Información para el usuario final de Duo
Plantillas de comunicación

Índice

Mejores prácticas de comunicación por correo electrónico

Glosario del usuario final + preguntas frecuentes

- Glosario
- Preguntas frecuentes

Plantillas de correo electrónico: presentación de Duo a los usuarios finales

- Utilice estas plantillas si su organización presenta MFA/Duo por primera vez a los usuarios finales:
- Utilice estas plantillas de correo electrónico si su organización está reemplazando una solución MFA preexistente por Duo:

Plantillas de correo electrónico: nueva comunicación de pólizas

- Utilice estas plantillas para informar a los usuarios de los próximos cambios de pólizas:

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Mejores prácticas de comunicación por correo electrónico

A continuación, se detallan algunas prácticas recomendadas al enviar correos electrónicos a los usuarios sobre la próxima implementación de Duo 2FA:

- **Días para enviar correos electrónicos:** los martes, miércoles y jueves son los mejores días para enviar correos electrónicos que los usuarios deben abrir.
- **Quién debe enviar el correo electrónico:** recomendamos que el correo electrónico provenga de una persona (gerente de TI, director de operaciones, etc.) o de su servicio de asistencia técnica.

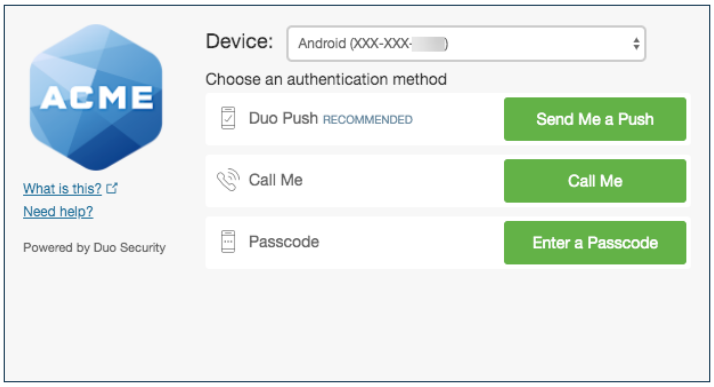
Glosario del usuario final y preguntas frecuentes

A continuación, encontrará términos y preguntas clave que pueden ser útiles para los usuarios cuando se les presenta Duo. Siéntase libre de utilizar esta información tal como está o personalizarla, según sea necesario para su organización.

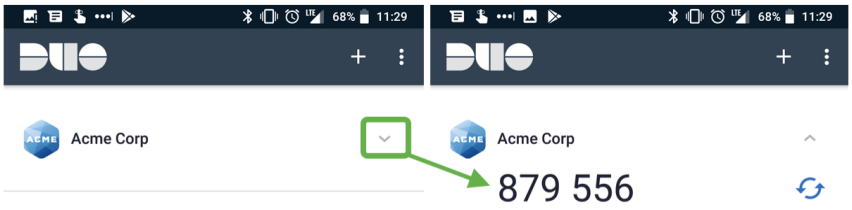
Glosario

2FA (doble factor de autenticación): es una capa adicional de autenticación que va más allá de un nombre de usuario y una contraseña. 2FA involucra algo que usted conoce (contraseña), más algo que lleva con usted (como Duo Mobile en su smartphone), para evitar que alguien inicie sesiónes solo con su contraseña. Con Duo 2FA, todavía introduce su nombre de usuario y contraseña. El segundo factor proporcionado por Duo es simplemente una capa adicional de seguridad, además de sus credenciales existentes. Recomendamos usar Duo Push, a través de la aplicación Duo Mobile, para ejecutar 2FA.

Duo Prompt: este aviso interactivo le permite elegir cómo verificar su identidad cada vez que inicie sesión (por ejemplo, «Duo Push» o «Llámame») a una aplicación web. Además, Duo Prompt le permite registrarse y autenticar.



Código de acceso: estos son códigos numéricos que se pueden generar a través de la aplicación Duo Mobile, SMS (mensaje de texto) o mediante un token de hardware, dependiendo de lo que permita su administrador de TI. Los códigos de acceso se pueden usar en cualquier momento y son especialmente útiles para la autenticación cuando su dispositivo 2FA no tiene servicio de Internet o móvil.



Notificación Push (Duo Push): es una solicitud de autenticación push que se envía a la aplicación Duo Mobile en un dispositivo registrado. Las notificaciones automáticas incluyen información como la ubicación geográfica del dispositivo de acceso, la dirección IP del dispositivo de acceso y la aplicación a la que se accede, para que pueda verificar si la notificación push es real o fraudulenta.

