Determinar los niveles de garantía de la seguridad para sus productos de IoT

Empowering Trust®

Resumen ejecutivo

No hace mucho tiempo, se digitalizaba muy poco de nuestra información y de nuestros sistemas Si nos remontamos a 1989, la World Wide Web apenas se estaba inventando y ningún usuario doméstico tenía acceso real a Internet en general. Nuestras fotos todavía se tomaban en un rollo, y la fotografía digital no sería de uso principal hasta 1994, cuando Apple lanzó la primera cámara digital, y en el 2000, cuando apareció la Canon Ixus en el mercado. A principios de los 90, la mayoría de las personas no tenía un teléfono móvil, y quienes tenían uno lo llevaban en portafolios debido a su gran tamaño.

El software malicioso en ese momento, tal como era, consistía principalmente en proyectos de investigación académica y programas molestos que se hacían por diversión. Un programa como estos no podía encriptar nuestras fotos familiares y pedir dinero para que nos las devolvieran, no podía capturar grabaciones de nosotros en nuestras propias casas para chantajearnos, no podía tomar el control de la calefacción o las cerraduras de las puertas de entrada y no podía reclutar los dispositivos que llevábamos a nuestros hogares para usarlos como parte de un ejército global capaz de poner el tráfico de Internet alrededor del mundo de rodillas.

No podía hacer estas cosas porque la mayoría de nuestros datos y sistemas aún eran análogos. En 1989, la seguridad principalmente significaba seguridad física.

Hoy, 30 años después, confiamos el control de nuestros datos y en ocasiones de nuestra vida misma a los sistemas informáticos que nos rodean. Para la seguridad física, así como para la seguridad de nuestros datos, nuestro dinero y nuestros activos, siempre se debe considerar la seguridad del software que se encuentra en los sistemas que controlan o tienen acceso a estas cosas.

Y hoy en día, *todo* tiene un software.

Esto se ha entendido en el contexto de los sistemas informáticos de propósito general desde hace algún tiempo, ciertamente desde mediados de la década de los 90, cuando el uso de Internet aumentó dramáticamente con la World Wide Web. Sin embargo, ahora nos enfrentamos a una nueva etapa de evolución para nuestros sistemas conectados, la era del IoT, y con ella vienen nuevas inquietudes y requisitos para la seguridad.

En este documento hablaremos sobre la definición del IoT y por qué la seguridad del IoT es un problema más difícil de atender que la seguridad de los dispositivos informáticos de propósito general. Además, el documento técnico profundizará en cómo se puede abordar mejor la seguridad del IoT al comprender los riesgos involucrados y utilizar calificaciones de la seguridad implementadas en los sistemas de IoT para informar las decisiones de compra y determinar qué calificación es adecuada para su producto.

Definir el IoT

Aunque el término IoT literalmente significa “Internet of Things” (Internet de las cosas), es difícil definir con claridad lo que entra y lo que no entra en la definición del IoT. Muchos dispositivos inteligentes no se conectan directamente a Internet, utilizando proxies tales como hubs o utilizando únicamente conexiones locales inalámbricas a través de Bluetooth o ZigBee.
La gran mayoría de los sistemas de IoT tienen aplicaciones acompañantes o servicios de nube que aumentan o son efectivamente esenciales para la operación de la “cosa” misma.

Para los propósitos de este documento, usaremos el término IoT para referirnos a cualquier tipo de funciones que incluya al menos un componente físico al que se pueda conectar a través de una red inalámbrica o conmutada. Por lo tanto, el alcance incluye todos los componentes de ese sistema: los componentes físicos, el software residente en sus diversos elementos informáticos y cualquier software que resida en una aplicación móvil o instancia en la nube.

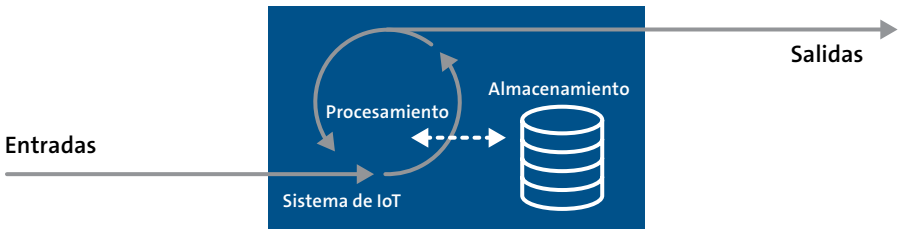
De esta manera, incluimos en la definición cosas como altavoces Bluetooth y cerraduras de puertas que normalmente no tienen ninguna conexión a Internet.
Esta es una definición importante, ya que la seguridad de la cerradura de una puerta es claramente una cuestión importante, mientras que la de un altavoz quizás se considere menos importante.

