Descripción de las capacidades de riesgo interno en Microsoft Purview

Descripción de la gestión de riesgos internos

Nota

El Cumplimiento de Microsoft 365 ahora se denomina Microsoft Purview y las soluciones dentro del área de cumplimiento se han cambiado de marca. La Administración de riesgos internos en Microsoft 365 ahora es la Administración de riesgos internos en Microsoft Purview. Para más información sobre Microsoft Purview, vea el **anuncio del blog**.

Administración de riesgos internos de Microsoft Purview es una solución que ayuda a minimizar los riesgos internos, ya que permite a una organización detectar, investigar y actuar sobre actividades peligrosas y malintencionadas. La administración de riesgos internos está disponible en el Portal de cumplimiento de Microsoft Purview.

La administración y reducción del riesgo en una organización comienza con la comprensión de los tipos de riesgos que se encuentran en el área de trabajo moderna. Algunos riesgos están controlados por eventos y factores externos y están fuera del control directo de una organización. Otros riesgos están impulsados por eventos internos y actividades de empleados que se pueden eliminar y evitar. Algunos ejemplos son los riesgos de acciones y comportamiento ilegales, inadecuados, no autorizados o no éticos por parte de los empleados y los administradores. Estos comportamientos pueden conducir a una amplia gama de riesgos internos de los empleados:

- Fugas de datos confidenciales y pérdida de datos
- Infracciones de confidencialidad
- Robo de propiedad intelectual (IP)
- Fraude
- Transacciones internas
- Infracciones de cumplimiento normativo

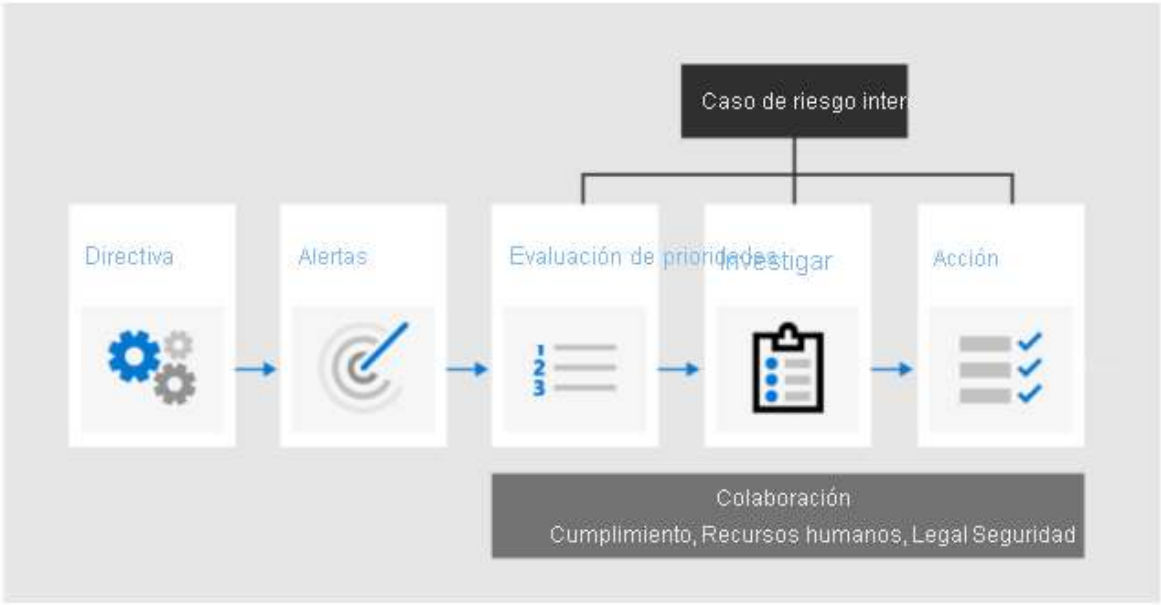
La administración de riesgos internos se centra en los siguientes principios:

- **Transparente**: equilibre la privacidad del usuario frente al riesgo de la organización con la arquitectura de privacidad por diseño.
- **Configurable**: directivas configurables basadas en grupos industriales, geográficos y empresariales.
- **Integrada**: flujo de trabajo integrado entre soluciones de Microsoft Purview.
- **Accionable**: proporciona información para habilitar las notificaciones de usuario, las investigaciones de datos y las investigaciones de usuario.