Portal de autoservicio: si el portal de autoservicio se ha habilitado para utilizarlo en Duo Prompt, puede hacer clic en «My Settings & Devices» para agregar dispositivos adicionales o actualizar la configuración del método de autenticación directamente desde Duo Prompt.

Preguntas frecuentes

A continuación, les presentamos algunas preguntas claves que los usuarios finales realizan frecuentemente. *Dependiendo de la configuración y las aplicaciones específicas de su organización, algunas preguntas pueden necesitar ser modificadas o pueden ser omitidas.*

¿Necesito un smartphone o un plan de datos para usar la autenticación de factor doble?

No. Tener un smartphone lo convierte en una experiencia más fácil y segura con Duo Push. Sin embargo, si su organización lo permite, también es posible registrar un dispositivo móvil que no sea un smartphone, o un teléfono fijo para recibir códigos de acceso o llamadas telefónicas.

¿Qué es Duo Mobile?

Duo Mobile es una aplicación móvil (app) que instala en su smartphone o tablet para generar códigos de acceso de inicio de sesión, o recibir notificaciones automáticas para una autenticación fácil en su dispositivo móvil. Funciona con el servicio de autenticación de factor doble (2FA) de Duo Security, para que sus inicios de sesión sean más seguros.

¿Cuál es el método de autenticación de doble factor recomendado?

Si tiene un smartphone o una tablet, recomendamos Duo Push, ya que es rápido, fácil de usar y seguro. Vea una introducción a Duo Security y una demostración de Duo Push en este breve video: https://www.youtube.com/watch?v=_T_sJXnSM98

¿Cuántos datos utiliza una solicitud de Duo Push?

Las solicitudes de autenticación Duo Push requieren una cantidad mínima de datos, menos de 2 KB por autenticación. Por ejemplo, solo consume 1 megabyte (MB) de datos si autentica 500 veces en un mes determinado.

¿Por qué dejé de recibir notificaciones automáticas de Duo Mobile?

Hay varias razones por las que esto podría estar sucediendo. Intente lo siguiente para solucionar este problema:

1. Asegúrese de que su dispositivo registrado tenga una red móvil o conexión WiFi;
2. Abra la aplicación Duo Mobile cuando se autentique.
3. Pruebe estos pasos adicionales de solución de problemas de push:
    - iPhone: https://help.duo.com/s/article/2051
    - Android: https://help.duo.com/s/article/2050
4. Si las soluciones anteriores no funcionan, intente utilizar otro método de autenticación, como los códigos de acceso que se proporcionan en la aplicación Duo Mobile.

¿Cómo puedo autenticar si estoy en un lugar sin servicio móvil o acceso a WiFi?

Consulte este artículo de Duo Knowledge Base para obtener información sobre cómo autenticar sin servicio móvil o de Internet: https://help.duo.com/s/article/4449

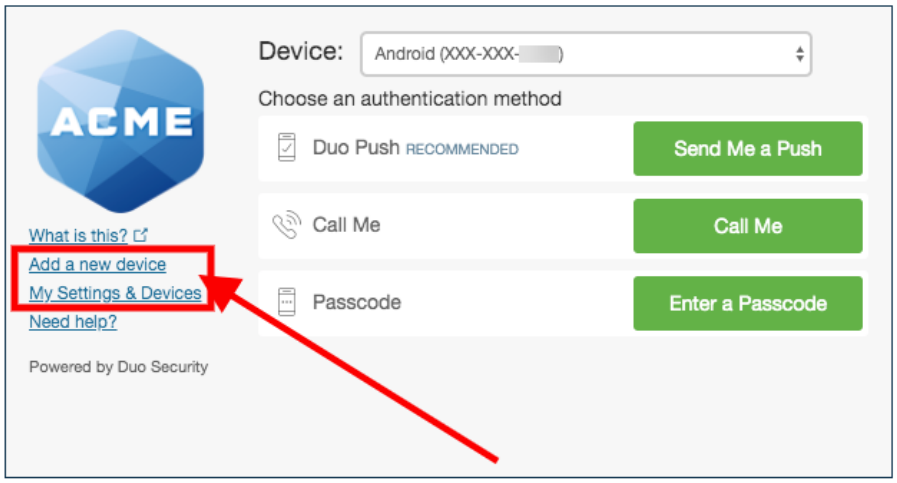
¿Cómo puedo administrar los dispositivos que uso para Duo?