¿Por qué consideraríamos la seguridad de estas dos cosas de manera diferente cuando se conectan utilizando la misma tecnología inalámbrica? ¿Qué reglas podemos usar para determinar las amenazas que se aplican a cualquier tipo de dispositivo, y qué implican esas amenazas sobre los niveles de seguridad requeridos en ese dispositivo?

Los riesgos del IoT

Al evaluar la seguridad requerida para cualquier sistema de IoT, es importante comprender los riesgos que enfrenta ese sistema, aquello que puede salir mal y por qué una parte malintencionada estaría interesada en comprometer ese sistema. Esencialmente, esto se reduce a la oportunidad y el valor: con qué facilidad se puede acceder a un sistema y cuánto valor puede obtener una parte malintencionada de dicho acceso y/o compromiso (esencialmente, cuál es el activo al cual se dirige el ataque).

En el nivel más fundamental, cualquier sistema informático (incluyendo el IoT) se puede resumir como un sistema de entradas, salidas, almacenamiento y procesamiento, como se ilustra a continuación:



La mayoría de las veces, el enfoque está en las entradas, los datos del usuario, como el factor que define por qué un sistema de IoT puede ser atacado. Sin embargo, todos los aspectos (el almacenamiento, la potencia de procesamiento, el ancho de banda de salida y los datos, las funciones de red y la ubicación de un dispositivo) pueden considerarse como activos inherentemente valiosos para un atacante. Por ejemplo, una cámara que no apunta a su casa se puede considerar que tiene datos de poco valor. Pero esa misma cámara podría comprometerse para volverse parte de una botnet de escala nunca antes vista utilizada por criminales para ver cuándo sale de casa o para ocultar su acertamiento, para comprometer la privacidad de otras personas en su calle o como el primero de una serie de ataques en una red más amplia.

En la siguiente tabla se resumen ejemplos de activos que puede tener un sistema de IoT que pueden ser el objetivo de un atacante, cómo se pueden atacar y con qué fines:

Activo objetivo	Tipo de ataque	Meta de ejemplo/propósito del ataque
Datos almacenados o accedidos	Robo de datos	Monetización/chantaje
	Modificación de datos	Ransomware
	Extracción de datos o código en todo el sistema	Ingeniería inversa de código
Poder de procesamiento	Uso de recursos de procesamiento	Minería de criptomoneda Descifrado de contraseña
Operación/funciones del sistema	Deshabilitar la operación	Ransomware/chantaje
	Alteración de la operación	Imágenes de la cámara de seguridad en bucle
	Determinación de la operación	Determinar si las personas están en casa
	Explotación de operaciones privilegiadas	Abrir puerta cerrada
Operación/funciones de la red	Uso de banda ancha	Ataque DDoS
	Explotación de funciones de red confiables	Modificación de DNS
Ubicación de la red	Acceso a otras redes o sistemas	Para atacar a otros sistemas
	Captura del tráfico de la red	Robar datos de otros sistemas

Debido a esta diversidad en las amenazas, lamentablemente no es fácil saber si algún tipo particular de dispositivo o sistema de IoT tiene algún valor para un atacante. Ese valor con frecuencia es determinado por la manera en que se despliega y utiliza el sistema, más que por el tipo de sistema que es.

Dicho de otra manera, la seguridad de un sistema de IoT se trata más de dónde se encuentra y de los datos y recursos a los que tiene acceso que de lo que es el sistema en sí. El "qué" puede ayudar a definir los datos y recursos, pero no es el factor principal. Un altavoz inteligente que se conecta directamente a Internet y proporciona vistas internas de la casa a través de una cámara integrada con grandes recursos de procesamiento y ancho de banda es un objetivo más atractivo que un altavoz Bluetooth que simplemente reproduce música desde un teléfono conectado.

