# RECOMENDACIONES DE SEGURIDAD EN HERRAMIENTAS DE REUNIONES VIRTUALES

## Introducción

El presente documento contiene algunas recomendaciones generales de seguridad para herramientas y servicios de videoconferencia a través de Internet, (como Google Meet, Zoom, Microsoft Teams, entre otros).

## Alcance

Las recomendaciones contenidas en este documento son válidas para aplicaciones de videoconferencia, reuniones, streaming, salas virtuales de clase y videollamadas.

## Análisis de seguridad al momento de escoger una plataforma o servicio

Una vez se tienen claras las necesidades funcionales para realizar un primer análisis sobre la plataforma, aplicativo o servicios es necesario tener en cuenta tres factores:

1. **La seguridad que brinda la plataforma**: Verificar directamente en el sitio Web del fabricante o desarrollador la seguridad que brinda su producto, es importante tener en cuenta si el producto contará con actualizaciones de seguridad y hasta dónde llega su cubrimiento, esto es importante para la gestión, actualización y mantenimiento de la plataforma tecnológica de la Universidad.
2. **Las vulnerabilidades activas y la velocidad para solucionarlas**: La mayoría de vulnerabilidades más críticas que se encuentran publicadas, son las que las empresas se centran en solucionar, en este sentido y por el auge de este tipo de herramientas se solucionan más rápidamente; sin embargo, vale la pena recordar que no siempre se realizarán en el menor tiempo posible, además existen vulnerabilidades que no son públicas y otras que intentan aprovecharse de los usuarios menos informados en los temas de seguridad, como los casos de phishing, suplantando los enlaces a reuniones oficiales por reuniones falsas incluso suplantando los ejecutables originales por otros modificados.
3. **El tipo de usuario y el uso que se le dará a la herramienta**: Es necesario definir los tipos de usuarios que emplearán la herramienta y diferenciar si es necesario que algunos tengan mayor conocimiento para administrar el servicio de los conocimientos generales requeridos para usar la aplicación. Lo anterior siguiendo las políticas y directrices institucionales de seguridad para poder gestionar los riesgos que pueden existir y si se está dispuesto a asumirlos para determinar el uso de la aplicación o el servicio.

Por lo tanto debido al constante avance de las tecnologías ninguna herramienta de videoconferencia es 100% segura, sin embargo si se tienen claras las necesidades de uso de la herramienta y se realiza un análisis detallado es posible determinar las mejores prácticas de uso necesarias para mantener la seguridad y privacidad de la información.



Carrera 45 No. 26-85
Edificio Uriel Gutiérrez, 4° piso, Oficina 460
Teléfono (57-1) 3165000 extensión 18197
Bogotá, Colombia
dned@unal.edu.co

**Recomendaciones**

Por lo anteriormente expuesto, se recomienda antes que nada definir las necesidades funcionales de la herramienta, y escoger la herramienta que cumpla con los criterios de seguridad definidos, en este sentido es de recordar que la información institucional tiene una clasificación y los riesgos deben ser evaluados con base a esta.

Antes de evaluar una nueva herramienta se aconseja verificar si la Universidad ya cuenta con aplicaciones similares, para este caso se hace necesario recordar que la Universidad dispone de Google Apps, por lo que se aconseja el uso de las herramientas institucionales sobre cualquier otro tipo de herramienta, salvo que se realicen los respectivos análisis de seguridad de la información y cumplan con las políticas y directrices internas.

En caso de que un área, dependencia, oficina, entre otras, decida usar una herramienta diferente, debe cumplir con cada uno de los lineamientos y políticas de seguridad definidas por la Universidad, y la operación, mantenimiento, soporte y responsabilidad queda a cargo de la persona u oficina que adquiera el producto, es importante aclarar que las oficinas de tecnologías no darán soporte técnico.

Recomendaciones generales de seguridad:

