Prácticas recomendadas de Cisco WebEx sobre seguridad en las reuniones para organizadores y administradores de sitios

Primera publicación: 15 de marzo de 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENIDO

Descripción general de la privacidad de WebEx

Las soluciones en línea de Cisco WebEx permiten que los equipos virtuales y los empleados de todo el mundo se reúnan y colaboren en tiempo real como si estuvieran trabajando en el mismo espacio físico. Muchas empresas, instituciones y agencias de la Administración Pública de todo el planeta confían en las soluciones de Cisco WebEx para simplificar los procesos empresariales y mejorar los resultados de los equipos de ventas, marketing, formación, gestión de proyectos y soporte.

La privacidad es una cuestión fundamental para todas estas organizaciones y sus usuarios. Cuando se colabora en línea, es preciso disponer de numerosos niveles de seguridad, ya sea en cuanto a la planificación de las reuniones, la autenticación de los participantes o el intercambio de contenido.

Cisco WebEx es un entorno seguro, aunque pueda establecerse como un espacio abierto para la colaboración. Conocer las funciones de privacidad como administradores de sitios y usuarios finales, permite adaptar WebEx a las necesidades del negocio.

Para obtener más información, consulte el informe sobre seguridad de WebEx.

Prácticas recomendadas para los administradores

Para lograr una privacidad eficaz, se debe empezar por usar la herramienta de administración del sitio de WebEx, que permite a los administradores gestionar y aplicar políticas de privacidad que conciernen a los privilegios de los organizadores y los presentadores. Por ejemplo, un administrador autorizado puede personalizar la configuración de las sesiones con el fin de inhabilitar la capacidad del presentador de compartir aplicaciones o transferir archivos en función del sitio y del usuario.

Le recomendamos utilizar las siguientes funciones de protección en sus reuniones.

Establecimiento de todas las reuniones como no anotadas

Incluso los títulos de las reuniones pueden revelar información confidencial. Por ejemplo, “Discutir la adquisición de la empresa A” puede tener consecuencias económicas si este dato se da a conocer antes de tiempo. Al crear reuniones sin anotar se mantiene la privacidad de la información confidencial.

En el caso de las anotadas, tanto el tema como otros datos de la reunión se muestran en el sitio web a los usuarios autenticados, a los no autenticados y a los invitados. A menos que su organización tenga una necesidad empresarial concreta por la que mostrar los títulos y la información de las reuniones al público, ninguna debería anotarse.

Procedimiento

Paso 1 Inicie sesión en la herramienta de administración del sitio de WebEx.

Paso 2 Vaya a **Configuración > Configuración de sitios comunes > Opciones > Opciones de seguridad**.

Paso 3 Marque la casilla **Todas las reuniones deben quedar sin listar (en MC, TC y EC)**.

Obligatoriedad de tener contraseña para todas las reuniones, eventos y sesiones

La manera más eficaz de reforzar la seguridad de todas las reuniones, eventos y sesiones de formación es exigir una contraseña. Con las contraseñas se evitan accesos no autorizados, ya que solo los usuarios que

disponen de la contraseña pueden unirse. Al solicitar contraseñas, se tiene la certeza de que todas las reuniones, eventos y sesiones de formación creadas por organizadores quedan protegidas.

Le recomendamos que utilice una contraseña de gran complejidad y que no sea trivial, es decir, una contraseña segura. Esta contraseña segura debe incluir mayúsculas, minúsculas, números y caracteres especiales (por ejemplo, "$Tu0psrOx!").

Nota Añadir contraseñas a las reuniones, eventos y sesiones de formación no repercute en la capacidad de unirse de los asistentes autorizados. Los participantes pueden unirse fácilmente haciendo clic en la URL de la invitación por correo electrónico o mediante el sitio web de WebEx.

Procedimiento

Paso 1 Inicie sesión en la herramienta de administración del sitio de WebEx.

Paso 2 Vaya a **Configuración > Configuración de sitios comunes > Opciones > Opciones de seguridad**.

Paso 3 En la sección Meeting Center, marque **Todas las reuniones deben disponer de una contraseña**.

Paso 4 En la sección Event Center, marque **Todos los eventos deben disponer de una contraseña**.

Paso 5 En la sección Training Center, marque **Todas las sesiones deben disponer de una contraseña**.

Paso 6 Para exigir contraseñas seguras, marque **Requerir contraseña segura para reuniones**.