El problema de la seguridad del IoT

Al comprender estos aspectos de la seguridad de IoT (los tipos de amenazas y riesgos involucrados) es evidente que es necesario atender la seguridad en estos sistemas. Sin embargo, eso no siempre es sencillo. Los sistemas de IoT con frecuencia son una colección de elementos de procesamiento diferentes y de código diferente que se ejecuta en ubicaciones diferentes con seguridad física y lógica diferente. Si el "dónde" es importante, tener múltiples "dóndes" solo puede hacer las cosas más complejas.

Y la complejidad es el enemigo de la seguridad.

Un problema fundamental con la seguridad del IoT es que, aunque la seguridad con frecuencia no cuesta mucho dinero para implementarse bien, no es gratis. La buena seguridad es una función del buen diseño, lo que implica más tiempo y conocimiento en las fases iniciales del desarrollo del producto. Mientras más complejo sea el diseño, más elementos y tipos de código tenga involucrados, más difícil será integrar el conjunto en un sistema seguro.

El mantenimiento de sistemas complejos es igualmente complicado. Mantener los sistemas actualizados a lo largo del tiempo con parches y actualizaciones de seguridad requiere contar con personal para hacerlo: personal que comprenda lo que significa la seguridad para los productos que están creando hoy y que pueda mantenerse al día con las actualizaciones en la investigación de seguridad para saber qué será la seguridad mañana también, pero que esté trabajando en productos después de que se hayan logrado los ingresos iniciales para ese producto. Mientras más complejo sea un sistema, más difícil es mantenerse al día con todos los problemas de seguridad, y se necesitan más personas para hacerlo.

Considerando las demandas globales para sus habilidades, estas personas con frecuencia implican un costo significativo. Por lo tanto, el buen diseño y el mantenimiento continuo tienen un costo tangible, dependiendo del trabajo y el tiempo adicionales que se requieran. De igual importancia, las pruebas y validaciones reales de las funciones de seguridad también tienen un costo. Es posible que se puedan realizar pruebas de seguridad "rápidas" con un costo menor, pero eso brinda solo un bajo nivel de garantía para la propiedad de seguridad que se está probando. Para lograr una garantía mayor, debe hacer pruebas más detalladas, lo que requiere más tiempo y cuesta más dinero. Ese costo se suma al costo de diseño y mantenimiento, que en total debe consumir los ya delgados márgenes de los sistemas de IoT o aumentar su precio en el punto de compra.

Debido a esto, en su raíz, la seguridad es de hecho principalmente un problema *comercial*.

Clasificación de la seguridad del IoT

¿Cómo nos adaptamos a este costo de seguridad? Si consideramos que el costo de seguridad solo puede ser un porcentaje máximo del costo total de un dispositivo (de lo contrario, los consumidores buscarán otras soluciones para comprar), entonces se debe considerar que los dispositivos de menor costo pueden necesitar administrarse con menores niveles de seguridad. Esto no quiere decir que no deba haber un nivel base aceptable de seguridad para todos los dispositivos, sino que la determinación del nivel aceptable puede ser una función del tipo de dispositivo y su implementación.

Sin embargo, la seguridad tampoco puede ser impulsada exclusivamente por el costo. Ya demostramos que las probabilidades de un ataque a un sistema depende más del dónde que del qué. Afortunadamente, con frecuencia (aunque *desafortunadamente* no siempre) existe una correlación entre la accesibilidad de un sistema y su costo para el consumidor. Por ejemplo, las bombillas de IoT a menudo se conectan a través de redes inalámbricas de corta distancia como Zigbee y, por lo tanto, no son directamente accesibles a través de Internet. Por lo tanto, el riesgo que representan estos sistemas se reduce: no pueden acceder directamente a la LAN del usuario, los atacantes no pueden acceder directamente a ellos a través de Internet, no contienen datos confidenciales y tienen muy pocos recursos de procesamiento o ancho de banda.

Un atacante puede usar una bombilla para ayudar a determinar si una persona está en casa, por lo que la seguridad sigue siendo importante para estos productos, pero a menudo se accede a estos dispositivos o se agrupan a través de un hub, que proporciona funciones de seguridad adicionales. Finalmente, todo esto se conecta detrás de un enrutador o firewall que (previsiblemente) proporciona aún más defensas de seguridad a la red interna.