- Control de los datos
    - Los propietarios de los datos deben ser la Universidad, no el intermediario, la empresa, fabricante o desarrollador del producto o servicio.
    - Que el intermediario, la empresa, fabricante o desarrollador del producto o servicio no utiliza los datos de la Universidad con fines publicitarios ni venda o ceda esta información a terceros.
    - Los datos de la Universidad se envían cifrados y las grabaciones realizadas por la Universidad serán almacenadas con cifrado de forma predeterminada.
    - Que el servicio o producto no contenga funciones ni software que realicen recolección de datos no autorizados de los usuarios.
    - Poder configurar políticas de conservación para las grabaciones, así, cumplir con las obligaciones legales.
- Verificar si el producto o servicio es sometido regularmente a controles de seguridad, privacidad y cumplimiento, es decir que cuente con certificaciones de cumplimiento en estándares de seguridad o informes de auditoría de acuerdo con estándares globales (como por ejemplo ISO/IEC 27001 y/o ISO/IEC 27017 y/o ISO/IEC 27018 y/o FedRAMP y/o HIPAA, HITRUST CSF y/o RGPD y/o Marco del Escudo de la privacidad (UE-EE. UU. y Suiza-EE. UU.) y/o BSI C5 (EMEA), ENS alto (España) y/o MTCS de nivel 3 (Singapur) y/o OSPAR (Asia-Pacífico) y/o CSA STAR. dependiendo de la funcionalidad)
- Cifrado: Para asegurar la seguridad y la privacidad de los datos
    - De forma predeterminada, todos los datos de se envían cifrados entre la universidad y el fabricante o desarrollador del producto o servicio en las videollamadas hechas tanto desde navegadores web como desde las aplicaciones para dispositivos móviles y de escritorio, así como en las que se hacen en salas de reuniones


Carrera 45 No. 26-85
Edificio Uriel Gutiérrez, 4° piso, Oficina 460
Teléfono (57-1) 3165000 extensión 18197
Bogotá, Colombia
dned@unal.edu.co

mediante el hardware de salas de reuniones del fabricante o desarrollador.
    - En caso de unirse una videollamada por teléfono, el audio utilizará la red de un operador y el cifrado que el mismo operador ofrezca para la transmisión de datos por lo que su uso deberá limitarse o en caso de ser considerado tener en cuenta los posibles riesgos asociados
    - Las grabaciones almacenadas deben estar cifradas en reposo de forma predeterminada.
    - Cumplir con los estándares de seguridad de Internet Engineering Task Force (IETF) sobre la seguridad en la capa de transporte de datagramas (DTLS) y el protocolo de transporte en tiempo real seguro (SRTP).
- Medidas contra el uso inadecuado: implementar medidas contra el uso inadecuado para proteger tus reuniones, como los controles contra intrusos, tanto si se trata de videollamadas web como de llamadas telefónicas. Estas son algunas de las medidas básicas clave que se deben tener en cuenta en el navegador web y aplicaciones:
    - Códigos de reuniones: cada código de reunión tiene mínimo 10 caracteres aplicando las recomendaciones de contraseñas seguras de la política de seguridad. De este modo, es más difícil adivinar los códigos de reunión.
    - Detalles de la reunión: se pueden cambiar en la invitación. Al cambiar completamente la invitación a una videollamada, se modifican el código de la reunión y el PIN del teléfono. Esta opción resulta especialmente útil si un usuario ya no forma parte de la invitación a la reunión.
    - Protección ante la reutilización de reuniones finalizadas: los participantes de las reuniones no pueden volver a unirse a ellas después de que se haya ido el último participante, a menos que tengan privilegios de creación para iniciar una nueva reunión. Esto significa que, el creador de la reunión es el único que puede reiniciar una reunión
    - Unirse a una reunión: cuando se unen personas a una videollamada, se deben aplicar las siguientes restricciones:
        - Los participantes externos sólo pueden unirse directamente si están incluidos en la invitación del calendario o si el administrador de la reunión lo agrega.
        - El resto de participantes externos deben enviar una solicitud para unirse a la reunión y un miembro de la organización que ha creado la llamada debe aceptarla si así lo considera, sin embargo la recomendación es que desde un principio se definan los asistentes.
        - Incorporar la capacidad de que el administrador de la reunión pueda retirar a un asistente de una reunión, para un mayor control sobre el comportamiento no deseado durante las reuniones.
    - En telefonía
        - PINs de reuniones: los PIN deben tener 9 dígitos o más.
        - Detalles de la reunión: las combinaciones de número de teléfono y PIN solo deben ser válidas a la hora programada para la reunión.


Carrera 45 No. 26-85
Edificio Uriel Gutiérrez, 4° piso, Oficina 460
Teléfono (57-1) 3165000 extensión 18197
Bogotá, Colombia
dned@unal.edu.co

