociación de convenios colectivos, campaña de captación de estudiantes, contrato de afiliación o investigación, desarrollo del campus, estrategia de recaudación de fondos, presentación de patentes, protocolo de investigación, etc.

Confidencial - Cifrado:

- ✓ Almacenar **siempre en un servidor cifrado** o en un archivo 7zip cifrado.
- ✓ Los documentos se pueden almacenar en una carpeta privada de OneDrive.
- ✓ Almacenamiento de papel: marcados como Confidencial, archivadores y locales cerrados con llave.
- ✓ Puede utilizarse para intercambios con un contacto externo.
- ✓ Para todos los envíos de correo interno y externo, utilice sobres cerrados.
- ✓ Si está impreso, destruya el documento con una máquina específica.
- ✗ No está permitida la transferencia de información sin informar del propietario de los datos. Sólo deben tener acceso a la información quienes necesiten conocerla.

Ejemplos de documentos con fines de difusión Confidencial:

Documentos que contienen información personal no sensible.

- Documentos relativos a los antecedentes académicos del estudiante
- Trabajos y exámenes terminados, lista de resultados académicos, expedientes académicos, registros de estudiantes que no contengan información sanitaria, etc.
- Datos "clásicos" de RRHH (expediente profesional, opinión de los gestores, bonificación, etc.)

Identificación de personas sin información personal sensible.

- Lista de inscripción a los cursos, lista de asignación de tareas docentes, lista de profesores y asistentes a la enseñanza, lista y datos de contacto de los invitados a un acto, documentos de registro y verificación del tiempo de los empleados (hojas de asistencia, tarjetas perforadas, hojas de asistencia, registro de asistencia), número de estudiante o empleado, dirección, número de teléfono, etc.

Documentos de valor estratégico para la Universidad Pontificia Comillas.

- Documentos relacionados con la gestión de los programas educativos ofrecidos por la universidad (creación, evaluación, modificación, supresión, administración), formularios de examen en blanco, normas aplicadas para negociar y establecer condiciones específicas para la contratación de nuevo personal, normas presupuestarias, documentos justificativos que no contengan información personal sensible, comprobantes de transferencia de documentos, etc.
- Informe de auditoría interna o externa (identificación de deficiencias técnicas, de seguridad o seguridad o debilidades organizativas, descripción de vulnerabilidades)
- Documentos sujetos a un acuerdo de confidencialidad (NDA) con otra institución.

Confidencial - Básico:

Los documentos clasificados como Confidencial – Básico contienen información que, aunque no requiere cifrado, **necesita una atención especial por parte de los usuarios** para evitar su divulgación accidental.

- ✓ Almacenamiento digital: pueden guardarse en carpetas personales de **OneDrive** o en repositorios internos autorizados, pero siempre evitando el almacenamiento en ubicaciones públicas o compartidas sin control de acceso.
- ✓ Almacenamiento físico: si están impresos, los documentos deben guardarse en archivadores o cajones cerrados.
- ✓ La información puede circular libremente dentro de la universidad.
- ✓ Si es necesario compartir esta información con terceros, se recomienda utilizar medios seguros, como los repositorios de la Universidad con control de acceso.
- ✓ Si se imprimen, deben destruirse posteriormente del uso con una máquina trituradora.
- ✓ Solo las personas con necesidad de conocer (“need to know”) deberían manejar estos documentos.
- ✗ No debe enviarse datos de la Universidad a contactos externos que no sean proveedores oficiales de la universidad o que no tengan un acuerdo de confidencialidad (NDA).
- ✗ No se debe utilizar para el envío de datos personales, tanto si permiten identificar directamente a una persona como si lo hacen de forma indirecta, y sean o no sensibles.

Esta clasificación suele ser el nivel de confidencialidad por defecto.

Ejemplos de documentos Confidencial – Básico:

- Informes internos que contienen datos agregados, anonimizados o pseudonimizados de estudiantes o empleados sin información personal sensible.
- Documentos de planificación interna de proyectos, con presupuestos preliminares no públicos.
- Listas de distribución interna que incluyen correos electrónicos, extensiones o cargos de personal.
- Procedimientos internos no destinados para difundir fuera de la Universidad.

Interno solo:

- ✓ Los documentos se pueden almacenar en una carpeta de OneDrive.
- ✓ Almacenamiento de papel: marcados como de uso interno y almacenados en un armario o cajón cerrado.
- ✓ Si está impreso, destruya el documento con una máquina específica.
- × No está permitida la transferencia de información “Interno solo” a un contacto externo a la universidad o sin NDA.

El documento y la información que contiene pueden circular libremente dentro de la universidad, pero no fuera.

