Controles Empresariales

Su aliado en la Transformación Digital

PROPUESTA COEM 365 SECURITY

Presentado a:

CLIENTE

Bogotá, Colombia

octubre de 2024

CONFIDENCIALIDAD

La información contenida en este documento presentado a CLIENTE es propiedad intelectual de CONTROLES EMPRESARIALES.

Esta propuesta ha sido desarrollada en respuesta a una solicitud expresa de CLIENTE y/o sus representantes, dirigida a CONTROLES EMPRESARIALES.

Se entiende que este documento es una propuesta de negocios y no constituye a priori un compromiso formal de CONTROLES EMPRESARIALES, sus directivos o empleados, debido a las fases subsiguientes en el proceso de selección que deberán ser evacuadas por parte de CLIENTE. Sin embargo; en caso de ser aprobada la propuesta, se generará un acuerdo de trabajo conjunto entre CONTROLES EMPRESARIALES, el cual será revisado y suscrito por las partes.

CONTROLES EMPRESARIALES se reserva el derecho de tomar las acciones que estimen necesarias conforme a las leyes nacionales e internacionales, si considera que el acuerdo ha sido transgredido y si las razones o perjuicios derivados pudiesen afectar su imagen o buen nombre.

Bogotá, octubre de 2024

Señores

CLIENTE

Bogotá, Colombia

Atención: CARGO, NOMBRE APELLIDO CONTACTO

Asunto: PROPUESTA GESTIÓN SEGURIDAD MICROSOFT 365

Apreciados señores:

Atendiendo su requerimiento, nos permitimos presentarle la propuesta técnica y comercial para la contratación de PROPUESTA GESTIÓN SEGURIDAD MICROSOFT 365 para CLIENTE. Estamos seguros representar la mejor alternativa de nuestros servicios para poder cumplir con sus necesidades.

Es muy satisfactorio para nosotros encontrarnos entre sus proveedores, a lo cual estamos dispuestos a responder con seriedad, calidad y cumplimiento. Es por eso que contamos en la actualidad con la infraestructura adecuada y un excelente equipo de trabajo, tanto interno como externo, para ofrecer el mejor respaldo a sus requerimientos.

Agradecemos de antemano su confianza en nuestra firma y es de nuestro interés hacer una presentación de esta oferta en donde podamos ampliar sobre las ventajas y beneficios del alcance de la misma. Por tal razón, extendemos desde ya nuestra cordial disposición para resolver cualquier inquietud que se presente durante su evaluación.

Esperamos poder seguir contando con ustedes como nuestro cliente y poder ofrecer nuestra experiencia, apoyo a éste y a todos sus proyectos.

Cordialmente,

CONTROLES EMPRESARIALES

TABLA DE CONTENIDO

1. RESÚMEN EJECUTIVO

Actualmente, en las organizaciones se está a la expectativa de importantes cambios en los procesos de Ciberseguridad y Seguridad de la Información; por consiguiente, se hace necesario alinear los objetivos de gestión con los estándares y recomendaciones de la industria. De ahí que aseguran que las instalaciones y todos los sistemas como un conjunto hayan sido diseñados, instalados, probados, operados y mantenidos para satisfacer las necesidades del cliente interno y externo, prolongando la vida útil y reduciendo la probabilidad de fallas prematuras.

La planificación estratégica desde el punto de vista de la seguridad de la información se relaciona con la dirección a largo plazo y las organizaciones quieren aprovechar la tecnología de la información para mejorar su proceso comercial, las compañías operan con dinamismo en el mundo digital por lo cual deben asegurar que las transacciones, datos e infraestructura sean el foco en la arquitectura de seguridad empresarial, desde este punto las empresa y sus actividades deben protegerse y recordar que la seguridad de las computadoras y las redes es solo un medio para este fin.

La seguridad de la información es solo un componente del ecosistema de las organizaciones el cual se encuentra integrado con la garantía comercial y el aseguramiento de negocios abarcando tres áreas principales:

- Seguridad de la información
- Continuidad del negocio
- Seguridad física y ambiental

Es decir, el aseguramiento comercial se refiere a todos los aspectos operativos de la gestión de riesgos y solo a través de un enfoque integrado de estos aspectos es posible que las organizaciones logren mayor rentabilidad y beneficios a través de las decisiones de la gestión del riesgo operacional.