Por lo tanto, es posible que las bombillas no necesiten un alto nivel de garantía de seguridad, pero los hubs a los que se conectan probablemente sí. Los enrutadores y firewalls necesitan los más altos niveles de seguridad, al igual que otros dispositivos que pueden permitir el acceso directo a Internet a través del firewall independientemente de cualquier otra característica de seguridad de la red.

¿Cuánta garantía de seguridad necesita un dispositivo?

Garantía alta
Dispositivos accesibles directamente desde Internet

Dispositivos de seguridad o del perímetro de Internet

Productos de ejemplo
- Cámaras
- Monitores para bebés o mascotas
- Enrutadores, módems
- Hubs expuestos a Internet

Garantía de alta a media
Dispositivos con funciones "inteligentes" relacionadas con la seguridad que pueden o no estar directamente conectados a Internet

Dispositivos con acceso a Internet

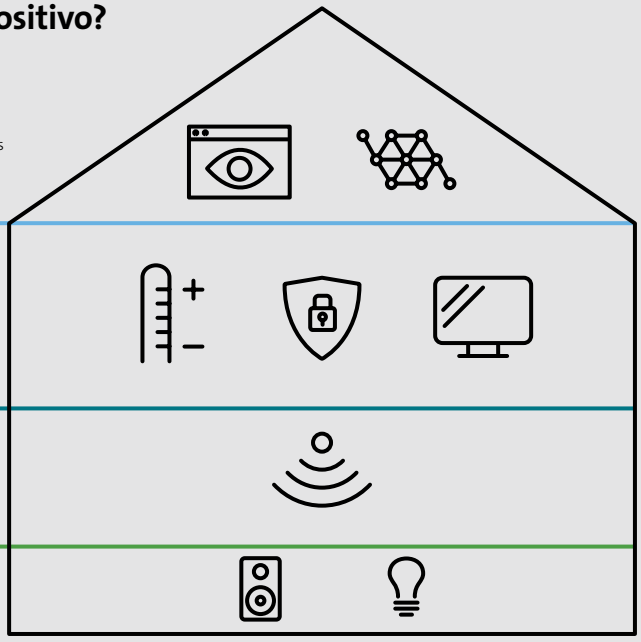
- Calentadores
- Cerraduras para puerta
- Televisores
- Altavoces controlados por voz

Garantía de media a baja
Dispositivos que conectan redes con LAN, pero no directamente con Internet

- Hubs locales
- Puentes de red
- Puntos de acceso

Garantía baja
Dispositivos que no están directamente conectados a la LAN

- Altavoces Bluetooth
- Bombillas (que no son de wi-fi)



Esto nos brinda una vista en capas de la seguridad requerida para los sistemas en un hogar, oficina u otro entorno, con las capas definidas por la accesibilidad y el valor del sistema en sí. Este tipo de capas se ilustra a continuación.

Los sistemas que son menos accesibles y tienen recursos y datos menos valiosos, esencialmente pueden cumplir con un nivel de seguridad más bajo (un nivel más bajo de garantía de seguridad) que los dispositivos que se encuentran en la periferia de la red, los cuales necesitan una clasificación más alta. Por supuesto, estos niveles aceptables de seguridad dependen en gran parte de cómo se despliegan y utilizan los sistemas de IoT, lo que a menudo es difícil de determinar por un fabricante antes de la venta. De hecho, un cliente puede decidir usar bombillas Wi-Fi y conectarlas directamente a Internet, lo que aumentará el riesgo y, por lo tanto, requerirá mayores niveles de seguridad.

Sin embargo, hay algunas preguntas generales que se pueden hacer para ayudar a determinar los riesgos que plantea un sistema y, por lo tanto, el nivel de seguridad que se requiere. Estas se proporcionan en la tabla del lado derecho, mostrando recomendaciones para altos niveles de garantía a niveles más bajos de garantía. El elemento principal que es aplicable para cualquier sistema es el nivel previsto. Por ejemplo, considere una cerradura de puerta Bluetooth. Es posible que solo sea accesible a través de conexiones enrutables que no sean de Internet (lo cual se recomienda para un bajo nivel de garantía), pero como proporciona seguridad física y funciones relacionadas con la seguridad, es apropiado un alto nivel de garantía de seguridad.

