Gobernanza del Dato Microsoft 365

integra

"Trabajando en el ahora con visión del mañana"

www.integratecnologia.es

1.

INTRODUCCIÓN Y ALCANCE DEL PROTOTIPO

INTRODUCCIÓN

Objetivo del prototipo

El presente documento resume los pasos a realizar para **asegurar el entorno del cliente y empoderar a los responsables de la gestión de los accesos y la información** de forma que puedan conocer y gestionar correctamente. Se identifican las siguientes necesidades:

- Un **análisis inicial de las necesidades** en materia de seguridad de los accesos y la información.
- Una segunda fase consistente en **la configuración de las herramientas** según los requisitos que se hayan acordado previamente en la fase anterior.
- **Formación** a los responsables del servicio para conocer y gestionar las soluciones.
- **Soporte y apoyo a los usuarios y administradores** para facilitar la transición del servicio y descargar al equipo técnico del cliente de las consultas de los usuarios

ANÁLISIS Y VALIDACIÓN
Conocimiento de las necesidades del cliente

CONFIGURACIÓN
Configuración del entorno para adaptarlo a las necesidades encontradas

FORMACIÓN A MEDIDA
Capacitación al equipo técnico del cliente

FASE DE SOPORTE Y MEJORAS
Soporte técnico ante incidencias y CAU para usuarios finales

integra

INTRODUCCIÓN

Ventajas M365

Todo el ecosistema de M365 se sienta sobre el pilar básico de la **seguridad** a diferentes niveles como:

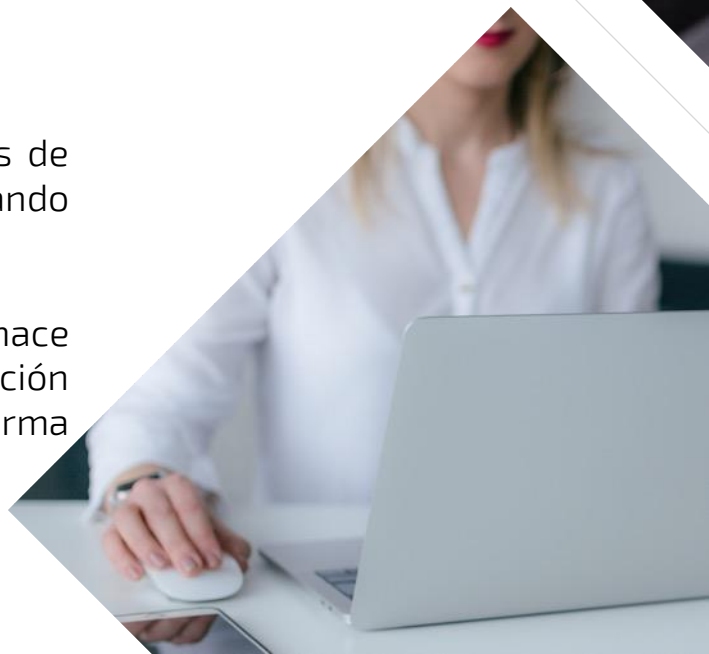
Datos: proporcionando servicios de encriptación, versionado y garantizando la confidencialidad de la información con sistemas como **Azure Information Protection**, incluso cuando la información no se encuentra alojada en la nube Microsoft, **Data Loss Prevention** para evitar fugas de información no deseadas, o **Advanced Threat Protection** que permite detener amenazas avanzadas utilizando sistemas de inteligencia artificial para detectarlas.

Accesos: Usando soluciones como **MFA, SSO y Azure AD** se consigue una gestión de la identidad única, facilitando la gestión, evitando el fallo humano y asegurando los accesos a las aplicaciones de Microsoft y terceros.

Cumplimiento: Alojando los datos en territorio Europeo sin perder la alta disponibilidad geográfica.

Dispositivos y sistemas: Con herramientas como **Intune** para gestionar equipos y dispositivos móviles de forma centralizada, permitiendo aplicar políticas unificadas, incluso en dispositivos fuera de la red, evitando posibles focos de problemas.