Para lograr este objetivo, visionamos a CLIENTE con planes que le permitan comprender los niveles de madurez del entorno de Seguridad de la Información en su entorno de Microsoft 365 y poder generar una

línea base de seguridad bajo la cual operar de forma segura en la plataforma, el equipo extendido de CONTROLES EMPRESARIALES está decidido a ayudarle a tener éxito y lograr un mayor rendimiento en su empresa. PROPUESTA GESTIÓN SEGURIDAD MICROSOFT 365 que presta CONTROLES EMPRESARIALES a sus clientes, busca fortalecer la planeación, el despliegue, la operación y la actualización de su plataforma tecnológica Microsoft 365 (antes Office 365) a través de administración, soporte y capacitación, de primer y segundo nivel.

1.1. Ofertas de Suscripción de Servicios

Dominio de Seguridad	Componentes de seguridad de Microsoft	Suscripciones de Servicio					
		M365 E3	**M365 E5**	**EMS E3**	**EMS E5**	**M365 E5 Security**	**O365 E5**
Administración de Identidad y Acceso	Entra ID Plan 1	✓	✓	✓	✓		
	Entra ID Plan 2		✓		✓	✓	
	Microsoft Defender for Cloud Apps		✓		✓	✓	
Protección Contra Amenazas	Protección de Exchange Online	✓	✓				✓
	Microsoft Defender for Office Plan 2		✓			✓	✓
	Office 365 Audit Log	✓	✓				✓
	Microsoft Defender for Identity		✓		✓	✓	
	Windows Defender	✓	✓				
	Microsoft Defender for Endpoint		✓			✓	
	Microsoft Defender for Cloud Apps		✓		✓	✓	
Protección del Dispositivo	Intune Plan 1 MDM + MAM	✓	✓	✓	✓		
	BitLocker	✓	✓				

Dominio de Seguridad	Componentes de seguridad de Microsoft	Suscripciones de Servicio					
	App Locker	☐	☐				
	Guardián de Credenciales	☐	☐				
	Windows Defender Control de Aplicaciones (Guardián de Dispositivos)	☐	☐				

1.2. Seguridad Administrada Microsoft 365

Ofrecimiento	Descripción
Propuesta Administración Seguridad Microsoft 365	CONTROLES EMPRESARIALES responderá a las Solicitudes de Servicio y los informes de incidentes enviados por el cliente a través de sus representantes autorizados. “Solicitud de Servicio” significa una solicitud formal del Administrador de TI para que se brinden los Servicios. "Incidente" significa una interrupción o degradación del servicio no planificada.
Horas de cobertura	24 X 7 X 365
Canales entrantes	Los representantes autorizados del cliente se comunican con los canales de CONTROLES EMPRESARIALES Teléfono ☐ Correo electrónico ☐ Soporte Unificado en Línea ☐
Tiempos de respuesta a incidentes	Los tiempos de respuesta para los incidentes dependen del nivel de gravedad. E1 – el evento de emergencia se responderá dentro de ≤30 minutos (Incidentes planteados solo por teléfono) P1 – el evento crítico se responderá dentro de ≤1 hora (Incidentes planteados solo por teléfono) P2 – el evento urgente se responderá dentro de ≤2 horas P3 – el evento importante se responderá dentro de ≤4 horas P4 – la consulta de facturación se responderá dentro de ≤4 horas P5 – los comentarios de asesoramiento se responderán dentro de ≤48 horas

Ofrecimiento	Descripción
Tiempos de respuesta de Solicitud de Servicio	Los tiempos de respuesta para las solicitudes de servicio dependen del nivel de gravedad. S1 – el evento de emergencia se responderá dentro de ≤1 hora (solo por teléfono) S2 – el evento urgente se responderá dentro de ≤4 horas S3 – el evento importante se responderá dentro de ≤8 horas
Soporte de Tickets	Ilimitado
Representantes Autorizados	Cinco (5)
Escalamiento al Soporte Premier de Microsoft	CONTROLES EMPRESARIALES escalará los elementos que el equipo del Centro de Operaciones de Seguridad (SOC) de CONTROLES EMPRESARIALES no pueda resolver a partir de los elementos del alcance definidos en la Sección 1.1
Administración de Servicios	Los Gerentes de Éxito del Servicio de CONTROLES EMPRESARIALES se miden en función de la satisfacción del Cliente. A través de revisiones comerciales estructuradas, brindan información sobre los incidentes y las Solicitudes de Servicio, lo que demuestra el desempeño frente al SLA y resalta cualquier tendencia o aprendizaje que se pueda extraer de las interacciones anteriores. Proporcionan gestión de escalamiento para problemas en los que el Cliente desea una mejor visibilidad de su caso de soporte.
Punto de contacto único para Contactos designados	Gerente de Éxito del Servicio
Responsable por	Incidentes E1 y P1 y Solicitudes de Servicio S1
Reunión de Revisión de Negocios	Conferencia en línea realizada cada dos (2) meses con contactos nominados de administrador de TI y administrador de contratos. Esto incluye recomendaciones para: • Solicitud / Informes de Incidentes • Oportunidades de mejora del servicio • Solicitud/ Tendencias de Incidentes • Administración de escalonamiento
Revisión Operativa de Seguridad	Conferencia en línea realizada mensualmente con contactos designados de Administradores de Seguridad o de TI que cubren los informes técnicos detallados en la Sección 1.4:

<table>
<tr><th>Ofrecimiento</th><th>Descripción</th></tr>
<tr><td></td><td>Informe de Administración de Seguridad
Informe de Evaluación de TI en la Sombra
Esto incluye recomendaciones para:<table><tr><td>• Tendencias de alerta / Incidentes de seguridad</td><td>• Principales categorías de ataques</td></tr><tr><td>• Principales Incidentes de Seguridad / Usuarios riesgosos</td><td>• Recomendaciones de configuración, políticas y control de seguridad</td></tr></table></td></tr>
<tr><td>Incorporación a Seguridad Administrada 365</td><td>CONTROLES EMPRESARIALES habilitará configuraciones de seguridad 365 basadas en las prácticas recomendadas de CONTROLES EMPRESARIALES, los requisitos del cliente y los derechos de licencia del cliente como se describe a continuación en la Sección 1.1.1.3. Todos los talleres serán realizados por un consultor de nube experimentado y se entregarán de forma remota</td></tr>
<tr><td>Inicio</td><td>Alinee a las partes interesadas del Cliente con el modelo de entrega y compromiso de Seguridad Administrada 365. La definición se proporciona en la Sección 1.1.1.1 - Taller de lanzamiento.</td></tr>
<tr><td>Descubrimiento</td><td>Descubrimiento centrado en los siguientes dominios de seguridad
Administración de identidad y acceso
Protección contra amenazas
Protección del dispositivo
La definición se proporciona en la Sección 1.1.1.2 - Taller de Descubrimiento.</td></tr>
<tr><td>Diseño</td><td>Configuración recomendada y personalizada en los siguientes dominios de seguridad
Administración de identidad y acceso
Protección contra amenazas
Protección del dispositivo
La definición se proporciona en la Sección 1.1.1.3 - Taller de Diseño</td></tr>
<tr><td>Implementación</td><td>Implementación de los componentes de seguridad de Microsoft (alineados con las Suscripciones de servicio en la Sección 1.1). La definición se proporciona en la Sección 1.1.1.4 - Implementación</td></tr>
</table>

[2] S1 Solicitudes planteadas solo por teléfono

1.3. Taller de Lanzamiento

Descripción	Un taller impartido de forma remota para alinear a las partes interesadas del Cliente con el modo de compromiso y entrega de Seguridad Administrada 365.
Inclusiones	Introducción y mapeo de partes interesadas Descripción general del modelo de participación y entrega Recopilar requisitos para la evaluación de seguridad basada en herramientas
Exclusiones	Cualquier otro trabajo no especificado en Inclusiones
Principales Interesados	Contacto (s) autorizado (s) como se define en la Sección 3 Gerente de Seguridad de TI Gerente de Proyecto designado para coordinar los requisitos de las partes interesadas
Duración	Una (1) sesión de máximo dos (2) horas
Dependencias	El cliente facilitará la asistencia de las partes interesadas clave a la sesión programada Autorización del Cliente para evaluar la configuración de seguridad de los Tenant del Cliente
Entregables	Documento de requisitos previos técnicos específicos del cliente

1.4. Taller de Descubrimiento

Descripción	Un taller impartido de forma remota para revisar las políticas y controles existentes
Inclusiones	CONTROLES EMPRESARIALES realizará las siguientes tareas Evaluación basada en herramientas de la (s) configuración (es) de seguridad de los Tenant de Microsoft 365 suscritos Recopilar requisitos para políticas y controles de seguridad, prioridades, restricciones y exclusiones.
Exclusiones	Cualquier otro trabajo no especificado en Inclusiones
Principales Interesados	Contacto (s) autorizado (s) como se define en la Sección 3 Gerente de seguridad de TI

Descripción	Un taller impartido de forma remota para revisar las políticas y controles existentes
	Gerente de proyecto designado para coordinar los requisitos de las partes interesadas
Duración	Hasta dos (2) sesiones de un máximo de dos (2) horas cada una
Dependencias	El cliente facilitará la asistencia de las partes interesadas clave a la sesión programada Cuenta creada dentro del Tenant de Microsoft 365 con el rol de administrador global asignado para su uso por CONTROLES EMPRESARIALES
Entregables	Matriz de trazabilidad de requisitos de requisitos identificados Informe de evaluación específico del cliente que proporciona el análisis de brechas, exclusiones aprobadas y recomendaciones priorizadas de políticas y controles