Paso 7 Marque y configure las siguientes opciones:

- Requerir combinación de mayúsculas y minúsculas
- Longitud mínima
- Número mínimo de caracteres numéricos
- Número mínimo de caracteres alfabéticos
- Número mínimo de caracteres especiales
- No permitir que ningún carácter se repita más de tres veces
- No permitir el uso de texto de páginas web dinámicas para las contraseñas de la reunión (nombre del sitio, nombre de organizador, nombre del usuario, tema de la reunión)
- No permitir el uso de las contraseñas de la reunión de esta lista

Imposición de contraseña de reunión al unirse con sistemas de conferencia por teléfono o vídeo (WBS30)

Además de exigir contraseñas cuando los usuarios se unan con una aplicación de reuniones (por ejemplo, en Windows o Mac), también debe exigir contraseñas a los usuarios que se unan con sistemas de conferencia por teléfono o vídeo. Esta opción se ofrece de la versión WBS30 en adelante. Al seleccionarla, el sistema genera automáticamente una contraseña numérica de ocho dígitos para quienes utilizan sistemas de conferencia

por teléfono o vídeo y la incorpora a la invitación de la reunión. De esta forma, se garantiza que solo quienes disponen de la invitación puedan unirse con un sistema de conferencia por teléfono o vídeo.

Procedimiento

Paso 1 Inicie sesión en la herramienta de administración del sitio de WebEx.

Paso 2 Vaya a **Configuración > Configuración de sitios comunes > Opciones > Opciones de seguridad**.

Paso 3 En la sección Meeting Center, marque **Imponer la contraseña de reunión al unirse por teléfono**.

Paso 4 En la sección Event Center, marque **Imponer la contraseña de evento al unirse por teléfono**.

Paso 5 En la sección Training Center, marque **Imponer la contraseña de sesión de formación al unirse por teléfono**.

Paso 6 En la sección Meeting Center, marque **Imponer la contraseña de reunión al unirse con un sistema de videoconferencia**.

Requisito de iniciar sesión al unirse a una reunión, evento o sesión de formación (WBS30)

Le recomendamos que exija a todos los usuarios disponer de una cuenta en su sitio web de WebEx si en él organizará reuniones, eventos y sesiones de formación confidenciales. Si sigue nuestra recomendación, además de a los organizadores, a los asistentes se les solicitarán sus credenciales cuando intenten unirse a una reunión, un evento o una sesión de formación.

De la versión WBS30 en adelante, además de exigir el inicio de sesión en su sitio web, le recomendamos que establezca el requisito de que los asistentes inicien sesión cuando marquen el número desde un teléfono. De esta forma, nadie entrará en la reunión o sesión de formación sin las credenciales adecuadas.

Nota Los participantes que se unen mediante la aplicación de Meeting Center o Training Center ya tienen que autenticarse, por lo que no se les pedirá que se autentiquen al conectarse al audio. Por lo tanto, esta restricción solo afecta a los usuarios que se unen por teléfono.

Asimismo, debe considerar restringir que los sistemas de videoconferencia puedan llamar a una reunión que requiera que los asistentes inicien sesión. Dado que los usuarios no pueden iniciar sesión mediante sistemas de videoconferencia, permitir que se unan con ellos conlleva el riesgo de que los usuarios no autorizados se unan a las reuniones.

Procedimiento

Paso 1 Inicie sesión en la herramienta de administración del sitio de WebEx.

Paso 2 Vaya a **Configuración > Configuración de sitios comunes > Opciones > Opciones de seguridad**.

Paso 3 Para exigir que todos los usuarios tengan una cuenta en su sitio web de WebEx para organizar una reunión, un evento o una sesión de formación de WebEx o asistir a ellos, marque la casilla **Requerir conexión antes de acceder al sitio** (solo en Meeting Center, Event Center y Training Center).

Paso 4 Para establecer el requisito de que se inicie sesión al unirse a una reunión o sesión de formación por teléfono, marque la casilla **Es necesario que los usuarios tengan una cuenta al unirse por teléfono** (solo en Meeting Center y Training Center).
Si se activa esta opción y el organizador exige que se inicie sesión, los asistentes tendrán que iniciar sesión en sus teléfonos. Los asistentes deberán haber añadido un número de teléfono y un PIN a su configuración de perfil.

Paso 5 Cuando sea necesario iniciar sesión para entrar en una reunión, seleccione **Bloqueado** (solo en Meeting Center) para evitar que los usuarios se unan mediante sistemas de videoconferencia.
Si lo hace, los usuarios de sistemas de videoconferencia no podrán comenzar reuniones que requieran iniciar sesión ni unirse a ellas. Esto también ocurre con las salas personales cuando, según su configuración, se debe iniciar sesión.