Flujo de trabajo de administración de riesgos internos

La administración de riesgos internos ayuda a las organizaciones a identificar, investigar y abordar los riesgos internos. Con las plantillas de directiva enfocadas, la señal de actividad completa en

Microsoft 365 y un flujo de trabajo flexible, las organizaciones pueden aprovechar la información accionable para ayudar a identificar y resolver rápidamente el comportamiento arriesgado. La identificación y resolución de las actividades de riesgo interno y los problemas de compatibilidad con la administración de riesgos internos en Microsoft Purview se consigue mediante el siguiente flujo de trabajo:



- **Directivas**: las directivas de administración de riesgos internos se crean mediante plantillas predefinidas y condiciones de directivas que definen qué indicadores de riesgo se examinan en áreas de características de Microsoft 365. Estas condiciones incluyen cómo se usan los indicadores para las alertas, qué usuarios están incluidos en la directiva, qué servicios están clasificados por orden de prioridad y el período de supervisión.
- **Alertas**: los indicadores de riesgo generan automáticamente alertas que coinciden con las condiciones de la directiva y se muestran en el **Panel de alertas**. Este panel habilita una vista rápida de todas las alertas que necesitan revisión, las alertas abiertas a lo largo del tiempo y las estadísticas de alertas de la organización.
- **Evaluación de prioridades**: las nuevas actividades que necesitan investigación generan automáticamente alertas a las que se les asigna un estado de *Necesita revisión*. Los revisores de la organización pueden identificar rápidamente estas alertas y desplazarse por cada una de ellas para evaluarlas y evaluar las prioridades. Las alertas se resuelven abriendo un nuevo caso, asignando la alerta a un caso existente o descartando la alerta. Como parte del proceso de evaluación de prioridades, los revisores pueden ver los detalles de la alerta para la coincidencia de la directiva, la actividad de usuario asociada con la coincidencia y la gravedad de la alerta, así como revisar la información de perfil de usuario.
- **Investigación**: los casos se crean para las alertas que requieren una revisión y una investigación más detalladas de la información y las circunstancias de la coincidencia de la directiva. El **Panel de casos** proporciona una vista general de todos los casos activos, los

casos abiertos a lo largo del tiempo y las estadísticas de casos de la organización. Al seleccionar un caso en el panel, se abre para su investigación y revisión. Esta área es donde las actividades de riesgo, las condiciones de la directiva, los detalles de las alertas y los detalles del usuario se sintetizan en una vista integrada para los revisores.

- **Acción**: después de investigar los casos, los revisores pueden actuar rápidamente para resolver el caso o colaborar con otras partes interesadas de riesgo de la organización.
    - Las acciones pueden ser tan simples como enviar una notificación cuando los empleados infrinjan las condiciones de la directiva accidental o involuntariamente.
    - En casos más serios, es posible que los revisores necesiten compartir la información de los casos de administración de riesgos internos con otros revisores de la organización. La remisión de un caso para la investigación permite transferir datos y la administración del caso a eDiscovery (Premium) en Microsoft Purview.

La administración de riesgos internos puede ayudarle a detectar, investigar y tomar medidas para mitigar los riesgos internos de la organización en varios escenarios comunes. Estos escenarios incluyen el robo de datos por parte de los empleados, la fuga intencional o accidental de información confidencial, el comportamiento ofensivo, etc.

Descripción del cumplimiento de comunicaciones

Nota

El Cumplimiento de Microsoft 365 ahora se denomina Microsoft Purview y las soluciones dentro del área de cumplimiento se han cambiado de marca. El Cumplimiento de comunicaciones en Microsoft 365 es ahora el Cumplimiento de comunicaciones en Microsoft Purview. Para más información sobre Microsoft Purview, vea el **anuncio del blog**.

El Cumplimiento de comunicaciones en el Portal de cumplimiento de Microsoft Purview ayuda a minimizar los riesgos de comunicación, ya que permite a las organizaciones detectar, capturar y realizar acciones de corrección para mensajes inadecuados. Las directivas predefinidas y personalizadas en el cumplimiento de comunicaciones permiten examinar las comunicaciones internas y externas de las coincidencias de directivas para que puedan examinarlas los revisores elegidos.

La identificación y resolución de problemas de compatibilidad con el Cumplimiento de comunicaciones en Microsoft Purview utiliza el siguiente flujo de trabajo:

- **Configuración**: en este paso, los administradores identifican los requisitos de cumplimiento y configuran las directivas de cumplimiento de comunicaciones aplicables.
- **Investigación**: los administradores tienen un análisis más profundo de los problemas detectados cuando coinciden con las directivas de cumplimiento de comunicaciones. Herramientas y pasos que ayudan a incluir alertas, administración de problemas para ayudar a corregir, revisar documentos, revisar el historial de usuarios y los filtros.
- **Corrección**: corrija los problemas de cumplimiento de comunicaciones. Entre las opciones se incluyen resolver una alerta, etiquetar un mensaje, notificar al usuario, remitir a otro revisor, marcar una alerta como falso positivo, quitar un mensaje de Teams y emitir para la investigación.
- **Supervisión**: el mantenimiento del seguimiento y la administración de los problemas de cumplimiento identificados por las directivas de cumplimiento de comunicaciones abarca todo el proceso del flujo de trabajo. Los widgets del panel de cumplimiento de comunicaciones, los registros de exportación y los eventos registrados en los registros de auditoría unificados se pueden usar para evaluar y mejorar continuamente su postura de cumplimiento.

El cumplimiento de comunicaciones permite a los revisores investigar correos electrónicos examinados y mensajes en Microsoft Teams, Exchange Online, Yammer o comunicaciones de terceros en una organización, con las acciones de corrección adecuadas para asegurarse de que cumplen con los estándares de mensajes de la organización.