Ejemplos de documentos con fines de difusión Interno solo:

Documentos relativos a la información y comunicación internas

- ➢ Actas de reuniones, boletines, documentos de enlace.

Cualquier información potencialmente sensible que no esté destinada a ser compartida con el público.

- ➢ Notas y actas de reuniones no confidenciales.
- ➢ Correspondencia variada con el personal y los profesores e información sobre los proyectos en curso.
- ➢ Listas de contactos internos y direcciones de correo electrónico.
- ➢ Estadísticas, listados e inventarios, reglamentos y políticas en desarrollo o revisión, calendarios de actividades, documentos relativos a la relación de la unidad con otras unidades universitarias descripciones de puestos y funciones, guías de formación, lista de cursos o eventos por locales, inventario de bienes, plantillas y formularios, etc..

Publico - No confidencial:

- ✓ Los documentos se pueden almacenar en una carpeta de OneDrive.

- ✓ Esta información no tiene ninguna restricción.
- ✓ Se reciclan los documentos públicos impresos.

Estos documentos no contienen información personal y no tienen valor estratégico para la Universidad Pontificia Comillas.

Ejemplos de documentos con fines de difusión Publico:

Se trata de información que puede ser divulgada a cualquier persona, independientemente de su afiliación a la universidad.

- ➢ Como comunicados de prensa, la información ya difundida por el departamento de comunicación, los catálogos de cursos y formación y los procedimientos de solicitud.

Personal - No confidencial:

Se trata de datos personales del usuario, no relacionados con su actividad o interacciones con la universidad, y por tanto destinados a permanecer privados.

Conviene recordar que, según el buen uso de los recursos digitales, el uso privado de los recursos digitales se tolera si es mínimo en términos de tiempo y frecuencia, implica un uso insignificante de los recursos, no compromete ni obstaculiza la actividad profesional ni la de la organización, y no es ilícito ni contrario al decoro o la decencia.

Anexo: A continuación, se presenta un resumen de las clasificaciones de información, junto con una descripción sintética y ejemplos asociados.

Sensibilidad	Descripción	Ejemplos
Publico	Información de carácter general y accesible para todos. Su difusión ha sido autorizada por su propietario y su divulgación no es susceptible de causar daño a ninguna persona ni a la Universidad.	❖ Los folletos de la universidad ❖ Documentos sobre la formación y los servicios ofrecidos por la Universidad ❖ Sitio web de la Universidad ❖ Información general que ya es de dominio público ❖ Resultados financieros publicados en los informes anuales ❖ Documentos clasificados como públicos por el servicio de comunicación
Interno	Información que no es accesible a partes externas de la Universidad, y que se considera disponible sólo para los empleados. La divulgación de información interna puede perjudicar a la Universidad, pero no afectar gravemente a sus actividades.	❖ Directorio telefónico interno ❖ Sitio Intranet y documentación ❖ Documentos a disposición de los empleados, como las actas no confidenciales de las reuniones
Confidencial - Básico	Información interna que no contiene datos personales ni sensibles y cuya divulgación no autorizada tendría un impacto moderado en la Universidad. No requiere cifrado por defecto, pero sí almacenamiento en repositorios corporativos con control de acceso y compartición solo bajo el principio de necesidad de conocer.	❖ Informes internos con datos agregados/anonimizados o pseudonimizados sin datos sensibles. ❖ Documentación y presupuestos preliminares de proyectos no publicados. ❖ Listas de distribución internas ❖ Procedimientos internos no destinados a difusión externa. ❖ Borradores sin información sensible pendientes de validación.
Confidencial - Cifrado	Información accesible a un grupo limitado de personas que necesitan conocerla en el ejercicio de sus funciones. Su divulgación podría causar un perjuicio importante o ser contraria a una obligación contractual o reglamentaria.	❖ Datos personales ❖ Sueldos y prestaciones de los empleados ❖ Datos financieros ❖ Información detallada sobre estudiantes y proveedores ❖ Actas de reuniones ❖ Datos de seguridad ❖ Informes de auditoría
Restringido (Secreto)	Información que debe protegerse con el mayor nivel de seguridad posible y que suele estar sujeta a requisitos contractuales o normativos. Por definición, este tipo de información está destinada a ser conocida por un número muy limitado de personas. Su divulgación puede causar un daño significativo a la Universidad, a sus estudiantes, o tener consecuencias para sus operaciones, rendimiento financiero, reputación o cumplimiento de la normativa.	❖ Contraseñas ❖ Datos personales ❖ Certificados digitales ❖ Claves de cifrado ❖ Información de carácter estratégico ❖ Información que pueda perjudicar la reputación de la Universidad ❖ Informes que necesitan un nivel muy alto de secreto