Prohibición de unirse antes que el organizador

En ninguna reunión permita que los usuarios se unan antes que el organizador a menos que precise que así sea o sea totalmente consciente de los riesgos de seguridad.

Plantéese desactivar en su sitio web las opciones que permiten que alguien se una antes que el organizador. Le recomendamos desactivarlas en el caso de las reuniones anotadas, ya que los asistentes externos podrían usar la reunión planificada en beneficio propio sin que el organizador lo sepa o sin su consentimiento.

De igual modo, si permite que los usuarios entren antes que el organizador, considere prohibirles que se unan al audio antes que él. Si la reunión está anotada en su sitio web o no está protegida con contraseña, es posible que los usuarios sin autorización logren acceder e inicien costosas llamadas sin que el organizador lo sepa o sin su consentimiento.

Le recomendamos que desactive la opción que permite unirse al audio antes que el organizador en el caso de las reuniones de conferencia personal (PCN). De esa forma, el organizador primero tendrá que marcar el número de WebEx Access del puente de audio y, a continuación, introducir el código de acceso y el PIN de organizador para que los asistentes puedan unirse a la reunión.

Procedimiento

Paso 1 Inicie sesión en la herramienta de administración del sitio de WebEx.

Paso 2 Vaya a **Configuración > Configuración de sitios comunes > Opciones > Opciones de seguridad**.

Paso 3 Para evitar que los asistentes se unan antes que el organizador, desmarque las siguientes casillas:

- **Permitir a los asistentes o miembros del panel unirse antes que el organizador** (en MC, TC y EC)

- **El primer asistente en unirse será el presentador** (solo en MC)
- **Permitir a los asistentes o miembros del panel unirse a la teleconferencia antes que el organizador** (en MC, TC y EC)
- **Permitir al asistente que se una a la parte de audio de la conferencia personal antes que el organizador** (en reuniones PCN)

Gestión de cuentas

Para establecer los ajustes de las políticas que conciernen a todos los usuarios de su sitio web, la página de administración del sitio web de WebEx también ofrece las siguientes posibilidades.

Gestión de cuentas de organizador

- Bloquee una cuenta una vez alcanzado el número de intentos fallidos de inicio de sesión, que puede configurarse como se desee.

Creación de cuentas

- Exija a los nuevos usuarios que escriban las letras o los dígitos de la imagen distorsionada que aparezca en la pantalla.
- Solicite la confirmación por correo electrónico de las cuentas nuevas.
- Configure reglas para el registro propio de cuentas nuevas.

Contraseñas de cuentas

- Exija que se cumplan reglas concretas en cuanto al formato, la longitud y la reutilización de las contraseñas.
- Permita cambiar la contraseña con frecuencia.
- Prohíba el uso de contraseñas que se puedan averiguar fácilmente (por ejemplo, “contraseña”).
- Establezca un período mínimo para el cambio de contraseña.

Prácticas recomendadas para los organizadores

Como organizador, es la persona que toma la última decisión sobre los ajustes de seguridad de la reunión. Nunca olvide que ostenta el control de la mayoría de los aspectos relativos a la reunión, incluidos el inicio y el final.

Siga las prácticas de seguridad recomendadas al planificar una reunión, durante dicha reunión y una vez finalizada según las necesidades de su empresa para mantener las reuniones y la información protegidas.

Uso de salas personales (WBS30)

Bloqueo automático de salas personales

Con WBS30, tiene la posibilidad de bloquear automáticamente la sala personal una vez iniciada la reunión. Para ello, vaya a **Mi WebEx > Preferencias > Mi sala personal** en el sitio web de WebEx. Le recomendamos que establezca el bloqueo en **0 minutos**. Básicamente, es bloquear la sala en cuanto usted entra en ella. De esta forma, evita que todos los asistentes del lobby se unan automáticamente a la reunión. No obstante, verá una notificación cuando los asistentes estén esperando en el lobby. Así, podrá negar la entrada a ciertos asistentes y permitírsela solo a los autorizados.

Nota Tenga en cuenta que la URL de la sala personal es pública y, a menos que el administrador del sitio haya configurado las salas personales de manera que solo puedan usarlas los usuarios que han iniciado sesión, cualquiera puede esperarle en el lobby. Compruebe siempre los nombres de los asistentes antes de permitirles entrar en la sala.

Notificaciones de la sala personal antes de la reunión

Cuando los usuarios entran en el lobby de la sala personal, pueden enviarle una notificación por correo electrónico para informarle de que están esperando a que la reunión comience. Incluso los usuarios no autorizados que logran acceder al lobby de su sala personal pueden enviarle notificaciones.