Algunas áreas de cumplimiento importantes en las que las directivas de cumplimiento de la comunicación pueden ayudar con la revisión de mensajes incluyen:

- **Directivas corporativas**: los usuarios deben seguir las directivas corporativas, como el uso y los estándares éticos, en sus comunicaciones empresariales cotidianas. Con el cumplimiento de comunicaciones, los administradores pueden examinar las comunicaciones de los usuarios en la organización en busca de posibles preocupaciones de lenguaje ofensivo o acoso.

- **Administración de riesgos**: el cumplimiento de comunicaciones puede ayudar a los administradores a analizar la comunicación no autorizada de los proyectos que se consideran confidenciales, como las adquisiciones, la divulgación de ganancias y mucho más.
- **Cumplimiento normativo**: se espera que la mayoría de las organizaciones sigan algunas normas de cumplimiento normativo durante sus operaciones cotidianas. Por ejemplo, un reglamento puede requerir que las organizaciones revisen las comunicaciones de sus agentes para protegerse frente a posibles transacciones internas, blanqueo de dinero o soborno. El cumplimiento de comunicaciones permite a la organización examinar estos tipos de comunicaciones, así como informar sobre ellos, de forma que cumplan sus requisitos.

Vea el vídeo siguiente para consultar un tutorial sobre el Cumplimiento de comunicaciones de Microsoft Purview.

https://www.microsoft.com/es-mx/videoplayer/embed/RE4xlaF?postJsllMsg=true&autoCaptions=es-mx

Nota

La interfaz de usuario (UI) de Microsoft 365 está evolucionando continuamente, por lo que es posible que la interfaz de usuario que se muestra en el vídeo no refleje las actualizaciones más recientes.

El cumplimiento de comunicaciones es una herramienta eficaz que puede ayudar a mantener y proteger al personal, los datos y la organización.

Descripción de las barreras de información

Nota

El Cumplimiento de Microsoft 365 ahora se denomina Microsoft Purview y las soluciones dentro del área de cumplimiento se han cambiado de marca. Barreras de información en Microsoft 365 ahora es Barreras de información en Microsoft Purview. Para más información sobre Microsoft Purview, vea el **anuncio del blog**.

Microsoft 365 proporciona a las organizaciones capacidades eficaces de comunicación y colaboración. Sin embargo, es posible que una organización quiera restringir las comunicaciones entre algunos grupos para evitar que se produzca un conflicto de interés en la organización o para restringir la comunicación entre ciertas personas para proteger la información interna. Con barreras de información, la organización puede restringir las comunicaciones entre grupos de usuarios específicos.

La característica de Barreras de información en Microsoft Purview se admite en Microsoft Teams, SharePoint Online y OneDrive para la Empresa.

Las barreras de la información son directivas que los administradores pueden configurar para impedir que personas o grupos se comuniquen entre sí. Cuando se aplican directivas de barrera de información, las personas que no deben comunicarse con otros usuarios específicos no pueden encontrar ni seleccionar esos usuarios, así como tampoco chatear con ellos ni llamarlos. Con las barreras de información, las comprobaciones están en vigor para evitar la comunicación no autorizada.

Nota

Es importante tener en cuenta que las barreras de información *solo admiten restricciones bidireccionales*. Las restricciones unidireccionales, como marketing, pueden comunicarse con los comerciantes del día, pero *no se admiten* los comerciantes del día que no pueden comunicarse con el departamento de marketing.

Estos son algunos ejemplos de cómo se pueden aplicar barreras de información:

- **Educación**: los alumnos de una escuela no pueden buscar información de contacto de estudiantes de otras escuelas.
- **Legal**: mantenimiento de la confidencialidad de los datos obtenidos por el abogado de un cliente para evitar el acceso de un abogado de la misma empresa que representa a otro cliente.
- **Servicios profesionales**: un grupo de personas de una empresa solo puede chatear con un cliente o un cliente específico a través de la federación o el acceso de invitado durante una interacción con el cliente.

Barreras de la información en Microsoft Teams

En Microsoft Teams, las directivas de barreras de información determinan y evitan los siguientes tipos de comunicaciones no autorizadas:

- Búsqueda de un usuario
- Adición de un miembro a un equipo
- Inicio de una sesión de chat con alguien
- Inicio de un chat de grupo
- Invitación para que un usuario se una a una reunión
- Uso compartido de una pantalla
- Realización de una llamada
- Uso compartido de un archivo con otro usuario
- Acceso al archivo a través del vínculo de uso compartido

Si las personas implicadas se incluyen en una directiva de barreras de información para evitar la actividad, no podrán continuar. Potencialmente, se puede impedir que todos los usuarios incluidos en una directiva de barreras de información se comuniquen con otros usuarios de Microsoft

Teams. Cuando los usuarios afectados por las directivas de barreras de información forman parte del mismo equipo o chat de grupo, es posible que se quiten de esas sesiones de chat y que no se permita la comunicación adicional con el grupo.

Para obtener más información sobre la experiencia del usuario con barreras de información, vea Barreras de información en Microsoft Teams.