Si tiene acceso al enlace «Mis configuraciones y dispositivos» (el portal de autoservicio) en Duo Prompt, y puede autenticarse con un dispositivo, podrá:

- agregar dispositivos adicionales;
- designar su dispositivo «predeterminado», que reciba solicitudes de autenticación, además de su método de autenticación preferido;

- desactivar Duo Mobile si tiene un teléfono nuevo, pero mantiene su número;
- cambiar el nombre de su dispositivo (ej. «teléfono móvil» o «Teléfono de trabajo»);
- eliminar un dispositivo.

Obtenga más información sobre cómo administrar sus dispositivos aquí: https://guide.duo.com/manage-devices



¿Qué debo hacer si pierdo mi teléfono?

Póngase en contacto con su servicio de asistencia de TI de inmediato.

¿Duo puede ver mi contraseña?

No. Su contraseña solo es verificada por su organización y nunca se envía a Duo. Duo solo proporciona el segundo factor, usando su dispositivo registrado para verificar que en realidad es usted quien está intentando acceder.

¿El uso de Duo facilita el control de mi smartphone?

No. La aplicación Duo Mobile no tiene acceso para cambiar configuraciones o borrar de manera remota su teléfono. La visibilidad que Duo Mobile requiere es verificar la seguridad de su dispositivo, como la versión del sistema operativo, el estado de cifrado del dispositivo, el bloqueo de pantalla, etc. Usamos esto para ayudar a recomendar mejoras de seguridad en su dispositivo. Usted siempre tendrá el control de seguir o no estas recomendaciones.

Plantillas de correo electrónico: presentación de Duo a los usuarios finales

Utilice estas plantillas si su organización presenta MFA/Duo por primera vez a los usuarios finales:

Correo electrónico n. ° 1 - *Duo se estrenará pronto. No se requiere acción inmediata.*

CRONOGRAMA:

30 días antes de la fecha de inicio de envío/aplicación del correo electrónico de registro.

ASUNTO:

¡La autenticación factor doble de Duo se estrenará pronto!

CUERPO:

Para mejorar nuestra posición de seguridad, incorporaremos Duo Security como una **solución de autenticación de factor doble** en nuestra infraestructura de TI existente.

Acción requerida:

No es necesaria una acción inmediata. Este correo electrónico es para notificar y mostrar el próximo lanzamiento de la autenticación de factor doble de Duo.

¿Qué es Duo Security?

Duo Security es una empresa que brinda un servicio de software basado en la nube, que utiliza la autenticación de factor doble para garantizar el acceso seguro a servicios y datos. Obtenga más información haciendo clic **aquí**.

¿Qué es la autenticación de factor doble?

La autenticación de factor doble proporciona un segundo canal de seguridad para cualquier tipo de inicio de sesión **que requiera información adicional, o un dispositivo físico para iniciar sesión,** además de su contraseña.

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Al requerir dos canales de autenticación diferentes, podemos proteger los inicios de sesión de los usuarios de ataques remotos que puedan explotar nombres de usuario y contraseñas robadas.

Los factores pueden incluir:

Algo que conozca:
- un nombre de usuario y contraseña únicos.

Algo que tenga:
- un smartphone con una aplicación para aprobar solicitudes de autenticación.

Algo personal:
- biometría: como su huella dactilar o un escáner de la retina.

¿Por qué necesitamos la autenticación de factor doble?

Las credenciales de inicio de sesión son muy importantes, y cada vez son más fáciles de verse en riesgo. En la actualidad, más del 90 % de las infracciones implican nombres de usuario y contraseñas expuestas a riesgos.

La autenticación de factor doble mejora la seguridad de su cuenta, mediante el uso de un dispositivo secundario para verificar su identidad. **Esto impide que alguien, salvo usted, acceda a su cuenta, incluso si conocen su contraseña, no disponen de su dispositivo móvil.**

¿Cómo Duo cambiará mi experiencia de inicio de sesión?

Cuando inicie sesión en una aplicación que esté protegida por Duo, deberá ingresar su nombre de usuario y contraseña. Después de ingresar su información de inicio de sesión, **Duo le pedirá que complete un método de autenticación de factor doble**.

Duo no reemplaza ni exige cambiar su nombre de usuario y contraseña. Imagine que Duo es un canal de seguridad adicional a su método de inicio de sesión preexistente. **Pronto tendrá más información sobre el lanzamiento de Duo.**

Correo electrónico n.º 2: *Duo se estrenará el <FECHA>. No se requiere acción inmediata.*

CRONOGRAMA:

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

15 días antes de la fecha de inicio de envío/aplicación del correo electrónico de registro.