Le recomendamos que consulte las notificaciones por correo electrónico antes de iniciar una reunión para no dejar entrar a quienes no tienen autorización. Si no ha establecido el bloqueo automático de su sala personal en 0 minutos, todos los asistentes que estén esperando en el lobby entrarán en la reunión cuando usted lo haga. Revise la lista de participantes y expulse a aquellos que no tengan autorización.

Si ha establecido el bloqueo automático de su sala personal y ve demasiadas notificaciones por correo electrónico de asistentes no autorizados, considere desactivar dichas notificaciones. Vaya a **Mi WebEx >**

Preferencias y desactívelas desmarcando la casilla **Notificarme por correo electrónico cuando alguien entre en el lobby de mi sala personal si no estoy**.

Notificaciones de sala personal durante la reunión

Si bloquea su sala personal, puede impedir la entrada a cualquiera que espere en el lobby. Cuando ya haya entrado en su reunión, recibirá una notificación siempre que un usuario nuevo entre en el lobby y podrá decidir si quiere admitirle o no. Cuando sean varios los asistentes que esperen en el lobby de la sala personal, podrá revisar la lista de nombres y seleccionar a ciertos usuarios o a todos para que entren en la reunión.

Planificación de una reunión

Planificación de reuniones sin anotar

Para reforzar la privacidad de la reunión, los organizadores pueden decidir no anotarla en el calendario de reuniones. Si así lo desea, desmarque esta opción para evitar que se acceda a la reunión sin autorización y oculte la información al respecto, como el organizador, el tema y la hora de inicio.

- Las reuniones que no se anotan no se muestran en el calendario de reuniones de la página Examinar reuniones, ni en la página Mis reuniones.
- Para unirse a una reunión sin anotar, los asistentes deberán facilitar un número de reunión único.
- Además, el organizador tendrá que informar a los asistentes, por ejemplo, enviando un enlace en una invitación por correo electrónico, aunque también puede introducir el número de la reunión mediante la página Unirse a la reunión.

Nota Al anotar una reunión, el título y la información quedan expuestos al público y, si dicha reunión no está protegida con contraseña, cualquiera podrá unirse.

Consejo Elija el nivel de seguridad en función del objetivo de la reunión. Por ejemplo, si está planificando una reunión para hablar sobre una excursión de trabajo, probablemente solo tenga que especificar una contraseña para la reunión. Si, por el contrario, está planificando una reunión en la que se dará información financiera confidencial, no deberá incluir la reunión en el calendario. También puede restringir el acceso a la reunión cuando se hayan unido todos los asistentes.

Selección cuidadosa del tema de la reunión

Cuando se anota una reunión o se reenvía la invitación por correo electrónico, puede exponerse a público no deseado, como mínimo, el nombre de la reunión. Los títulos pueden, involuntariamente, revelar información privada, por lo que debe asegurarse de que se redacten con cautela para minimizar la revelación de datos confidenciales, como nombres de empresa o eventos.

Protección de las reuniones con contraseñas difíciles de averiguar

Usar una contraseña compleja para cada sesión es lo mejor que se puede hacer para proteger las reuniones. Aunque no es lo habitual, los administradores de sitios pueden optar por permitir la creación de reuniones sin

contraseñas. En la mayoría de los casos, se recomienda encarecidamente proteger todas las reuniones con una contraseña segura.

El método más eficaz para reforzar la seguridad de una reunión es crear una contraseña de gran complejidad y que no sea trivial, es decir, una contraseña segura. Esta contraseña segura debe incluir mayúsculas, minúsculas, números y caracteres especiales (por ejemplo, "$Tu0psrOx!"). Con las contraseñas se evitan accesos no autorizados, ya que solo los usuarios que disponen de la contraseña podrán unirse a la reunión.

No reutilice las contraseñas para otras reuniones, pues planificarlas con la misma contraseña reduce considerablemente su seguridad.

Nota Añadir contraseñas a las reuniones no repercute en la capacidad de unirse de los asistentes autorizados. Los participantes podrán unirse fácilmente haciendo clic en la URL de la invitación por correo electrónico, con la aplicación de WebEx para dispositivos móviles o mediante otros canales como Cisco Jabber.

Omisión de la contraseña de la reunión en las invitaciones

Si invita a los asistentes a una reunión, la contraseña de la reunión no aparecerá en las invitaciones por correo electrónico que reciban los asistentes. Deberá facilitar la contraseña a los asistentes mediante otros métodos, por ejemplo, por teléfono.

