Clasificación de la información de terceros y Especificación para el tratamiento

Introducción

No toda la información tiene el mismo valor o nivel de sensibilidad. Por eso, clasificarla nos ayuda a saber de qué forma se debería proteger, demuestra nuestro compromiso con esa protección y nos ayuda a tratarla de forma eficiente.

Tenemos cuatro niveles de clasificación:

- Pública
- Interna
- Confidencial
- Estrictamente confidencial

La tabla siguiente ofrece orientación sobre los tipos de información que se incluirán en cada una de estas cuatro categorías.

Por defecto, cualquier información de BT se clasificará como Confidencial salvo que se indique otra cosa.

Si no está seguro de en qué categoría se incluye la información, consulte con su Contacto de Seguridad de BT.

Clasificación	Descripción general	Ejemplos
Pública - Cat. 1	La información pública es información que está disponible para las personas, internas o externas a BT.	• Campañas publicitarias. • Comunicaciones genéricas ya de dominio público (por ej. declaraciones en notas de prensa, artículos públicos sobre BT) • Información comercial de dominio público como precios publicados u ofertas
Interna - Cat. 2	Información de BT que está disponible para el personal de BT y otras personas que tengan acceso a la red de información de BT; el acceso a ella supone un riesgo empresarial mínimo para BT. La información interna puede incluir información sujeta a obligaciones de confidencialidad de carácter general (por ej. mensajes e-mail empresariales habituales, informes o documentos contractuales), siempre y cuando esa información no sea lo suficientemente sensible desde el punto de vista comercial como para requerir una mayor protección tal y como se describe a continuación.	• Boletines de noticias internos como BT News • Artículos FixIt • Mensajes de e-mail generales no sensibles (por ej. información no comercial o datos personales restringidos, como se detalla en la columna izquierda, contenidos en el cuerpo de un mensaje de e-mail)
Confidencial - Cat. 3	La información Confidencial es información que debería limitarse a un público específico y que si se divulgara sin autorización, podría dañar la reputación de BT, o su divulgación resultaría potencialmente perjudicial para las personas a las que se refiere la información (por ejemplo, mayoría de datos personales sobre empleados o clientes). En la información	• Datos de registro del sistema; • Datos de ventas y marketing sensibles a nivel comercial; • Planes comerciales locales; • Mayoría de datos personales; y • Datos de riesgo. • Todos los datos personales (como se definen en la condición titulada

	Confidencial, se debería aplicar el principio de 'necesidad de conocer'. **Recopilación de múltiples documentos de información Confidencial** Si tiene una recopilación de documentos de información "Confidencial" en un lugar, la clasificación podría aumentar un nivel, pudiendo desembocar en la reclasificación de los documentos individuales como "Estrictamente confidencial" o incluso requerir medidas de seguridad adicionales para proteger la ubicación si: • Juntos pudieran causar un daño excepcional a BT en caso de que se filtraran; o • Si se utilizaran con otras combinaciones de datos, pudieran ser un objetivo atractivo.	"**Protección de la información"**), salvo que estén clasificados como Estrictamente confidencial, como se indica a continuación.
Estrictamente confidencial - Cat. 4	La información o datos 'Estrictamente confidencial' circula de forma definida y reducida; se ejecuta de manera estricta el principio de "necesidad de conocer" (debe saber quién tiene copias y quién tiene acceso). La divulgación no autorizada podría provocar un daño excepcional a BT. Debería considerar cuidadosamente si la información es 'Estrictamente confidencial', porque requiere los controles de seguridad más exhaustivos.	• Detalles de cuentas bancarias • Los detalles de autenticación se deberían tratar como 'Estrictamente confidencial'. • Contraseñas informáticas, contraseñas en general, se deberían guardar y proteger de conformidad con las Especificaciones de Criptografía de BT • Los datos contables y financieros reservados hasta la publicación del informe anual • Planes empresariales estratégicos, estrategia competitiva, nuevos productos estratégicos y nuevas políticas de marketing • Evaluaciones altamente sensibles de la competencia, socios o contratistas • Información de RR.HH. sensible que puede alienar a un número significativo de empleados • Detalles de adquisiciones importantes, alianzas, planes de desinversión y fusiones • Detalles sobre puntos vulnerables significativos de la red • Códigos de seguridad de clientes, códigos de encriptación maestros, cálculos clave, datos de transacciones, cuentas o auditorías, códigos de seguridad de clientes, códigos de encriptación maestros, cálculos clave, datos de transacciones, cuentas o auditorías • Informes de auditoría o conclusiones que contengan detalles de deficiencias/puntos vulnerables graves en las prácticas o procesos de BT