1.5. Taller de Diseño

Descripción	Un taller impartido de forma remota para revisar y aprobar las recomendaciones de configuración de seguridad
Inclusiones	Facilitar y realizar un taller remoto para presentar los siguientes temas Configuraciones y políticas de seguridad recomendadas alineadas con los requisitos del cliente Revisión de las licencias existentes frente a las licencias requeridas o cambios en la suscripción del servicio en línea (según sea necesario) Recopilar información de configuración técnica del Cliente para las políticas y configuraciones de seguridad para producir el Plan de Seguridad Administrada 365 personalizado para los componentes incluidos en las Suscripciones de Servicio).

Producto	Componente	Diseño
Office 365 E3	Exchange Online Protection	Antispam y antimalware Definición de políticas Definición de ajustes de configuración
Office 365 E5	Microsoft Defender for Office Plan 2	Definición de políticas y configuración para Antiphishing Motor Antimalware Archivos adjuntos seguros Enlaces seguros

Descripción	Un taller impartido de forma remota para revisar y aprobar las recomendaciones de configuración de seguridad		
			Antispam (filtrado de correo) Investigación y respuesta automatizadas Registros de auditoría de Office 365
	Enterprise Mobility + Security E3	Microsoft Entra ID Plan 1	Definición de políticas contextuales a nivel de usuario, ubicación, dispositivo y aplicación para el acceso condicional Habilitar el restablecimiento de contraseña de autoservicio Aprobación para la habilitación de MFA en aplicaciones en la nube de Microsoft O365 Aprobación para la configuración de SSO en aplicaciones en la nube de Microsoft O365 Definición de hasta cinco (5) aplicaciones en la nube con políticas estándar de la Galería de Microsoft.
		Intune Plan 1 MDM + MAM	Definición de políticas sobre • Configuración • Cumplimiento • Acceso condicional • Inscripción de dispositivos corporativos • Distribución y actualizaciones de software
	Enterprise Mobility + Security E5	Microsoft Entra ID Plan 2	Definición de políticas para: Protección de identidad ○ Detección de vulnerabilidades y cuentas de riesgo ○ Investigación de eventos de riesgo ○ Políticas de acceso condicional basadas en riesgos Gobernanza de la identidad ○ Administración de identidad privilegiada ○ Acceder a las revisiones
		Microsoft Defender for Identity	Definir configuración

Descripción	Un taller impartido de forma remota para revisar y aprobar las recomendaciones de configuración de seguridad		
		Microsoft Defender for Cloud Apps	Definición de políticas Creación de lista blanca / lista negra
	Windows E3	App Locker	Definición de reglas
		BitLocker	Definición de políticas para ejecutar a través de MDM o políticas de grupo
		Acceso condicional para Windows	Definición de políticas contextuales a nivel de usuario, ubicación, dispositivo y aplicación
		Guardia de Credenciales	Habilite y configure Guardia de Credenciales, configure políticas para que se ejecuten a través de MDM o políticas de grupo
		Control de aplicaciones de Windows Defender (Guardia del dispositivo)	Definición de las reglas de la política de control de aplicaciones de Windows Defender
		Antivirus de Windows Defender	Definición de política
		MDM + MAM (Windows)	Definición de políticas de línea base de seguridad de MDM para lo siguiente Tecnología de seguridad de la bandeja de entrada de Microsoft (no obsoleta) como BitLocker, SmartScreen y Device Guard (seguridad basada en virtual), Exploits Guard, Defender y Firewall Restringir el acceso remoto a los dispositivos Establecer requisitos de credenciales para contraseñas y PIN Restringir el uso de tecnología heredada Políticas de tecnología heredada que ofrecen soluciones alternativas con tecnología moderna

Descripción	Un taller impartido de forma remota para revisar y aprobar las recomendaciones de configuración de seguridad		
	Windows E5	Microsoft Defender for Endpoint Plan 2	Definición de políticas Configuración de respuesta automatizada y remediación
Exclusiones	Implementación de Diseño Adopción de usuarios y gestión de cambios Productos de Microsoft o componentes de seguridad no incluidos en las Suscripciones de Servicio Cualquier otro trabajo no especificado en Inclusiones		
Principales Interesados	Contacto (s) autorizado (s) como se define en la Sección 3 Administradores de desktop del cliente Gerente de seguridad de TI del cliente Gerente de proyecto del Cliente designado para coordinar los requisitos de las partes interesadas Miembros del equipo de Operaciones de TI del cliente Personal de la mesa de Servicio al cliente		
Duración	Una (1) sesión de máximo cuatro (4) horas		
Dependencias	El Cliente facilitará la asistencia de los Principales Interesados a la sesión programada. El cliente deberá aprobar el plan de implementación y el plan de implementación de seguridad Administrada 365 antes de que pueda comenzar la implementación		
Entregables	Plan de Seguridad Administrada 365 específico del cliente para suscripciones de servicio seleccionadas Plan de implementación específico del cliente		