En el caso de las reuniones de estricta confidencialidad, no incluya la contraseña en la invitación por correo electrónico. Así, evitará accesos no autorizados a los detalles de la reunión si el mensaje de invitación por correo electrónico se reenvía a un destinatario no deseado.

Obligatoriedad de estar en posesión de una cuenta en el sitio web

Cuando se activa la opción pertinente, todos los asistentes deberán tener una cuenta de usuario en su sitio para asistir a la reunión. Para obtener información acerca de cómo los asistentes pueden conseguir una cuenta de usuario, consulte al administrador del sitio.

En el planificador avanzado del centro de reuniones, active la opción **Requerir que los asistentes dispongan de una cuenta en este sitio web para unirse a esta reunión.**

Uso de Tono de entrada y salida o Anunciar nombre

Con esta función, evita que un usuario se una al audio de la reunión sin que usted lo sepa.

Está activada de manera predeterminada en Meeting Center y Training Center. Para establecer los parámetros, seleccione **Configuración de audioconferencia > Tono de entrada y de salida**.

Restricción de las funciones disponibles

Limite las funciones disponibles, como el chat y el audio, si permite que los asistentes entren en la reunión antes que el organizador.

Requisito de no reenviar invitaciones

Solicite a sus invitados que no reenvíen la invitación, en especial, cuando se trata de reuniones confidenciales.

Asignación de organizadores alternativos

Asigne un organizador alternativo para que inicie y controle la reunión. De esta forma, las reuniones son más seguras, ya que es imposible que la función de organizador se asigne a asistentes inesperados o sin autorización en caso de que, sin querer, se desconecte de la reunión.

Nota Al invitar asistentes a una reunión planificada, puede designar uno o varios asistentes como organizadores alternativos de la reunión. Los organizadores alternativos pueden iniciar la reunión y actuar como el organizador. Es por ello por lo que el organizador alternativo debe tener una cuenta de usuario en el sitio web de Meeting Center.

Durante la reunión

Restricción de acceso a la reunión

Bloquee la reunión una vez estén presentes todos los asistentes. De este modo, evitará que se unan más asistentes. Los organizadores pueden bloquear y desbloquear la reunión en cualquier momento de la sesión en curso. Para bloquear una reunión, seleccione **Reunión > Restringir acceso**.

Consejo Esta opción impide que nadie se pueda unir a la reunión, incluidos los participantes invitados que aún no se hayan unido. Para desbloquear una reunión, seleccione **Reunión > Restaurar acceso**.

Validación de la identidad de todos los usuarios de una llamada

Una práctica segura consiste en corroborar la presencia de todos los asistentes pasando lista. Pida a los usuarios que activen la función de vídeo o digan su nombre para confirmar su identidad.

Nota

- Para asistir a una reunión por teléfono, la persona que llama solo tiene que conocer el número de WebEx válido que debe marcar y el ID de reunión de nueve dígitos. Las contraseñas de las reuniones no evitan que los asistentes puedan unirse desde el audio de la conferencia de WebEx.
- Si se permite que se unan a la reunión asistentes sin cuenta, los usuarios no autorizados podrán identificarse con cualquier nombre.

Expulsión de un participante de una reunión

Se pueden expulsar participantes de la reunión en cualquier momento.

Seleccione el nombre de quien desee eliminar y, a continuación, seleccione **Participante > Expulsar**.

Intercambio de aplicaciones (no uso compartido de la pantalla)

Utilice la opción **Compartir > Aplicación** y no **Compartir > Pantalla** para intercambiar ciertas aplicaciones y evitar exponer por error información confidencial en la pantalla.

Después de la reunión

Asignación de contraseñas para las grabaciones

La mejor manera de evitar que personas sin autorización accedan a las grabaciones es no crearlas.

Si se deben realizar grabaciones de la reunión, puede editarlas y añadir contraseñas antes de compartirlas para mantener la información segura. Para ver las grabaciones protegidas con una contraseña, los destinatarios deben disponer de dicha contraseña.

Eliminación de grabaciones

Elimine las grabaciones en el momento en el que carezcan de importancia.

Conferencias personales para organizadores

En la sección Preferencias de Mi WebEx que encontrará en el sitio web de WebEx, cree un PIN de audio seguro y guárdelo.

Este PIN es la última capa de protección para prevenir accesos no autorizados en la cuenta de conferencias personales. Si una persona consigue sin autorización el código del organizador para acceder a una reunión de conferencia personal (PCN), dicha conferencia no podrá comenzar sin el PIN de audio. Guarde su PIN de audio y no lo comparta con nadie.