¿Cómo he de tratar los datos?

La información debe tratarse según el nivel de clasificación para que esté debidamente protegida, ya sea en un ordenador, a través de la red, ya sea escrita o hablada.

Tenemos unas normas para el tratamiento de datos e información.

- **Hablada y multimedia** por ejemplo, hablar, redes sociales, mensajes de texto, Skype
- **Documentos en papel,** por ejemplo, impresiones, publicaciones, eliminación
- **Documentos electrónicos,** por ejemplo, guardar, enviar por e-mail, transferir, eliminar
- **En aplicaciones o sistemas,** por ejemplo, centros de datos

Asimismo, disponemos de ciertas directrices independientes sobre el nivel y el tipo de encriptación que esperamos que se usen para proteger la información (nuestro "Estándar de Encriptación").

Tratamiento de datos hablados y multimedia

Ref.	¿Qué quiere hacer?	Clasificación	Requisitos de tratamiento	Motivo
HSM10	Quiero publicar información en las redes sociales/sitios de redes sociales, por ejemplo, una cuenta personal de Twitter	Pública	No debe participar en sitios ni publicar afirmaciones online que pudieran atribuirse de forma razonable como opiniones de BT o sean difamatorias para BT y puedan provocar un daño a la marca y reputación de BT.	La publicación no autorizada de información o los comentarios personales podrían dañar nuestra marca
		Interna	No permitido	
		Confidencial	No permitido	
		Estrictamente confidencial	No permitido	
HSM20	Quiero hablar o presentar algo a través de una conferencia o mensaje interno	Interna	Puede utilizar Live Meeting, WebEx, Webjoin y Lync/Skype for Business	Los datos internos los pueden ver las personas invitadas a la reunión
		Confidencial	Puede utilizar Live Meeting, WebEx, Webjoin y Lync/Skype for Business	Los datos Confidenciales los pueden ver las personas invitadas a la reunión
		Estrictamente confidencial	• Puede utilizar Lync/Skype for Business alojado de BT • Debe comprobar quién participa en la conferencia • Debe bloquear la reunión por conferencia para que nadie se pueda incorporar a la misma	Lync/Skype for Business encriptan según los datos del Estándar de Encriptación indicados más adelante.
HSM30	Quiero hablar de algo a través de un chat en directo externo, por ejemplo, en el sitio de soporte de un distribuidor como Cisco	Pública	Las conversaciones se deben limitar a la 'información pública' que esté disponible en nuestro sitio web	Evitar la divulgación no autorizada de información
		Interna	No permitido	
		Confidencial	No permitido	
		Estrictamente confidencial	No permitido	
HSM40	Quiero hablar de algo cara a cara/en una conversación telefónica	Interna	Asegúrese de que nadie que no trabaje para o en representación de BT pueda escuchar la conversación	Evitar la divulgación no autorizada de información
		Confidencial	Como 'Interna' y • Compruebe la identidad de la persona con la que está hablando y confirme que tiene 'necesidad de conocer' antes de	Proteger la información confidencial y asegurar que se limite a aquellas personas que necesiten conocerla