Con esta tabla, los fabricantes y proveedores pueden determinar fácilmente qué nivel mínimo de garantía es adecuado para sus productos. Esto no significa que los niveles más altos no sean una buena idea. Los niveles más altos siempre serán mejores, y pueden ayudar con la diferenciación de los productos en el mercado. Esta tabla se proporciona solo como una guía inicial para ayudar a determinar un nivel mínimo que puede ser adecuado.

También se espera que estas recomendaciones puedan cambiar con el tiempo, o que los requisitos y la garantía en cada nivel puedan cambiar, a medida que mejore la madurez de seguridad general del panorama del IoT. Esto sería similar a cómo el estándar de seguridad de automóviles del Australasian New Car Assessment Program (ANCAP) ha incluido elementos de seguridad adicionales con el tiempo, a medida que la seguridad de los automóviles ha mejorado.

Ahora que tenemos una directriz sobre qué niveles pueden ser adecuados, también necesitamos una forma de mostrar

Pregunta de alcance del sistema	Nivel de garantía de seguridad mínimo recomendado
¿El sistema implementa funciones relacionadas con la seguridad, como control de HVAC, red o seguridad física?	Alta
¿El sistema requiere o puede configurarse para tener una conexión directa a Internet?	Alta
¿El sistema tiene acceso a datos confidenciales, tales como grabaciones de video o audio, información de pagos, etc.?	Media a alta
¿El sistema (incluso si se trata de un hub que conecte otros sistemas) permite la conexión directa a Internet (conectarse hacia afuera, en lugar de conectarse hacia adentro como se mencionó anteriormente)?	Media a alta
¿El sistema actúa como un hub o puente entre diferentes redes a la LAN del cliente, pero no proporciona directamente acceso a Internet?	Media a baja
¿El sistema solo es accesible con redes enrutables de banda ancha baja que no son de Internet, como audio de Bluetooth o ZigBee?	Baja

al comprador del sistema de IoT qué nivel de seguridad ha alcanzado realmente un sistema de IoT, cómo se ha evaluado y qué implica para el despliegue esperado del sistema. Esto permite al usuario seleccionar un sistema que puede ser más costoso, pero con una clasificación de seguridad más alta, si tiene la intención de desplegarlo de una manera que implique más riesgo, como conectarlo a Internet, usarlo para el almacenamiento o procesamiento de datos confidenciales o conectarlo a otros sistemas de alto valor.

Aumentar la seguridad básica y permitir que los clientes elijan opciones de seguridad que se adapten a sus necesidades es el papel de los sistemas de clasificación de seguridad.

El viaje de la seguridad

Otro valor de calificar la seguridad de los sistemas, en lugar de proporcionar una salida binaria segura/insegura, es que ayuda a incentivar la inversión y el crecimiento en la seguridad de IoT. No es realista esperar que todos los productos lanzados mañana cumplan automáticamente con los estándares más altos que se pueden establecer para la seguridad. De hecho, es probable que alcanzar estos niveles más altos solo sea posible con un rediseño completo o cambios culturales muy grandes en la forma en que los productos se diseñan, construyen, envían y mantienen.

Esto presenta un dilema para un programa de seguridad apto/no apto. ¿Bajamos el nivel de los requisitos al mínimo que pueden alcanzar la mayoría de los productos hoy en día, entendiendo que este no es el nivel final que realmente queremos lograr, o ponemos el listón donde creemos que debería estar y simplemente esperamos a que la industria se ponga al día?

Si el listón se fija demasiado bajo, al menos podemos tener un poco de validación de los requisitos mínimos, pero no habría ningún incentivo o reconocimiento para que las empresas superen estos requisitos para demostrar que se preocupan por sus clientes. Si el listón está demasiado alto, podemos estar seguros de que los productos que cumplen estos requisitos son muy seguros, pero no es de utilidad si nada puede alcanzar el nivel y toda la industria está desincentivada.

Ninguna de las dos formas proporciona información útil a los consumidores sobre cómo los diferentes productos han aplicado e implementado sus prácticas de seguridad.

Atender la seguridad a través de las clasificaciones: una solución comercial

Impulsar un mayor nivel de madurez de seguridad en los sistemas de IoT requiere una comprensión de los aspectos comerciales que impulsan el diseño y despliegue del IoT, así como los riesgos que informan el nivel de seguridad que se requiere para diferentes tipos de productos y usos. Ese riesgo es una función de muchos factores diferentes: a qué datos puede acceder el sistema, cuánto ancho de banda y potencia de procesamiento tiene, a qué otros sistemas tiene acceso o qué sistemas controla y con qué facilidad se puede acceder a ese sistema de IoT y comprometerlo.