ASUNTO:

Regístrese en la autenticación de factor doble de Duo el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**

CUERPO:

Para mejorar nuestra posición de seguridad, incorporaremos Duo Security como una **solución de autenticación de factor doble** en nuestra infraestructura de TI existente.

Recibirá un correo electrónico de registro de Duo el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**. En los próximos días, recibirá información más detallada sobre este tema.

Acción requerida:

No es necesaria una acción inmediata. Este correo electrónico es para notificar y mostrar el próximo lanzamiento de la autenticación de factor doble de Duo el **<FECHA DEL CORREO ELECTRÓNICO DE REGISTRO>**.

¿Qué es Duo Security?

Duo Security es una empresa que brinda un servicio de software basado en la nube, que utiliza la autenticación de factor doble para garantizar el acceso seguro a servicios y datos. Obtenga más información haciendo clic **aquí**.

¿Qué es la autenticación de factor doble?

La autenticación de factor doble proporciona un segundo canal de seguridad para cualquier tipo de inicio de sesión **que requiera información adicional, o un dispositivo físico para iniciar sesión,** además de su contraseña.

Al requerir dos canales de autenticación diferentes, podemos proteger los inicios de sesión de los usuarios de ataques remotos que puedan explotar nombres de usuario y contraseñas robadas.

Los factores pueden incluir:

Algo que conozca:

- un nombre de usuario y contraseña únicos.

Algo que tenga:

- un smartphone con una aplicación para aprobar solicitudes de autenticación.

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Algo personal:

- biometría: como su huella dactilar o un escáner de la retina.

¿Por qué necesitamos la autenticación de factor doble?

Las credenciales de inicio de sesión son muy importantes, y cada vez son más fáciles de verse en riesgo. En la actualidad, más del 90 % de las infracciones implican nombres de usuario y contraseñas expuestas a riesgos.

La autenticación de factor doble mejora la seguridad de su cuenta mediante el uso de un dispositivo secundario para verificar su identidad. **Esto impide que alguien, salvo usted, acceda a su cuenta, incluso si conocen su contraseña, no disponen de su dispositivo móvil.**

¿Cómo Duo cambiará mi experiencia de inicio de sesión?

Cuando inicie sesión en una aplicación que esté protegida por Duo, deberá ingresar su nombre de usuario y contraseña. Después de ingresar su información de inicio de sesión, **Duo le pedirá que complete un método de autenticación de factor doble**.

Duo no reemplaza ni exige cambiar su nombre de usuario y contraseña. Imagine que Duo es un canal de seguridad adicional a su método de inicio de sesión preexistente. **Pronto tendrá más información sobre el lanzamiento de Duo.**

Correo electrónico n.º 3: *Duo se presentará el <FECHA> + información de registro. No se necesita realizar ninguna acción en este momento.*

CRONOGRAMA:

3 días antes de la fecha de inicio de envío/aplicación del correo electrónico de registro.

ASUNTO:

Recordatorio: la autenticación de factor doble de Duo se presentará el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**

CUERPO:

Para mejorar nuestra posición de seguridad, incorporaremos Duo Security como una **solución de autenticación de factor doble** en nuestra infraestructura de TI existente.

Recibirá un correo electrónico de registro de Duo el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>.** Este correo electrónico contiene un **enlace personalizado que le permitirá registrarse con Duo**. Este proceso de autoregistro de 2 minutos hace que sea fácil **registrar su teléfono e instalar la aplicación Duo Mobile.**

Si no tiene un smartphone, puede registrar un teléfono celular regular (SMS y llamadas) o un teléfono fijo (llamadas) para la autenticación de factor doble.

Acción requerida:

No se requiere acción inmediata. Este correo electrónico es para recordarle el próximo lanzamiento de la autenticación de factor doble de Duo el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**.

¿Qué son Duo Mobile y Duo Push?

Duo Mobile es la aplicación gratuita de Duo Security que le permitirá aprobar rápida y fácilmente una solicitud de autenticación de factor doble usando **Duo Push**.

Con **Duo Mobile y Duo Push** no es necesario cargar un token pesado o perder tiempo ingresando manualmente códigos de acceso. Solo toque para autenticar directamente en su smartphone.

Aquí tiene un ejemplo de Duo Push en acción.

¿Cómo Duo cambiará mi experiencia de inicio de sesión?

Cuando inicie sesión en una aplicación que esté protegida por Duo, deberá ingresar su nombre de usuario y contraseña. Después de ingresar su información de inicio de sesión, **Duo le pedirá que complete un método de autenticación de factor doble**.

Duo no reemplaza ni exige cambiar su nombre de usuario y contraseña. Imagine que Duo es un canal de seguridad adicional a su método de inicio de sesión preexistente.