			hablar de cualquier cosa confidencial • Verificar que existe un contrato con terceros pertinentes antes de iniciar la conversación si procede (NOTA: Antes de ceder o subcontratar una parte o la totalidad del contrato a un tercero, debe obtener el consentimiento previo por escrito de BT) • Verificar que nadie pueda escuchar la conversación • No deje información 'Confidencial' en los sistemas de buzones de voz	
		Estrictamente confidencial	Como 'Confidencial' y • Mantenga cualquier información 'Estrictamente confidencial' al mínimo absoluto	
HSM50	Quiero enviar un mensaje/contenido por SMS/MMS a todas las partes (internas y externas)	Pública	El contenido de los mensajes se debe limitar a la 'información pública' disponible en nuestro sitio web	Evitar la divulgación no autorizada de información
		Interna	Ningún requisito especial de tratamiento	
		Confidencial	Verificar que el mensaje solo se envíe a aquellas personas que deban conocerlo. Lo siguiente no se debe divulgar: • Datos de tarjetas de pago • Datos bancarios • Datos de contraseñas	Estos tres elementos son Estrictamente confidenciales
		Estrictamente confidencial	No permitido	

Tratamiento de documentos en papel

Ref.	¿Qué quiere hacer?	Clasificación	Requisitos de tratamiento	Motivo
HPD10	Quiero trabajar con información en papel en las instalaciones de un tercero o en casa	Interna	Debe aplicarse la política de mesa despejada cuando no se esté trabajando en ella	Evitar la divulgación accidental
		Confidencial	Como 'Interna' y • Cuando no se esté trabajando con los documentos, retirar de la vista y guardar bajo llave.	
		Estrictamente confidencial	Como 'Confidencial'	
HPD20	Quiero imprimir	Interna	• Comprobar que se envía a la impresora correcta • No dejar documentos en la bandeja de impresión	Evitar la divulgación accidental
		Confidencial	Como 'Interna' y	

			• Usar una impresora con acceso controlado, una impresora conectada a un PC o una impresora en una sala con acceso controlado	
		Estrictamente confidencial	Como 'Confidencial'	
HPD30	Quiero utilizar una impresora que no está ni en el edificio de un proveedor ni en mi casa (por ej. está en las instalaciones de un tercero, un hotel, etc.)	Interna	Normalmente, esto no está permitido, porque las impresoras pueden tener memoria y se pueden recuperar los datos. Use su sentido común: ¿realmente quiere que otras personas vean esta información?	Se pueden recuperar los datos y la información de la memoria de una impresora
		Confidencial	No permitido	
		Estrictamente confidencial	No permitido	
HPD40	Quiero llevar información en papel fuera de mi lugar de trabajo	Interna	Llevar en una carpeta o bolso opacos	Protegerla de la divulgación accidental
		Confidencial	Como 'Interna' y • No debe sacar datos de los clientes y/o pagos de las oficinas del proveedor	
		Estrictamente confidencial	Como 'Confidencial'	
HPD50	Quiero compartir o enviar información en papel a otras partes internas	Interna	• Introducir en un sobre y usar el correo interno.	Protege de la observación casual
		Confidencial	• No escribir 'Confidencial' en el sobre externo. • Si la información está cubierta por 'privilegios legales', recurrir al departamento jurídico para que le asesoren.	Evita que observadores casuales se den cuenta de que el contenido es 'Confidencial'. Firmado para entrega proporciona una prueba del envío, la firma a la entrega y la confirmación online de la entrega del artículo
		Estrictamente confidencial	• Usar dos sobres y enviar a través de una entrega 'con seguimiento' • No indicar en el sobre externo 'Estrictamente confidencial' • Conseguir el permiso del titular del documento para compartir la versión en papel • Compartir preferiblemente en mano con personas autorizadas identificadas • Vincular las copias con las personas con marcas de agua con un nombre o un número (si es posible) • Si se pierde, informar como incidente de seguridad	Evita que observadores casuales se den cuenta de que el contenido es 'Estrictamente confidencial'. Firmado para entrega proporciona una prueba del envío, la firma a la entrega y la confirmación online de la entrega del artículo
HPD60	Quiero compartir o enviar información en papel a personas externas	Interna Confidencial Estrictamente confidencial	Comprobar que se dispone de un contrato según HSM40 con los terceros pertinentes. Los controles son los mismos que para compartir con	Ver HPD50