Idealmente, la seguridad de IoT podría abordarse objetivamente como un binario seguro/no seguro, pero esto simplemente no es posible y no proporciona una representación justa de los esfuerzos realizados por la industria. El logro de los niveles más altos de seguridad no ocurre por accidente, y tanto el diseño de productos seguros como las pruebas de seguridad requieren tiempo y cuestan dinero. Esto tiene un impacto en la viabilidad comercial de los productos, reduciendo potencialmente la capacidad de gastar dinero en asegurar la próxima generación de dispositivos.

Con la próxima legislación que exige ciertos mínimos para la seguridad de IoT y varios organismos de la industria que trabajan en sus propios conjuntos de requisitos de seguridad de IoT, ¿cuáles son las mejores formas de lograr el cumplimiento, competir en el mercado y seguir manteniendo una gama de productos comercialmente viable?

Para responder a esta pregunta, no podemos esperar los niveles más altos de seguridad para todos los sistemas desde el principio. Esta simplemente no es una postura comercialmente viable. En lugar de eso, debemos adoptar un enfoque por etapas para la seguridad de IoT e impulsar una base mínima de seguridad para todos los dispositivos, con una mayor seguridad para los sistemas que presentan un mayor riesgo.

Con el tiempo, a medida que crece la comprensión del mercado tanto de la necesidad como del diseño de la seguridad, se pueden incrementar los niveles y sistemas a los que se aplican. Esta conciencia ayudará a aumentar la presión comercial para los sistemas seguros. Por el momento, los clientes han renunciado por completo a la seguridad de IoT o simplemente esperan que la seguridad se incorpore sin una comprensión real de si está ahí o no. Para solucionar este problema, necesitamos hacer que la seguridad sea más visible para el consumidor. Pero sin niveles, nos quedamos con la aceptación de los niveles más bajos que se pueden lograr comúnmente o evitando la adopción de estándares de seguridad que requieren un cambio demasiado rápido en la postura de seguridad.

Mejorar la seguridad debe implicar trabajar con la industria, y no en su contra. Debemos brindar soluciones en lugar de simplemente catalogar los problemas y asegurarnos de que se atiendan los aspectos comerciales de la seguridad. Para hacer esto, debemos poder demostrar fácilmente a los consumidores qué productos han dedicado más tiempo y esfuerzo a su postura de seguridad, y eso solo se puede lograr a través de una metodología de clasificación.

¿Qué clasificación es correcta para usted o para sus productos? Para responder eso, necesita entender a su mercado, sus clientes y la forma en la cual se utiliza su tecnología. El enfoque por capas presentado en este documento, que utiliza información sobre el acceso y los activos, proporciona una forma rápida de tomar esa determinación.

Para obtener más información, contacte a UL escribiendo a IMSecurity@ul.com o visite IMS.UL.com/IoT-Security-Rating.

Ciberseguridad de UL

La clasificación de seguridad de IoT de UL se une a una lista creciente de soluciones de seguridad de IoT de UL, incluyendo el Nivel de Confianza Cibernética de Proveedores de UL, el Programa de Garantía de Ciberseguridad de UL, IEC 62443 y otros servicios de capacitación y asesoría, que atienden las evaluaciones de seguridad en los ecosistemas, la seguridad y calidad de la cadena de suministro, así como los mercados regulados para la seguridad.

Acerca de UL

UL ayuda a crear un mundo mejor al aplicar la ciencia para solucionar desafíos de seguridad y sostenibilidad. Potenciamos la confianza al permitir la adopción segura de tecnologías y productos innovadores. Todos en UL compartimos una pasión por hacer del mundo un lugar más seguro. Todo nuestro trabajo, desde las investigaciones independientes y el desarrollo de estándares, hasta las pruebas y certificaciones, así como la oferta de soluciones analíticas y digitales, ayuda a mejorar el bienestar global. Las empresas, los sectores de la industria, los gobiernos, las autoridades de regulación y el público en general depositan su confianza en nosotros para poder tomar decisiones más inteligentes.

Para obtener más información, visite UL.com.

UL.com

0220