1.6. Implementación

Descripción	Implementación de los componentes de seguridad de Microsoft (alineados con las Suscripciones de Servicio seleccionadas		
Inclusiones	Seguridad Administrada 365 incluye lo siguiente:		
	Producto	**Componente**	**Implementación**
	Office 365 E3	Exchange Online Protection	Habilitar políticas, configuraciones y alertas según el plan de Seguridad Administrada 365
	Office 365 E5	Microsoft Defender for Office Plan 2	Habilitar políticas, configuraciones y alertas según el plan de Seguridad Administrada 365

Descripción	Implementación de los componentes de seguridad de Microsoft (alineados con las Suscripciones de Servicio seleccionadas		
	Enterprise Mobility + Security E3	Microsoft Entra ID Plan 1	Habilitar las políticas y configuraciones según el plan de Seguridad Administrada 365 Configuración hasta cinco (5) aplicaciones en la nube con políticas estándar de la Galería de Microsoft
		Intune Plan 1 MDM + MAM	Habilitar las políticas y configuraciones según el plan de Seguridad Administrada 365
	Enterprise Mobility + Security E5	Microsoft Entra ID Plan 2	Habilitar y configure módulos según el plan de Seguridad Administrada 365
		Microsoft Defender for Identity	Crear una instancia de Microsoft Defender for Identity Configurar los ajustes según el plan de Seguridad Administrada 365 Proporcionar orientación al cliente para conectar el bosque de Active Directory del cliente Descargar, instalar y configurar el sensor Microsoft Defender for Identity
		Microsoft Defender for Cloud Apps	Habilitar y configurar según el plan de Seguridad Administrada 365 Integrar con Microsoft Defender for Endpoint y Microsoft Defender for Identity, como se define en el Plan de Seguridad Administrada 365
	Windows E3	App Locker	Habilitar y configurar según el plan de Seguridad Administrada 365
		BitLocker	Habilitar y configurar según el plan de Seguridad Administrada 365
		Acceso condicional para Windows	Habilitar y configurar según el plan de Seguridad Administrada 365
		Guardián de Credenciales	Habilitar Credential Guard según el plan de Seguridad Administrada 365
		Control de aplicaciones de Windows Defender	Habilitar Device Guard según el plan de Seguridad Administrada 365

Descripción	Implementación de los componentes de seguridad de Microsoft (alineados con las Suscripciones de Servicio seleccionadas		
		(Guardián del Dispositivo)	
		Antivirus de Windows Defender	Habilitar y configurar según el plan de Seguridad Administrada 365
		MDM + MAM (Windows)	Habilitar y configurar según el plan de Seguridad Administrada 365
	Windows E5	Microsoft Defender for Endpoint Plan 2	Habilitar y configurar según el plan de Seguridad Administrada 365
Exclusiones	Implementación o configuración de los siguientes requisitos previos Sincronización de Microsoft Entra ID Migración de datos o buzón de Exchange Online Inscripción de usuarios y dispositivos en Intune Remediación de eventos identificados por CONTROLES EMPRESARIALES y / o el Cliente donde CONTROLES EMPRESARIALES no es el propietario del servicio Administración principal y / o propiedad del Tenant del cliente Administración de cuentas de usuario, como agregar, modificar o eliminar usuarios y privilegios de acceso Crear soluciones alternativas para permitir que las tecnologías heredadas sigan funcionando con la autenticación moderna Carga de aplicaciones en tiendas del mercado de la nube. P.ej. Tienda Google Play u otra tienda de aplicaciones Solución de problemas de la funcionalidad de la aplicación en dispositivos administrados por MDM Cualquier otro trabajo no especificado en Inclusiones		
Principales Interesados	Contacto (s) autorizado (s) como se define en la Sección 3 Administradores de desktop del cliente Gerente de Seguridad de TI del cliente Administrador de mensajería del cliente Gerente de proyecto del Cliente designado para coordinar los requisitos de las partes interesadas Miembros del equipo de operaciones de TI del cliente Personal de la mesa de Servicio al cliente		
Duración	Según el Plan de implementación acordado en la Sección de Durección del Servicio		