Usuarios: Usando soluciones "Shadow IT" como **Cloud App Security** que permite controlar el uso que se hace de la información y las aplicaciones, advirtiendo o impidiendo al usuario antes de realizar una mala acción automáticamente y ofreciendo a los administradores un único panel de gestión donde visualizar de forma gráfica las incidencias.



https://www.microsoft.com/es-es/security/business

integra

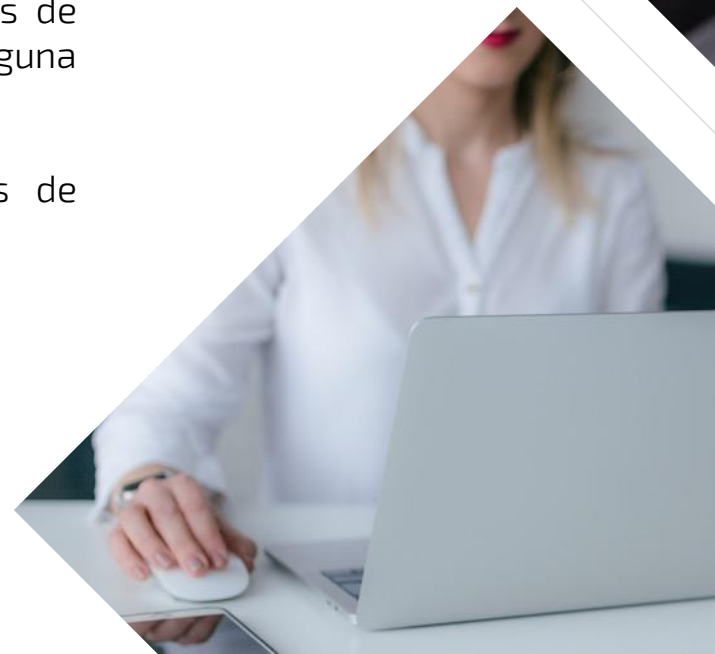
INTRODUCCIÓN
Soluciones M365

Advanced Threat Protection (ATP). Permite aplicar una capa de seguridad adicional correo electrónico de las cuentas alojadas en Office 365:

- **Vínculos seguros**: protege de forma preventiva los usuarios de los hipervínculos malintencionados en un mensaje. La protección permanece cada vez haga clic en el vínculo, como vínculos malintencionados se bloquean dinámicamente.

- **Datos adjuntos seguros:** protegen contra los virus y códigos dañinos y proporcionan protección de día cero para proteger el sistema de mensajería. Todos los mensajes y datos adjuntos que no tienen una firma de virus/código dañino conocida se enrutan a un entorno especial donde ATP usa diversas técnicas de análisis y aprendizaje automático para detectar intentos malintencionados. Si no se detecta ninguna actividad sospechosa, se libera el mensaje para su entrega al buzón de correo.

- **Capacidades avanzadas contra suplantación de identidad**: Esta característica utiliza modelos de aprendizaje de máquina para detectar los mensajes de suplantación de identidad.



integra

INTRODUCCIÓN
Soluciones M365

Data Loss Prevention (DLP): Las directivas de prevención de pérdida de datos (DLP) ayudan a identificar y proteger la información confidencial de nuestra organización.
Con una directiva DLP, podemos:

- Identificar información confidencial en varias ubicaciones, como Exchange Online, SharePoint Online, OneDrive para la empresa y Microsoft Teams.
- Evitar el uso compartido accidental de información confidencial.
- Ver informes de DLP que muestran contenido que coincide con las directivas DLP de la organización.

Etiquetas de confidencialidad: Permiten clasificar y de manera opcional, proteger los documentos y correos mediante la aplicación de etiquetas.

- Estas etiquetas además de permitir clasificar y proteger la información, permiten añadir distintos visuales a los documentos, como marcas de agua, encabezados o pies de página.
- Las etiquetas se agregan como metadatos a los archivos y encabezados de correo en texto no cifrado, y permanecerán con la información independientemente de dónde se encuentre.

integra

INTRODUCCIÓN
Soluciones M365

Microsoft Intune: Intune es un servicio de administración de la movilidad empresarial basado en la nube que se centra en la administración de dispositivos (MDM) y la administración de aplicaciones (MAM).
Con Intune podemos definir políticas de configuración y administración de los dispositivos y aplicaciones, como por ejemplo:

- Realizar borrados o bloqueos remotos.
- Decidir desde qué S.O. se puede acceder a los servicios.
- Aplicar condiciones al acceso a los recursos.
- Disponer de un antivirus actualizado.
- Realizar instalaciones remotas de aplicaciones, etc.

Acceso Condicional de Azure: Mediante el uso de directivas de acceso condicional pueden aplicarse los controles de acceso correctos cuando sea necesario para mantener la organización segura y no interferir con los usuarios cuando no se necesita.
Las directivas de acceso condicional son instrucciones if-then; si un usuario desea tener acceso a un recurso, deben completar una acción, por ejemplo: un usuario de administración desea acceder a la aplicación de nóminas y es necesario realizar la autenticación multifactor para tener poder hacerlo.

integra

2.