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

¿Qué es Duo, qué es la autenticación de factor doble, y por qué la necesitamos?

Si no recibió o no puede encontrar nuestros correos electrónicos anteriores, mire **este video** para obtener más información.

¿Tiene más preguntas?

Por favor, comuníquese con el **<servicio de asistencia/servicio técnico>** para cualquier pregunta sobre el registro o uso de Duo.

- **Número de teléfono de <servicio de asistencia/servicio técnico>:**
- **Correo electrónico de <servicio de asistencia/servicio técnico>:**

Correo electrónico n.º 4: *Revise su bandeja de entrada para buscar el correo electrónico de registro de Duo. Regístrese ahora.*

CRONOGRAMA:

Día de envío/aplicación de correo electrónico de registro.

ASUNTO:

Acción requerida: regístrese en Duo hoy.

CUERPO:

Para mejorar nuestra posición de seguridad, incorporaremos Duo Security como una **solución de autenticación de factor doble** en nuestra infraestructura de TI existente.

Hoy recibirá un correo electrónico de registro de Duo Security. Este correo electrónico contiene un **enlace personalizado que le permitirá registrarse con Duo**. Este proceso de autoregistro de 2 minutos hace que sea fácil **registrar su teléfono e instalar la aplicación Duo Mobile.**

Si no tiene un smartphone, puede registrar un teléfono celular regular (SMS y llamadas) o un teléfono fijo (llamadas) para la autenticación de factor doble.

Tendrá hasta **<FECHA DE LA APLICACIÓN + INICIO DE DUO>** para registrarse. Después de esta fecha, el acceso a **<APLICACIÓN>**, requerirá la autenticación de factor doble de Duo.

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Acción requerida:

Regístrese hoy. Busque en su bandeja de entrada un correo electrónico de registro de Duo y complete el proceso.

¿Qué son Duo Mobile y Duo Push?

Duo Mobile es la aplicación gratuita de Duo Security que le permitirá aprobar rápida y fácilmente una solicitud de autenticación de factor doble usando **Duo Push**.

Con **Duo Mobile y Duo Push** no es necesario cargar un token pesado o perder tiempo ingresando manualmente códigos de acceso. Solo toque para autenticar directamente en su smartphone.

Aquí tiene un ejemplo de Duo Push en acción.

¿Cómo Duo cambiará mi experiencia de inicio de sesión?

Cuando inicie sesión en una aplicación que esté protegida por Duo, deberá ingresar su nombre de usuario y contraseña. Después de ingresar su información de inicio de sesión, **Duo le pedirá que complete un método de autenticación de factor doble**.

Duo no reemplaza ni exige cambiar su nombre de usuario y contraseña. Imagine que Duo es un canal de seguridad adicional a su método de inicio de sesión preexistente.

¿Qué es Duo, qué es la autenticación de factor doble, y por qué la necesitamos?

Si se perdió nuestros correos electrónicos anteriores, mire **este video** para obtener más información.

¿Tiene más preguntas?

Por favor, comuníquese con el **<servicio de asistencia/servicio técnico>** para cualquier pregunta

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

sobre el registro o uso de Duo.

- **Número de teléfono de <servicio de asistencia/servicio técnico>:**
- **Correo electrónico de <servicio de asistencia/servicio técnico>:**

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Utilice estas plantillas de correo electrónico si su organización está reemplazando una solución MFA preexistente por Duo:

Correo electrónico n. ° 1: *Duo se estrenará pronto. No se requiere acción inmediata.*

CRONOGRAMA:

30 días antes de la fecha de inicio de envío/aplicación del correo electrónico de registro.

ASUNTO:

Autenticación factor doble de Duo para reemplazar **<proveedor actual de 2FA>**

CUERPO:

Para mejorar nuestra posición de seguridad y la experiencia actual del usuario con la **autenticación de factor doble**, reemplazaremos **<proveedor actual de 2FA>** e incorporaremos Duo Security como nuestra nueva solución de **autenticación de factor doble** en nuestra infraestructura de TI existente.

Acción requerida:

No es necesaria una acción inmediata. Este correo electrónico es para notificar y mostrar el próximo cambio en la forma en que realizamos la autenticación de factor doble.

¿Por qué Duo Security es una mejor experiencia de usuario?

Con la aplicación móvil gratuita de Duo Security, **Duo Mobile**, ya no es necesario que cargue un token pesado ni pierda el tiempo ingresando un código de acceso al iniciar sesión en una aplicación protegida.