			personas internas	
HPD70	Quiero enviar un fax	Interna	Asegurarse de incluir una carátula de fax antes de las páginas con el contenido	Evitar la divulgación accidental
		Confidencial	• Debe enviar una carátula de fax con una página de prueba y después contactar con el destinatario para confirmar su recepción antes de enviar por fax el contenido • Si la información está cubierta por 'privilegios legales', acuda al departamento jurídico para que le asesoren	Evitar que personas no autorizadas reciban la información
		Estrictamente confidencial	No permitido	
HPD80	Quiero eliminar información en papel	Interna	Debe • triturarla o • colocarla en una papelera de documentos que no se puedan sacar fácilmente	Los contenedores generales y/o los de reciclaje no son formas seguras de eliminación
		Confidencial	Triturar hasta un tamaño de partículas mínimo de ≤ 160MM² y un ancho de tiras de partículas regular de ≤ 2MM, por ej. 2 X 15 mm.	Proteger información 'Confidencial' de la divulgación
		Estrictamente confidencial	Triturar hasta un tamaño de partículas mínimo de ≤ 160MM² y un ancho de tiras de partículas regular de ≤ 2MM, por ej. 2 X 15 mm, con una trituradora de corte transversal	Proteger información 'Estrictamente confidencial' de la divulgación

Tratamiento de documentos electrónicos

Ref.	¿Qué quiere hacer?	Clasificación	Requisitos de tratamiento	Motivo
HED10	Quiero guardar información electrónica en mi portátil/PC de la empresa	Interna	Se utiliza la encriptación total del disco, de acuerdo con el Estándar de Encriptación indicado más adelante.	Esto convierte la información en código ilegible que no se puede descifrar fácilmente por personas no autorizadas.
		Confidencial	Se utiliza la encriptación total del disco, de acuerdo con el Estándar de Encriptación indicado más adelante.	
		Estrictamente confidencial	Se utiliza la encriptación total del disco, de acuerdo con el Estándar de Encriptación indicado más adelante.	
HED20	Quiero guardar mis documentos en SharePoint o en otro sistema de gestión de documentos que NO está alojado en la nube o con Servicios de Internet	Interna	• Usar grupos y niveles de permiso para establecer el control del acceso basado en los roles. Deben establecerse al nivel mínimo para que las personas puedan realizar su trabajo • Revisar los controles de acceso cada año	Limita el acceso y/o la edición a aquellos que necesitan conocer la información
		Confidencial	Como 'Interna' y	

			• Documentar el proceso para asignar personas a roles. • Los roles y las personas asignadas a ellos deben revisarse cada 90 días • Los documentos deben ser encriptados según el Estándar de Encriptación	
		Estrictamente confidencial	Como 'Interna' y • Documentar el proceso para asignar personas a los roles. • Los roles y las personas asignadas a ellos deben revisarse cada 90 días • Los documentos deben ser encriptados según el Estándar de Encriptación	
HED30	Quiero guardar información electrónica en la nube o con los Servicios de Internet, como Google docs, GitHub, btcloud.bt.com, Drobox, Pastebin, Facebook etc.	Interna	No permitido.	Los Servicios de Internet incrementan el riesgo de acceso no autorizado a la información
		Confidencial	No permitido.	
		Estrictamente confidencial	No permitido.	
HED40	Quiero guardar información electrónica en medios extraíbles como una unidad de memoria.	Interna	• Los dispositivos USB se deben encriptar según el Estándar de Encriptación Bajo ninguna circunstancia se pueden guardar datos personales en estos dispositivos salvo que estén encriptados según el Estándar de Encriptación indicado más adelante.	Los medios extraíbles se pueden extraviar o robar más fácilmente que un ordenador completo, por lo que el riesgo de que personas no autorizadas accedan a los datos es mayor. Para proteger la información, se debe convertir en código ilegible que no pueda ser descifrado fácilmente por personas no autorizadas
		Confidencial	Como 'Interna'	
		Estrictamente confidencial	Como 'Interna'	
HED50	Quiero guardar documentos electrónicos o información de BT en mi portátil o dispositivo personales	Interna	No permitido	Personas no autorizadas pueden acceder a datos de BT, sobre todo si se extravía el dispositivo, lo roban, se cambia por un modelo más nuevo.
		Confidencial	No permitido	
		Estrictamente confidencial	No permitido	
HED60	Quiero enviar documentos electrónicos o	Interna	No permitido	Evitar la divulgación a personas no autorizadas