PLANIFICACIÓN

Administración Microsoft 365

PLANIFICACIÓN

Objetivos principales

Se presenta la siguiente planificación estudiada con los siguientes objetivos principales:

- Tener el menor impacto en la productividad del usuario
- Incrementar la seguridad de los accesos a las aplicaciones y datos
- Dar a conocer las posibilidades que ofrece M365 en materia de seguridad empoderando a los responsables de su gestión.

Para esto se tienen en cuenta los siguientes factores y consideraciones:

Calidad: Consideramos este factor de gran importancia, por lo que se cuidará que las actuaciones se realicen de forma profesional por personal experto.

Accesos: Se deberán tramitar y facilitar los accesos necesarios para realizar los servicios al personal técnico de Integra asignado

Documentación: En coordinación con el cliente se mantendrán documentadas todas las actuaciones realizadas, así como una documentación final del entorno configurado.

integra

PLANIFICACIÓN

Arranque y análisis

Una vez adjudicado el prototipo, como primer paso, se efectuará una **reunión de lanzamiento** donde se presentará al responsable de prototipo y equipo técnico asignado y se revisará junto con los responsables de prototipo del cliente entre otros aspectos:

- Presentación y composición del equipo de trabajo por ambas partes.
- Los objetivos y plazos principales a cubrir con el prototipo.
- Se identificarán los procedimientos generales de trabajo y comunicación durante el prototipo.
- Definición de hitos y composición del calendario de prototipo.

La **primera fase**, consiste en analizar las necesidades relativas a la seguridad y gobernanza necesarias dentro de la organización. Esta información se completará en una reunión técnica específica para definir las políticas de Intune a aplicar y se plasmar en un mapa conceptual de necesidades

1 jornada

Equipo cliente
Equipo Integra

integra

PLANIFICACIÓN

Preparación del entorno

Se proponen las siguientes configuraciones estándar que, en base a la experiencia obtenida de otros prototipos, pueden ser necesarias. Así pues se estima:

- **Advanced Threat Protection (ATP).** Configuración e implementación de 3 directivas: vínculos seguros, adjuntos seguros y suplantación de identidad. Para llevar a cabo la implementación se requerirá que el cliente proporcione datos concretos sobre las necesidades de la implementación.

- **Data Loss Prevention (DLP).** Configuración e implementación de directiva DLP para la identificación de información confidencial y/o bloqueo del uso compartido accidental. Para llevar a cabo la implementación se requerirá que el cliente proporcione datos concretos sobre las necesidades de la implementación.

- **Etiquetas de confidencialidad**. Configuración de 5 etiquetas de Confidencialidad. El cliente deberá indicar a Efor las características de las etiquetas a configurar (ámbito de aplicación, características de protección, etc.). Se proporcionará una formación de 1 hora a un máximo de 5 usuarios sobre el uso de las etiquetas. Entregables: Guías de usuario sobre etiquetas de confidencialidad y cifrado de correo.

2 semanas

Esp. M365

integra

PLANIFICACIÓN

Preparación del entorno

Microsoft Intune + acceso condicional Azure. Configuración e implementación de entorno base aplicado a 6 usuarios y/o 12 dispositivos, incluyendo:

- Despliegue de un máximo de 3 perfiles de configuración seguros/líneas base seguridad sobre dispositivos (max 10 políticas estándar).
- Configuración y despliegue controlado de aplicaciones sobre dispositivos (max. 10 aplicaciones Store).
- Configuración de políticas de acceso condicional para el control de acceso a aplicaciones (max. 3).
- En remoto, inscripción de dispositivos y despliegue piloto de perfiles de configuración sobre grupo usuarios.
- En remoto, formación online (2h) equipo IT (max. 5 usuarios). Resolución de dudas y documentación de la solución aplicada.

De forma opcional se valora el despliegue de la solución sobre el resto de los dispositivos de la organización.

2 semanas

Esp. M365

integra

PLANIFICACIÓN

Formación seguridad IT

Adicionalmente se plantea una **formación específica de seguridad** a los responsables de IT en formato taller para grupos de hasta 5 personas con una duración de 5h aprox.