        - Unirse a una reunión por teléfono: de ser necesaria esta funcionalidad debe tener la posibilidad de que los participantes puedan unirse por teléfono.
- Implementación, acceso y controles seguros: para mantener la privacidad y la seguridad de tus datos:
    - Acceso a la plataforma o servicio:
        - Mediante web se debe permitir a los usuarios conectarse desde Chrome, Mozilla Firefox, Apple Safari y el nuevo Microsoft Edge idealmente sin la necesidad de instalar ningún complemento ni software. De este modo se limitan las posibilidades de ataque y se reduce el número de parches de seguridad que sería necesario aplicar en los equipos del usuario final.
        - En los dispositivos móviles, se recomienda que se instale la aplicación desde las tiendas oficiales
    - Verificación en dos pasos: la plataforma o servicio debe ser compatible con varias opciones de verificación en dos pasos: llaves de seguridad, algún autenticador, mensajes de correo, SMS entre otros.
    - Debe contar con algún Programa de Protección Avanzada: Este programa ofrece medidas de protección contra el phishing y la interceptación de cuentas.
    - Métodos de autenticación adicionales: disponer del inicio de sesión único (SSO). Además, usar la autenticación multifactor (MFA)
    - Registros: el registro de auditoría del producto o servicio debe estar disponible en la consola de administración
    - Acceso al registro: debe registrar cualquier acceso de los administradores a las grabaciones almacenadas, junto con el motivo del acceso.
- Respuesta a incidentes: La gestión de incidentes es un aspecto importante de seguridad y privacidad, es clave para cumplir con las normativas globales sobre privacidad, como el RGPD.
    - Prevención de incidentes
        - Análisis automatizado de registros de redes y sistemas por parte del fabricante o desarrollador del producto o servicio: el análisis automatizado del tráfico de red y del acceso al sistema ayuda a identificar actividades sospechosas, inadecuadas o no autorizadas
        - Pruebas por parte del fabricante o desarrollador del producto o servicio: el equipo de seguridad del desarrollador o fabricante analiza de forma activa las amenazas de seguridad mediante pruebas de penetración, medidas de control de calidad, detección de intrusiones y revisiones de seguridad del software de su producto o servicio.
        - Revisiones del código interno por parte del fabricante o desarrollador del producto o servicio: la revisión del código fuente permite descubrir vulnerabilidades ocultas y fallos de diseño, y verificar si se han implementado los controles de seguridad.
    - Detección de incidentes por parte del fabricante o desarrollador del producto o servicio
        - Contar con herramientas y procesos específicos del producto: se utilizan herramientas automatizadas siempre


Carrera 45 No. 26-85
Edificio Uriel Gutiérrez, 4° piso, Oficina 460
Teléfono (57-1) 3165000 extensión 18197
Bogotá, Colombia
dned@unal.edu.co

que sea posible para mejorar la capacidad de detectar incidentes a nivel de producto.
        - Detección de anomalías de uso: utilizar muchas capas de sistemas de aprendizaje automático para diferenciar entre la actividad de usuario segura y la anómala en navegadores, dispositivos, inicios de sesión de aplicaciones y otros eventos de uso.
        - Alertas de seguridad sobre servicios de centros de datos o lugares de trabajo: las alertas de seguridad de los centros de datos buscan incidentes que puedan afectar a la infraestructura.
    - Respuesta a incidentes por parte del fabricante o desarrollador del producto o servicio
        - Incidentes de seguridad: Contar con un programa de respuesta a incidentes que ofrezca mínimo las siguientes funciones clave:
            - Sistemas de supervisión, analíticas de datos y servicios de aprendizaje automático que detectan y limitan incidentes de forma proactiva.
            - Expertos en la materia que se dedican a responder a cualquier tipo o tamaño de incidentes relacionados con los datos.
            - Un proceso bien desarrollado para notificar al instante a la universidad en caso de ser afectados.
- Usar siempre la última versión disponible de la aplicación, software o plataforma, ya que el uso de versiones desactualizadas es foco potencial de vulnerabilidades.
- Utilizar solo los instaladores oficiales distribuidos por los medios oficiales, los instaladores conseguidos por diferentes medios aunque parezcan oficiales pueden aumentar el riesgo de que incluyen amenazas
- Se recomienda no dejar abierto el ingreso a participantes nuevos en las conferencias, a menos que el administrador les permita entrar, de este modo se reduce el riesgo.
- Habilitar estos servicios bajo un perfil que requiera contraseña o un PIN para ingresar y no dejarlo público.
- Mantener actualizados los sistemas operativos de los dispositivos para contar con los parches de seguridad más recientes.
- Se recomienda que al realizar una grabación de una reunión se le debe manejar de acuerdo al perfil de clasificación de información de la Universidad
- Seguir las recomendaciones de seguridad oficiales del aplicativo, herramienta, producto o servicio.
- Evitar compartir masivamente los links de invitación a la sesión
- Las sesiones deben tener contraseña.



Carrera 45 No. 26-85
Edificio Uriel Gutiérrez, 4° piso, Oficina 460
Teléfono (57-1) 3165000 extensión 18197
Bogotá, Colombia
dned@unal.edu.co