	información a mi dirección de e-mail privada	Confidencial	No permitido	
		Estrictamente confidencial	No permitido	
HED70	Me quiero reenviar información a una dirección de e-mail	Interna	No permitido	Personas no autorizadas podrían acceder a los datos si la cuenta de e-mail, la ISP o la conexión de Internet se vieran comprometidas
		Confidencial	No permitido	
		Estrictamente confidencial	No permitido	
HED80	Quiero compartir *internamente* o enviar información electrónica por e-mail	Interna	Ningún requisito especial	
		Confidencial	• Indicar claramente que el mensaje de e-mail es 'Confidencial' • Usar los ajustes de sensibilidad para marcar el mensaje de e-mail como 'Confidencial' • Idealmente establecer permisos como 'No reenviar' • Si la información está cubierta por 'privilegios legales', recurra al departamento jurídico para que le asesoren •	Mantener el control sobre la información confidencial
		Estrictamente confidencial	Como 'Confidencial' más • Utilice un e-mail seguro para enviarla • Si no es posible utilizar un e-mail seguro, debe encriptarla de acuerdo con el Estándar de Encriptación antes de enviar el archivo • Configurar los permisos como 'No reenviar'	Proteger la información mientras esté en tránsito por distintas redes
HED90	Quiero compartir *externamente* o enviar información electrónica por e-mail	Interna	Solo puede enviar información a una persona externa si tiene un contrato según HSM40	Mantener el control sobre la información confidencial
		Confidencial	Como 'Interna' y • Encriptar según el Estándar de Encriptación • Confirmar que la está enviando a la dirección de e-mail correcta • Si la información está cubierta por 'privilegios legales', recurra al departamento jurídico para que le asesoren	
		Estrictamente confidencial	Como 'Confidencial'	
HED120	Quiero hacer una copia de seguridad de documentos electrónicos de BT	Interna	• Debe guardar sus documentos en unidades de red del Proveedor o en el sistema de	Las copias de seguridad deben tener el mismo nivel de clasificación y

			gestión de documentos del Proveedor según HED030. • El documento del que se ha hecho una copia de seguridad debe estar protegido con el mismo nivel que en la unidad en red, SharePoint. • Si utiliza medios extraíbles, el dispositivo debe estar encriptado utilizando el Estándar de Encriptación.	protección que los datos originales
		Confidencial	Como 'Interna' y • Encriptar el documento de acuerdo con el Estándar de Encriptación antes de hacer una copia de seguridad	
		Estrictamente confidencial	Como 'Confidencial'	

Tratamiento de datos de sistemas y aplicaciones

Ref.	¿Qué quiere hacer?	Clasificación	Requisitos de tratamiento	Motivo
HSADE	Quiero guardar y procesar datos electrónicos e información que están en un centro de datos o en un servidor de sistema	Interna	No hay ningún requisito especial, si se cumplen todos los requisitos aplicables anteriores para el almacenamiento de datos para esta clasificación.	
		Confidencial	Debe cumplir los requisitos para el alojamiento de datos externos de terceros http://www.selling2bt.com/working/ThirdPartySecurity standards/index.htm	
		Estrictamente confidencial	Como 'Confidencial' más Para proteger los datos de cuentas bancarias, al ser especialmente sensibles, se aplican los controles siguientes. Estos tienen prioridad sobre cualquier otro control aplicable en esta especificación de seguridad. 1. Las cuentas bancarias deben estar tokenizadas para las personas (cuentas bancarias personales de clientes y personal de BT); aquí se excluyen los datos de cuentas bancarias propias de BT y los datos bancarios de las distintas entidades legales de BT). 2. Si una aplicación solo contiene cuentas bancarias corporativas, el tercero debe plantear (en base a tiempo, coste, recursos, número de cuentas y número de usuarios con acceso a la aplicación, etc.) si	