Descripción	Implementación de los componentes de seguridad de Microsoft (alineados con las Suscripciones de Servicio seleccionadas
Dependencias	Licencias apropiadas de Microsoft (como se define en la Sección de características del servicio) Active Directory sincronizado con Microsoft Entra ID con identidades de usuario que residen en Microsoft Entra ID Buzones de correo de correo electrónico ubicados en Exchange Online Registros de correo (MX) apuntados a Exchange Online Dispositivos administrados por Intune y Microsoft Entra Endpoints que ejecutan Windows 10 Pro (para paquetes de servicios que incluyen Windows 10 E3 y E5) Privilegios delegados de administrador de seguridad e Intune con MFA habilitado Función de administrador de cumplimiento, administrador de flujo de correo Privilegios de Administrador de Seguridad o Administrador Global para configurar el Tenant y generar informes. (Existen razones debido a la implementación de Azure por parte de Microsoft que significan que los privilegios del Administrador de Seguridad pueden no permitir la configuración de la configuración de seguridad y pueden ser necesarios privilegios de Administrador Global) El Cliente facilitará la asistencia de los Principales Interesados a la sesión programada
Entregables	Guía de configuración de BitLocker para la implementación del cliente Guía de configuración de Guardia de Credenciales para la implementación del cliente Guía de configuración de Guardia del Dispositivo para la implementación del cliente

2. VISIÓN GENERAL DE LA INCORPORACIÓN

2.1. Sesión de Incorporación de Servicios Administrados

Descripción	**CONTROLES EMPRESARIALES** facilitará la incorporación a los Contactos Autorizados designados para la transición de Negocios como de Costumbre
Inclusiones	Programación de la sesión para los contactos autorizados designados Sesión de incorporación para los Contactos Autorizados nominados entregada a través de la solución de conferencias CONTROLES EMPRESARIALES Proporcionar credenciales a los contactos autorizados designados para la herramienta de administración de servicios de TI En Línea de Soporte Unificado Proporcionar URL de acceso, dirección de correo electrónico y número de teléfono de contacto a los Contactos Autorizados designados

Descripción	**CONTROLES EMPRESARIALES facilitará la incorporación a los Contactos Autorizados designados para la transición de Negocios como de Costumbre**
	Proporcionar una matriz de escalamiento
Exclusiones	Cualquier otro trabajo no especificado en Inclusiones
Principales Interesados	Contacto (s) autorizado (s) como se define en la Sección 3
Duración	Una (1) sesión de máximo dos (2) horas
Dependencias	El cliente facilitará la asistencia de los Contactos Autorizados a la sesión programada
Entregables	Credenciales para la herramienta de gestión de servicios de TI en línea de Soporte Unificado

3. ADMINISTRACIÓN DE SERVICIOS

Descripción	**CONTROLES EMPRESARIALES facilitará la incorporación a los contactos autorizados designados para la transición a Negocios como de costumbre**
Inclusiones	Hay dos partes involucradas en la administración del entorno Microsoft 365 del Cliente, específicamente: Cliente (incluido cualquier equipo de TI interno) CONTROLES EMPRESARIALES La Tabla 1: Responsabilidades delinea tareas entre las partes R - Responsable de actividad I - Informado de actividad Tabla 1: Responsabilidades

Característica	CONTROLES EMPRESARIALES	CLIENTE
Centro de Operaciones CONTROLES EMPRESARIALES		
Cobertura 24x7x365	R	I
Línea directa de Service Desk	R	I
Soporte Unificado Herramienta de Gestión de Servicios de TI en Línea	R	I
Notificaciones de interrupción de la plataforma	R	I
Soporte Respaldado por el Proveedor	R	I
Administración de Incidentes		