1. Configuraciones de seguridad en Office 365
   a) Autenticación Multifactor (MFA)
   b) Autoservicio de restablecimiento de contraseña
   c) Directiva de expiración de contraseñas
   d) Control de acceso a invitados en herramientas colaborativas: SharePoint y Microsoft Teams
   e) Directivas de uso compartido y control de acceso en SharePoint y OneDrive. Opciones de sincronización
2. Configuraciones de seguridad en Azure Active Directory
   a) Métodos de autenticación. Protección con contraseña.
   b) Personalización de marca de empresa
3. Gestión y administración de soluciones de seguridad de O365
   a) Centro de Seguridad y Cumplimiento de O365
      - Visión Global
      - Gestión de permisos y alertas
      - Clasificación de la información. Gobernanza en O365
        - Etiquetas de confidencialidad
        - Etiquetas de retención
        - Prevención contra la pérdida de datos (DLP)
      - Administración de Amenazas.
      - Directivas (incluye reglas correo)
      - eDiscovery
      - Informes
   b) Microsoft Intune. Directivas de acceso condicional

1 jornada

Equipo IT cliente
Equipo Integra

PLANIFICACIÓN

Documentación y soporte

Una vez terminada la configuración se activará un periodo de **soporte** destinado a solventar las incidencias que puedan surgir relacionadas con los elementos analizados en esta propuesta y realizado por el mismo equipo técnico implicado en el prototipo.

El soporte se efectuará de forma telemática preferentemente, en horario de oficina y tendrá una **duración de 1 mes** desde la fecha de finalización de la configuración.

Se documentará el entorno resultante reflejando entre otros aspectos:

- La documentación técnica asociada a las configuraciones realizadas.
- Enlaces a la documentación gráfica y procedimientos realizados
- Procedimiento de resolución de incidencias para la prestación del servicio de soporte asociado.

1 semana
1 mes de soporte

Esp. M365
CAU

integra

CREDENCIALES

¿Por qué Integra?

Integra es una compañía líder en el diseño, instalación, mantenimiento, soporte y gestión de infraestructuras de TI con **más de 35 años de experiencia** y con un equipo altamente especializado en soluciones de colaboración complejas sobre Microsoft 365.

Integra se compromete a abordar este prototipo con los mejores recursos humanos, incluidas certificaciones en la tecnología propuesta. Ventajas de la propuesta de servicios de Integra:

- **Conocimiento** de la arquitectura y necesidades del cliente
- **Equipo técnico** altamente especializado en la solución M365, además de la prestación de servicios considerados en la presente propuesta.
- Disponibilidad de **competencias, recursos y experiencia** en prototipos similares que avalan nuestra capacidad para afrontar con éxito la presente propuesta.
- **Liderazgo** en el mercado. En Integra, como una de las principales compañías nacionales, contamos con la suficiente solvencia técnica como financiera, además de contar con una trayectoria empresarial contrastada que permite afrontar modelos de servicio tanto a corto como a largo plazo.

integra

integra

SOMOS UNA CONSULTORA TECNOLÓGICA Y ESTRATÉGICA

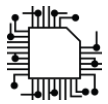
con una propuesta de valor que abarca seis áreas de servicio clave alrededor de las necesidades del hoy y del mañana de nuestros clientes

ESTRATEGIA

Consultoría y excelencia empresarial

TALENTO

Gestión del talento y soluciones RRHH



TECNOLOGÍA

Infraestructuras, ciberseguridad y tecnologías punta

EXPERIENCIA DIGITAL

Marketing, comunicación y transformación

IOT-DATA & AI

Estrategia y gobernanza del dato

SOLUCIONES DE NEGOCIO

Consultoría y procesos de gestión

Alianzas estratégicas

Microsoft — Top partner

IBM — Gold Business partner

salesforce — Business Partner

Lenovo — Partner Gold

sage — Gold partner

FORTINET — Silver partner

CLUB EXCELENCIA EN GESTIÓN — Partner preferente

INTEGRA: CONSULTORA *desde otra perspectiva*

¿QUÉ?
Nuestra propuesta

Oferta End2End de servicios tecnológicos y estratégicos.

¿CÓMO?
Nuestros comportamientos

- Somos **familiares**, como organización y como modelo de relación interna y externa.
- No tenemos **prejuicios**, ni **sesgos**, ni **jerarquías** limitantes. Somos **transparentes.**
- Somos **sensibles**. **Entendemos** y nos **adaptamos** a la situación de cada cliente.
- Somos **valientes.** Testamos nuevas ideas con la **innovación** como principio.

Nuestra diferencia está en nuestra cultura, en la forma de ver las cosas, en buscar otro punto de vista, en mirar **desde otra perspectiva.**

¿POR QUÉ?
Nuestro propósito

"Nuestra misión es **anticipar** las necesidades tecnológicas y estratégicas de nuestros clientes y nuestras personas, **entendiendo su ahora y visionando su entorno futuro**, **capacitándoles** para afrontar con garantías los desafíos de una nueva era."

integra

integra

¡MUCHAS GRACIAS!

"Trabajando en el ahora con visión del mañana"

www.integratecnologia.es