			BT aceptará en principio una solución de encriptación. Si se acuerda una solución de encriptación, BT revisará la decisión cuando todas las cuentas bancarias estén protegidas para determinar si es adecuado en adelante. Esto se verá afectado por los niveles de amenaza y el apetito de riesgo del negocio en su conjunto. 3. Cuando se muestren los datos de las cuentas bancarias reales a un agente dentro de un proceso empresarial (por ejemplo, para comprobar que tenemos la cuenta correcta para facturar, o cuando nos comuniquemos con un cliente, por ejemplo, por e-mail, o en una factura), solo debemos mostrar los cuatro últimos dígitos de la cuenta bancaria (es decir, datos de la cuenta bancaria ocultos). 4. Si hay necesidad de acceder a la cuenta bancaria completa (por ejemplo, para permitir una solicitud de crédito o débito de un banco), se deben destokenizar o desencriptar los datos bancarios y después pasar al banco usando un mecanismo de transferencia encriptada que cumpla la política de seguridad de BT. Inmediatamente después de usar datos bancarios desencriptados o destokenizados, se deben eliminar de forma segura.	

Estándares de encriptación

Controles criptográficos generales

Ref.	Control	Motivo
C1.10	Usar bibliotecas criptográficas actuales	Las bibliotecas criptográficas se actualizan regularmente. Además de actualizar los paquetes de software online con la dirección del distribuidor, los paquetes criptográficos se deberían revisar y actualizar regularmente.
C1.20	Usar solo suites de cifrado estándar del sector aprobadas para la encriptación. Por ej. para TLS SSLv2	Los cifrados no aprobados pueden presentar puntos vulnerables
C1.30	Usar la última versión de TLS para los nuevos despliegues. No usar SSL V1,2 y 3	Las versiones anteriores, hasta la TLS1.0 (incluida) ya no se consideran seguras
C1.40	Habilitar Perfect Forward Secrecy	Los algoritmos de Perfect Forward Secrecy evitan que los mensajes interceptados se puedan desencriptar, incluso si la clave privada de autenticación se ve comprometida en el futuro
C1.50	No usar certificados de autofirma	Los certificados de autofirma niegan el beneficio de autenticación de punto final y también reducen significativamente la capacidad de una persona de detectar un ataque *man-in-the-middle* (intermediario).
C1.60 **GTS2.370**	Usar una autoridad de certificación estándar del sector para la gestión del certificado. Por ej. verisign	Mantener un inventario de los certificados emitidos para detectar puntos vulnerables y la caducidad de los certificados
C1.70	Las contraseñas deben protegerse con una función matemática unidireccional no reversible (por ej. algoritmo de Hashing) con factor de	Los archivos de contraseñas guardados se pueden extraer y, por eso, todas las entradas deben protegerse para evitar la recuperación de

	randomización único (Salt) por contraseña. Nota 2: SALT son datos aleatorios que se utilizan como entrada adicional para una función unidireccional que 'hashea' una contraseña o frase de contraseña.	contraseñas de texto sin cifrar
C1.80	Las contraseñas protegidas, según C1.70 deben guardarse alejadas de los archivos de configuración del sistema e implementar un control de acceso para que solo los usuarios con los privilegios pertinentes puedan leer o copiar los contenidos.	Nunca debe poderse recuperar contraseñas protegidas a través de un directorio traversal (salto de directorio), SNMP walk, un volcado de la configuración, u otro mecanismo que pueda permitir intentos de craqueado offline.