Descripción	**CONTROLES EMPRESARIALES facilitará la incorporación a los contactos autorizados designados para la transición a Negocios como de costumbre**		
	Levantar Solicitud de Incidente (humano)	I	R
	Levantar Solicitud de Incidente (automatizado)	R	I
	Responder a una notificación de Incidente	R	I
	Resuelve el incidente	R	I
	Informes de administración	R	I
	Administración De Servicios		
	Levantar Solicitud de Servicio (humano)	I	R
	Levantar Solicitud de Servicio (automatizado)	R	I
	Ejecutar Solicitud de Servicio	R	I
	Cerrar Solicitud de Servicio	R	I
	Informes de administración	R	I
	Administración de Solicitudes de Cambio		
	Gestionar cambios y el proceso de cambio	R	I
	Presidir la Junta de Aprobación de Cambios "CAB" y el Comité de Emergencias / CAB	I	R
	Revisión de Solicitudes de Cambio "RFC"	R	I
	Aprobación de RFC	I	R
	Ejecutando RFC	R	I
	Cerrando RFC	R	I
	Informes de administración	R	I
Exclusiones	Administración principal y / o propiedad del Tenant del Cliente fuera de los Servicios de Seguridad Administrados definidos en este Anexo Soporte para tecnologías de Microsoft 365 no definidas en este Anexo Monitorización de eventos e incidentes de seguridad durante la fase de incorporación Cualquier otro trabajo no especificado en Inclusiones		
Principales Interesados	Contacto (s) autorizado (s) como se define en la Sección 3		
Dependencias	CSA firmado con representante (s) autorizado del cliente Anexo firmado Acceso administrativo delegado a la (s) suscripción (es)		
Entregables	Credenciales para la herramienta de Administración de Servicios de TI en línea de Soporte Unificado		

4. SERVICIO ADMINISTRADO

<table>
<tr><th>Descripción</th><th colspan="3">Las inclusiones del Servicio de Seguridad Administrado 365 están definidas por la suscripción como se especifica en 2.2 - Selección del nivel de servicio</th></tr>
<tr><td>Inclusiones</td><td colspan="3">CONTROLES EMPRESARIALES responderá a las Solicitudes de Servicio y los informes de Incidentes enviados por el Cliente a través de sus representantes autorizados y proporcionará monitoreo, investigación y respuesta de alerta de seguridad 24x7 e informes de servicio. La cobertura solo se proporciona para las Suscripciones al Servicio y los componentes de seguridad de Microsoft relacionados en la Sección 1.1

Tabla 2: Descripción General del Servicio Administrado
<table>
<tr><th>Producto</th><th>Componente</th><th>Cobertura</th></tr>
<tr><td>Office 365 E3</td><td>Exchange Online Protection</td><td>Supervisar y responder a las alertas de seguridad
Mantener las políticas de seguridad</td></tr>
<tr><td>Office 365 E5</td><td>Microsoft Defender for Office Plan 2</td><td>Supervisar y responder a las alertas de seguridad
Mantener las políticas de seguridad</td></tr>
<tr><td rowspan="2">Enterprise Mobility + Security E3</td><td>Microsoft Entra ID Plan 1</td><td>Mantener las políticas de seguridad
Configure SSO para 5 aplicaciones de nubes adicionales por trimestre con políticas estándar fuera de la Galería de Microsoft</td></tr>
<tr><td>Intune Plan 1 MDM + MAM</td><td>Mantener las políticas de cumplimiento de seguridad
Supervisar y responder a las alertas de seguridad
Alertas de dispositivos que no cumplen
El equipo de servicio administrado proporcionará recomendaciones para Windows 10
• Implementar una actualización del sistema operativo para mitigar los riesgos de seguridad.
• Modificar un valor de registro
• Deshabilitar o habilitar una configuración para mitigar los riesgos de seguridad</td></tr>
<tr><td>Enterprise Mobility +</td><td>Microsoft Entra ID Plan 2</td><td>Mantener las políticas de seguridad
Supervisar y responder a las alertas de seguridad y notificar sobre inicios de sesión / usuarios riesgosos.</td></tr>
</table></td></tr>
</table>

Descripción	Las inclusiones del Servicio de Seguridad Administrado 365 están definidas por la suscripción como se especifica en 2.2 - Selección del nivel de servicio		
	Security E5	Microsoft Defender for Identity	Monitorear y solucionar problemas del sistema ATP Mantener las políticas de seguridad Supervisar y responder a las alertas de seguridad
		Microsoft Defender for Cloud Apps	Mantener las políticas de seguridad Supervisar y responder a las alertas de seguridad
	Windows E3	App Locker	Mantener las políticas de AppLocker
		BitLocker	Mantener políticas
		Acceso condicional para Windows	Mantener las políticas de seguridad Supervisar y responder a las alertas de seguridad
		Guardián de Credenciales	Supervisar y responder a las alertas de seguridad
		Control de aplicaciones de Windows Defender (Guardián de dispositivo)	Mantener las políticas de seguridad Supervisar y responder a las alertas de seguridad Administrar la lista blanca del catálogo de aplicaciones
		Antivirus de Windows Defender	Mantener las políticas de seguridad Supervisar y responder a las alertas de seguridad
		MDM + MAM (Windows)	Mantener las políticas de seguridad Supervisar y responder a las alertas de seguridad
	Windows E5	Microsoft Defender for Endpoint Plan 2	Mantener las políticas de seguridad Supervisar y responder a las alertas de seguridad