Duo Mobile le permite aprobar rápida y fácilmente una solicitud de autenticación de factor doble en su smartphone a través de **Duo Push.** Si utilizó previamente un token de hardware o código de acceso, **su smartphone ahora lo reemplazará.** Aquí tiene un ejemplo de Duo Push en acción.

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

¿Por qué necesitamos la autenticación de factor doble?

Las credenciales de inicio de sesión son muy importantes, y cada vez son más fáciles de verse en riesgo. En la actualidad, más del 90 % de las infracciones implican nombres de usuario y contraseñas expuestas a riesgos.

La autenticación de factor doble mejora la seguridad de su cuenta, mediante el uso de un dispositivo secundario para verificar su identidad. **Esto impide que alguien, salvo usted, acceda a su cuenta, incluso si conocen su contraseña.**

¿Cómo Duo cambiará mi experiencia de inicio de sesión?

Cuando inicie sesión en una aplicación que esté protegida por Duo, deberá ingresar su nombre de usuario y contraseña. Después de ingresar su información de inicio de sesión, **Duo le pedirá que apruebe una notificación de Duo Push u otro método de autenticación de factor doble**.

Duo no reemplaza ni exige cambiar su nombre de usuario y contraseña. Imagine que Duo es un canal de seguridad adicional a su método de inicio de sesión preexistente. **Pronto tendrá más información sobre el lanzamiento de Duo.**

Correo electrónico n.º 2: *Duo se estrenará el <FECHA>. No se requiere acción inmediata.*

CRONOGRAMA:

15 días antes de la fecha de inicio de envío/aplicación del correo electrónico de registro.

ASUNTO:

Regístrese en la autenticación de factor doble de Duo el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**

CUERPO:

Para mejorar nuestra posición de seguridad y la experiencia actual del usuario con la **autenticación de factor doble**, reemplazaremos **<proveedor actual de 2FA>** e incorporaremos Duo Security como nuestra nueva solución de **autenticación de factor doble** en nuestra infraestructura de TI existente.

Recibirá un correo electrónico de registro de Duo el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**.

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Acción requerida:

No es necesaria una acción inmediata. Este correo electrónico es para notificarle que cambiaremos nuestra autenticación de factor doble de **<proveedor actual de 2FA>** a **Duo Security el <FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**.

¿Por qué Duo Security es una mejor experiencia de usuario?

Con la aplicación móvil gratuita de Duo Security, **Duo Mobile**, ya no es necesario que cargue un token pesado ni pierda el tiempo ingresando un código de acceso al iniciar sesión en una aplicación protegida.

Duo Mobile le permite aprobar rápida y fácilmente una solicitud de autenticación de factor doble en su smartphone a través de **Duo Push.** Si utilizó previamente un token de hardware o código de acceso, **su smartphone ahora lo reemplazará.** Aquí tiene un ejemplo de Duo Push en acción.

¿Por qué necesitamos la autenticación de factor doble?

Las credenciales de inicio de sesión son muy importantes, y cada vez son más fáciles de verse en riesgo. En la actualidad, más del 90 % de las infracciones implican nombres de usuario y contraseñas expuestas a riesgos.

La autenticación de factor doble **mejora la seguridad de su cuenta mediante el uso de un dispositivo secundario para verificar su identidad**. Esto impide que alguien, salvo usted, acceda a su cuenta, incluso si conocen su contraseña.

¿Cómo Duo cambiará mi experiencia de inicio de sesión?

Cuando inicie sesión en una aplicación que esté protegida por Duo, deberá ingresar su nombre de usuario y contraseña. Después de ingresar su información de inicio de sesión, **Duo le pedirá que apruebe una notificación de Duo Push u otro método de autenticación de factor doble**.

Duo no reemplaza ni exige cambiar su nombre de usuario y contraseña. Imagine que Duo es un canal de seguridad adicional a su método de inicio de sesión preexistente. **Pronto tendrá más información sobre el lanzamiento de Duo.**

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Correo electrónico n.º 3: *Duo se presentará el <FECHA> + información de registro. No se necesita realizar ninguna acción en este momento.*

CRONOGRAMA:

3 días antes de la fecha de inicio de envío/aplicación del correo electrónico de registro.

ASUNTO:

Recordatorio: la autenticación de factor doble de Duo reemplazará **<proveedor actual de 2FA>** el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**

CUERPO:

Para mejorar nuestra posición de seguridad y la experiencia actual del usuario con la **autenticación de factor doble**, reemplazaremos **<proveedor actual de 2FA>** e incorporaremos Duo Security como nuestra nueva solución de **autenticación de factor doble** en nuestra infraestructura de TI existente.