Implementación de Criptografía técnica

Protocolos SSL/TLS	
Se pueden usar	**No se pueden usar**
TLSv1.3 (por confirmar, disponible en OpenSSL después del 5 de abril).	SSLv3.0
TLSv1.2	SSLv2.0
TLSv1.1	
TLS v1.0*	

***** TLSv1.0 ya está a punto de descartarse y se puede desaprobar en cualquier momento debido a los problemas conocidos. Por motivos de cumplimiento (por ejemplo, PCI-DSS), puede que los protocolos como TLSv1.0 y TLSv1.1 se tengan que desactivar. Todos los desarrolladores deben estar preparados para deshabilitar este protocolo por configuración.

Tamaños de las claves			
	Simétrica	**Asimétrica**	**Curva elíptica**
Brownfield	≥ 112 bits	≥ 2048 bits	≥ 224 bits
Greenfield	≥ 128 bits	≥ 3072 bits	≥ 384 bits

Intercambio de claves	
Se pueden usar	**No se pueden usar**
ECDHE (Ephemeral (clave temporal) Intercambio de clave Diffie-Hellman (claves no basadas en certificados))	kRSA (Intercambio de clave RSA)
	kDHr (Intercambio de clave Diffie-Hellman con clave RSA)
	kDHd (Intercambio de clave Diffie-Hellman con clave DSA)
	kSRP (Secure Remote Password (SRP) o Intercambio de clave) kADH (Intercambio de clave Diffie-Hellman anónima)
	kPSK (Intercambio de clave precompartida)

Perfect Forward Security debería basarse en valores configurados o generados localmente del Grupo Diffie-Hellman que incluyan cebos 'seguros'.

Parámetros Diffie-Hellman

Parámetros Diffie-Hellman	
Se pueden usar	**No se pueden usar**

Grupo Diffie-Hellman de 3072-bit (mejor - debe generarse localmente).	Valores por defecto del servidor (generar los propios localmente)
Grupo Diffie-Hellman de 2048-bit (se acerca a su final - debe generarse localmente).	

Autenticación	
Se pueden usar	**No se pueden usar**
aRSA (Autenticación RSA)	aNULL (sin autenticación)
aECDSA (Autenticación con algoritmo de firma digital de curva elíptica)	aDSS (Autenticación DSS)
	aECDH (Curva elíptica Diffie-Hellman)
	aDH (Diffie-Hellman)
	aDSA (Algoritmo de firma digital)
	aPSK (Clave precompartida)
	aSRP (Contraseña remota segura)

Cifrado/Encriptación	
Se pueden usar	**No se pueden usar**
AES 256 GCM (Rijndael (Estándar de Encriptación Avanzada) - Modo de recuento Galois)	eNULL (sin encriptación)
AES 128 GCM (Rijndael (Estándar de Encriptación Avanzada) - Modo de recuento Galois)	DES (encriptación DES)
CHACHA20/POLY1305 (256)	3DES (encriptación 3DES)
AES 256 CCM (Rijndael (Estándar de Encriptación Avanzada) - (Modo de recuento con CBC-Mac)	RC4 (encriptación RC4)
AES 128 CCM (Rijndael (Estándar de Encriptación Avanzada) - (Modo de recuento con CBC-Mac)	RC2 (encriptación RC2)
AES 256 CBC (Encadenamiento de bloque de cifrado Rijndael) – se acerca su final.	IDEA (encriptación IDEA)
AES 128 CBC (Encadenamiento de bloque de cifrado Rijndael) – se acerca su final.	Seed (encriptación Seed)
	Camellia (encriptación Camellia)
	ARIA (encriptación ARIA)

Algoritmo MAC Digest	
Se pueden usar	**No se pueden usar**
AEAD (Datos adicionales de encriptación autenticada)	MD5 (Función MD5 Hash)
SHA512 (familia SHA2 - Función SHA512 Hash)	SHA1 (Función SHA1 Hash)
SHA384 (familia SHA2 - Función SHA384 Hash)	SHA (alias para SHA1)
SHA256 (familia SHA2 – Función SHA256 Hash)	