Informes	Frecuencia	Inclusiones
Informe de Administración de Seguridad	Mensual	Informe CAS Informe ATP Informe de inicio de sesión riesgoso Informe de usuarios en riesgo Visión general de incidentes abierto, en curso + tickets cerrados para el período

Descripción	Las inclusiones del Servicio de Seguridad Administrado 365 están definidas por la suscripción como se especifica en 2.2 - Selección del nivel de servicio		
			Visión general e solicitudes de servicio abierto, en curso + cerrado para el período Resumen de solicitud de administración de cambios Informe de SPAM Informe de dispositivo de incumplimiento Aplicaciones recomendadas para SSO
	Informe de Evaluación de TI en la Sombra	Trimestral	Informe que contiene una lista de posibles usos de TI en la sombra descubiertos y recomendaciones para una mayor investigación de estos Una hoja de ruta prioritaria y procesable para abordar el uso de la nube descubierto, especialmente su aspecto de TI en la sombra, que incluye las capacidades de mapeo de Cloud App Security en el entorno del Cliente.
Exclusiones	A medida que se introduzcan nuevos productos y funciones de Microsoft en Microsoft 365, se evaluarán para su alineación con MSS. Las actualizaciones del MSS se publicarán a través de Soporte Unificado en Línea CONTROLES EMPRESARIALES. Monitoreo de alertas, respuesta y recomendaciones para alertas de gravedad baja e informativa Cualquier otro trabajo no especificado en Inclusiones		
Principales Interesados	Contacto (s) autorizado (s) como se define en la Sección 3		
Dependencias	Los servicios solo están disponibles para componentes con licencia / suscripciones activas de los Productos de Microsoft y la cobertura del servicio administrado para cada componente. Algunos servicios pueden tener requisitos técnicos previos como una versión mínima de software u otros. Los informes proporcionados en el Servicio requieren las licencias de Microsoft 365 necesarias del Cliente; de lo contrario, el informe correspondiente no estará disponible Pertenencia al Grupo de Administradores de Seguridad Pertenencia al Grupo de Lectores de Seguridad Acceso de solo lectura a la información de licencia de Microsoft del Cliente para la facturación mensual de Seguridad Administrada 365		

Descripción	Las inclusiones del Servicio de Seguridad Administrado 365 están definidas por la suscripción como se especifica en 2.2 - Selección del nivel de servicio
Entregables	Configuración de alertas para componentes cubiertos en el Tenant Informes mensuales y trimestrales que se compartirían con el representante designado del Cliente. Los cambios razonables a los informes estándar se considerarán caso por caso. Los cambios importantes se pueden considerar en términos comerciales

5. DETALLES DE LA SUSCRIPCIÓN

5.1. Información de Suscripción

Suscripción	Nombre del Tenant
Suscripción Basada en el Usuario	<Tenant>.onmicrosoft.com

Confirme el nombre del Tenant actual del Cliente o el nombre preferido del Cliente. La disponibilidad de nombres se puede comprobar aquí

6. PROPUESTA ECONÓMICA

6.1.1.Servicio a 36 meses

Descripcion del Servicio	Valor mensual del servicio (COP $)	Valor del servicio total 36 meses (COP $)
Propuesta COEM 365 Security	COP $ 9.600.000	COP $ 345.600.000
	Total (COP $)	**COP $ 345.600.000**

Nota: Estos valores son antes de IVA.

7. DURACIÓN DEL SERVICIO

La duración del servicio es de 3 años a partir de la fecha de suscripción del acta de inicio. De ser necesarias Servicios adicionales como gobierno y seguridad de la información con Microsoft Purview, deben ser solicitadas a través de una nueva cotización.

8. FORMA DE PAGO

Los servicios serán facturados anticipado al inicio del servicio, las horas adicionales a las pactadas se cobrarán mensualmente relacionando las horas ejecutadas. El pago se realizará 30 días después de radicada la respectiva factura en las oficinas de CLIENTE según su proceso interno de pago a proveedores.

9. VALIDEZ DE LA OFERTA

La vigencia de esta propuesta es de (30) días calendario a partir de su fecha de recibo por parte de CLIENTE.

10. DATOS DE CONTACTO

NOMBRE1 NOMBRE 2 APELLIDO1 APELLIDO2

Gerente de Cuenta Corporativo

Número fijo: +57 (XXX) XXXXXXX

Número móvil: +57 (XXX) XXXXXXX

Línea Gratuita: 018000949297

https://www.controlesempresariales.com.co | xxxxxxxx@coem.co