Recibirá un correo electrónico de registro de Duo el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>.** Este correo electrónico contiene un **enlace personalizado que le permitirá registrarse con Duo**. Este proceso de autoregistro de 2 minutos hace que sea fácil **registrar su teléfono e instalar la aplicación Duo Mobile.**

Si no tiene un smartphone, puede registrar un teléfono celular regular (SMS y llamadas) o un teléfono fijo (llamadas) para la autenticación de factor doble.

Acción requerida:

No se requiere acción inmediata. Este correo electrónico es para recordarle el próximo cambio en la autenticación de factor doble de **<proveedor actual de 2FA>** a **Duo Security** el **<FECHA DE CORREO ELECTRÓNICO DE REGISTRO>**.

¿Qué es Duo, qué es la autenticación de factor doble, y por qué la necesitamos?

Si se perdió nuestros correos electrónicos anteriores, mire **este video** para obtener más información.

¿Por qué Duo Security es una mejor experiencia de usuario?

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Con la aplicación móvil gratuita de Duo Security, **Duo Mobile**, ya no es necesario que cargue un token pesado ni pierda el tiempo ingresando un código de acceso al iniciar sesión en una aplicación protegida.

Duo Mobile le permite aprobar rápida y fácilmente una solicitud de autenticación de factor doble en su smartphone a través de **Duo Push.** Si utilizó previamente un token de hardware o código de acceso, **su smartphone ahora lo reemplazará.** Aquí tiene un ejemplo de Duo Push en acción.

¿Cómo Duo cambiará mi experiencia de inicio de sesión?

Cuando inicie sesión en una aplicación que esté protegida por Duo, deberá ingresar su nombre de usuario y contraseña. Después de ingresar su información de inicio de sesión, **Duo le pedirá que apruebe una notificación de Duo Push u otro método de autenticación de factor doble**.

Duo no reemplaza ni exige cambiar su nombre de usuario y contraseña. Imagine que Duo es un canal de seguridad adicional a su método de inicio de sesión preexistente.

¿Tiene más preguntas?

Por favor, comuníquese con el **<servicio de asistencia/servicio técnico>** para cualquier pregunta sobre el registro o uso de Duo.

- **Número de teléfono de <servicio de asistencia/servicio técnico>:**
- **Correo electrónico de <servicio de asistencia/servicio técnico>:**

Correo electrónico n.º 4: *Revise su bandeja de entrada para buscar el correo electrónico de registro de Duo. Regístrese ahora.*

CRONOGRAMA:

Día de envío/aplicación de correo electrónico de registro.

ASUNTO:

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Acción requerida: Regístrese en Duo hoy.

CUERPO:

Para mejorar nuestra posición de seguridad y la experiencia actual del usuario con la **autenticación de factor doble**, reemplazaremos **<proveedor actual de 2FA>** e incorporaremos Duo Security como nuestra nueva solución de **autenticación de factor doble** en nuestra infraestructura de TI existente.

Acción requerida:

Hoy recibirá un correo electrónico de registro de Duo Security. Este correo electrónico contiene un **enlace personalizado que le permitirá registrarse con Duo**. Este proceso de autoregistro de 2 minutos hace que sea fácil **registrar su teléfono e instalar la aplicación Duo Mobile.**

Si no tiene un smartphone, puede registrar un teléfono celular regular (SMS y llamadas) o un teléfono fijo (llamadas) para la autenticación de factor doble.

Tendrá hasta **<FECHA DE LA APLICACIÓN + INICIO DE DUO>** para registrarse. Después de esta fecha, el acceso a **<APLICACIÓN>** requerirá la autenticación factor doble de Duo, mientras que la autenticación de factor doble de **<proveedor actual de 2FA>** será desactivada.

¿Qué es Duo, qué es la autenticación de factor doble, y por qué la necesitamos?

Si se perdió nuestros correos electrónicos anteriores, mire **este video** para obtener más información.

¿Por qué Duo Security es una mejor experiencia de usuario?

Con la aplicación móvil gratuita de Duo Security, **Duo Mobile**, ya no es necesario que cargue un token pesado ni pierda el tiempo ingresando un código de acceso al iniciar sesión en una aplicación protegida.

Duo Mobile le permite aprobar rápida y fácilmente una solicitud de autenticación de factor doble en su smartphone a través de **Duo Push.** Si utilizó previamente un token de hardware o código de acceso, **su smartphone ahora lo reemplazará.** Aquí tiene un ejemplo de Duo Push en acción.

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

¿Cómo Duo cambiará mi experiencia de inicio de sesión?

Cuando inicie sesión en una aplicación que esté protegida por Duo, deberá ingresar su nombre de usuario y contraseña. Después de ingresar su información de inicio de sesión, **Duo le pedirá que apruebe una notificación de Duo Push u otro método de autenticación de factor doble**.

Duo no reemplaza ni exige cambiar su nombre de usuario y contraseña. Imagine que Duo es un canal de seguridad adicional a su método de inicio de sesión preexistente.

¿Tiene más preguntas?

Por favor, comuníquese con el **<servicio de asistencia/servicio técnico>** para cualquier pregunta sobre el registro o uso de Duo.

- **Número de teléfono de <servicio de asistencia/servicio técnico>:**
- **Correo electrónico de <servicio de asistencia/servicio técnico>:**

Aviso legal: *asegúrese de leer las plantillas para cerciorarse de que las declaraciones sean precisas a sus casos de uso y método de registro.*

Plantillas de correo electrónico: nueva comunicación de pólizas

Utilice estas plantillas para informar a los usuarios de los próximos cambios de pólizas:

Correo electrónico n. ° 1: *Próximos cambios a la póliza de Duo el <FECHA>. No se requiere acción inmediata.*

CRONOGRAMA:

30 días antes de que se aplique el cambio de póliza.

ASUNTO:

Cambios en el inicio de sesión de Duo 2FA: **<Versión X.XX de OS/navegador/complemento o autenticación biométrica/cifrado de discos/bloqueo de pantalla requerido** a partir **de la FECHA>**

CUERPO:

Para mejorar nuestra posición de seguridad y garantizar el acceso continuo a las aplicaciones protegidas por Duo, pronto le solicitaremos que actualice su **<dispositivo móvil o de acceso>** para satisfacer los siguientes requisitos:

- **A**
- **B**
- **C**

Acción requerida:

No es necesaria una acción inmediata. Este correo electrónico es para notificar y mostrar el próximo cambio para que pueda tomar medidas proactivas si es necesario.

Sin embargo, si desea realizar estos cambios ahora, vea a continuación como:
<incluir instrucciones sobre cómo verificar/activar el cifrado/ biometría/bloquear pantalla o consultar su navegador/complemento/versión del sistema operativo y realizar actualizaciones.>

Correo electrónico n.º 2: *Próximos cambios a la póliza de Duo el <FECHA>. No se requiere acción inmediata.*

CRONOGRAMA:

1 semana antes de que se aplique el cambio de póliza.

ASUNTO:

Recordatorio: próximos cambios en el inicio de sesión de Duo 2FA: **<Versión X.XX del sistema operativo/navegador/complemento o autenticación biométrica/bloqueo de pantalla requerido a partir de FECHA>**

CUERPO:

Para mejorar nuestra posición de seguridad y garantizar el acceso continuo a las aplicaciones protegidas por Duo, pronto le solicitaremos que actualice su **<dispositivo móvil o de acceso>** para satisfacer los siguientes requisitos:

- **A**
- **B**
- **C**

Acción requerida:

No es necesaria ninguna acción inmediata, pero tiene una semana para realizar las actualizaciones necesarias (si es necesario). Este correo electrónico es para notificar y mostrar el próximo cambio para que pueda tomar medidas proactivas si es necesario.

Sin embargo, si desea realizar estos cambios ahora, vea a continuación como:
<incluir instrucciones sobre cómo verificar/activar el cifrado/ biometría/bloquear pantalla o consultar su navegador/complemento/versión del sistema operativo y realizar actualizaciones.

Correo electrónico n.º 3: *Cambios a la póliza de Duo MAÑANA. Actualizaciones de dispositivo/software pueden ser requeridas.*

CRONOGRAMA:

1 día antes de la aplicación de la póliza.

ASUNTO:

Recordatorio: próximos cambios en el inicio de sesión de Duo 2FA sera MAÑANA: las actualizaciones de dispositivo/software pueden ser necesarias o se arriesga a perder el acceso.

CUERPO:

Para mejorar nuestra posición de seguridad y garantizar el acceso continuo a las aplicaciones protegidas por Duo, pronto le solicitaremos que actualice su **<dispositivo móvil o de acceso>** para satisfacer los siguientes requisitos:

- **A**
- **B**
- **C**

Acción requerida:

Por favor, actualice su <dispositivo/software> hoy o perderá acceso a sus aplicaciones.

<incluir instrucciones sobre cómo verificar/activar el cifrado/ biometría/bloquear pantalla o consultar su navegador/complemento/versión del sistema operativo y realizar actualizaciones.