TOKIOTA

Assessment Seguridad entorno Azure

Propuesta de colaboración

Enjoy the journey!

Índice

01

Contexto, Retos y Objetivos

Contexto

La seguridad de negocio relacionado con el entorno Azure depende directamente de tener las herramientas, procesos y recursos para mantener un entorno seguro en todo su conjunto, frente amenazas, acceso a información sensible y protección de la información de las personas.

En la nube, reconocemos por adelantado que pueden ocurrir brechas de seguridad que, al final pueden afectar a las personas de manera muy directa. Es imposible evitar por completo estos riesgos, pero poner soluciones de detección temprana, mitigación y remediación robustas minimizan ese riego de una manera directa, de tal manera que con un esfuerzo relativo se pude mejorar considerablemente la protección de tus sistemas.

La decisión empresarial para acometer un plan de acciones de seguridad varía de una empresa a otra y depende de manera directa de la información que manejan, el grado de madurez tecnológico de su compañía y, el perjuicio directo que podría tener una brecha de seguridad en sus personas y su negocio.

El Cliente acude a Tokiota para evaluar el actual estado de madurez de su Compañía poniendo especial foco en la parte de su infraestructura Azure, donde de su resolución se espera poder elaborar de manera conjunta un plan de acción que le permita hacer frente a cualquier tipo amenaza actual o futura.

Necesidad

Los retos que plantea una evaluación de estado actual de seguridad de sus recursos y un posterior plan de acción requieren de un ejercicio de consultoría y planificación adecuado, con la participación de expertos tecnológicos y de negocio que aporten remediaciones técnicas, procedimentales y humanas ante cualquier riesgo de seguridad detectado.

Alcance de la colaboración

Analizar, Diseñar y planificar de manera conjunta las soluciones de ciberseguridad del **Cliente**, a través de un ejercicio de consultoría que ayude a generar un plan maestro de acciones tecnológicas para la prevención, detección y respuesta de riesgos de seguridad de la información.

El análisis de seguridad se enfocará en realizar una evaluación **de seguridad en toda su plataforma de Microsoft, principalmente enfocado a:**

- ✓ **Servicios Azure**
- ✓ **Entorno Microsoft 0365**
- ✓ **Active Directory Azure**

En base a la experiencia de Tokiota en situaciones similares, se plantea una iniciativa en torno a 2 fases:

1. **Assessment Semiautomático**
2. **Assessment Manual**

¿Cuáles son los Retos?

Gestión del Coste

Aunque la nube pública alguna vez fue conocida como una alternativa económica a las operaciones locales, esos ahorros se han vuelto más difíciles de realizar y trazar en los últimos años. Cualquier plan de recuperación ante desastres requerirá de un coste extra sobre el consumo global de la plataforma, así como el coste extra que supone los proyectos asociados que surgirán de estos ejercicios. La buena planificación y el control del coste desde la primera fase de análisis son claves para asegurar que pagas solo por lo que necesitas. Encontrar un balance adecuado entre coste/necesidad es clave.

Seguridad

El gobierno del dato replicado y la transparencia absoluta sobre quién tiene acceso y opera la información es fundamental, y uno de los puntos críticos a tener en cuenta en cualquier ejercicio de este tipo. Se deben tener en cuenta regulaciones europeas y normativas específicas del **Cliente** durante el proceso y anotar cualquier restricción o requerimiento de seguridad en la elaboración de plan.

Buenas practicas

Identificar los potenciales riesgos de seguridad y, en caso necesario, recomendar hacer uso de las buenas prácticas de Microsoft, o proponer adaptarlas según el uso que se vaya a tener en la plataforma de Azure, Entra ID y Microsoft 365.

Objetivos

"Colaborar con el Cliente para realizar una evaluación de seguridad en toda su plataforma de Microsoft, enfocada principalmente a Azure Cloud y Active Directory. El resultado de este análisis ayudará a definir las recomendaciones que formaran parte del plan de acción que permita al Cliente, con el soporte de Tokiota, reducir la exposición de su infraestructura ante potenciales amenazas de seguridad, incrementando de esta manera su grado de madurez en cuanto a seguridad de la información"

0 1

Entendimiento del alcance especifico a nivel de entorno Microsoft, diseñar y planificar acciones necesarias para poder realizar un preanálisis con colaboración del Cliente. Entender la plataforma será 100% necesario para poder enfocar el assessment con el mayor éxito posible.

0 2

Identificar y analizar los procesos de seguridad ante cualquier restricción (interna o externa) para la actuación y el gobierno de los entornos y de los datos que estos contienen.

0 3

Presentación de recomendaciones de seguridad, basándonos en las buenas prácticas de Microsoft y adaptándolas al Cliente.

0 4

Soporte en la remediación de los potenciales riesgos detectados durante el análisis de seguridad.

02

Assessment Seguridad

Assessment y Estrategia Azure:

Enfoque general

En base a nuestra experiencia en situaciones similares a la del Cliente, hemos definido un modelo de assessment que nos permita analizar y diagnosticar la situación actual con garantías, al tiempo que creamos una estrategia personalizada en un tiempo razonable

~2 – 2,5 meses

01. PREVENCIÓN Y PROTECCIÓN

Identificación de los controles para reducir **riesgos** en **Azure**, incluyendo acceso seguro, segmentación de red, protección de identidades y datos. **Evaluación** de políticas de seguridad, cumplimiento y mejores prácticas para minimizar **vulnerabilidades** antes de que sean explotadas.

~2-3 semanas

02. DETECCIÓN Y RESPUESTA

Evaluación de las capacidades de monitorización, detección de amenazas y respuesta ante incidentes en Azure. **Revisión** de los sistemas de seguridad y automatización de alertas para optimizar la visibilidad y la capacidad de respuesta frente a ataques y anomalías.

~2-3 semanas

03. AUDITORIA

Revisión de configuraciones, logs y cumplimiento en Azure para identificar desviaciones y riesgos. **Análisis** de accesos, privilegios y cambios en la infraestructura, garantizando trazabilidad y alineación con regulaciones y estándares de seguridad. **Evaluación** del scoring de seguridad para priorizar acciones de mejora.

~1-2 semanas

04. PLAN DE ACCIÓN

Definición de iniciativas prioritarias para fortalecer la seguridad en Azure. **Elaboración** de un roadmap que incluye medidas correctivas, recomendaciones estratégicas y tácticas, alineadas con los riesgos identificados y las capacidades del Cliente para una implementación efectiva y sostenible**.**

~1-2 semana

Prevención y Protección

Objetivo

Utilizamos los servicios de Azure y diseñamos las soluciones deseadas con los patrones de seguridad idóneos para cada tipo de entorno. Con el objetivo de minimizar el riesgo de la implementación de nuevas soluciones y estandarizar un marco de seguridad óptimo para vuestra plataforma.

Se plantea la seguridad en todos los ámbitos de la empresa, haciendo un repaso de la administración de identidades y accesos, la seguridad de red en Azure, el cifrado y almacenamiento de datos, la seguridad en entornos IaaS y en las Aplicaciones.

Se plantea desarrollar un marco de seguridad para minimizar los nuevos riesgos de seguridad y asumir los conocidos.

Responsables Principales:

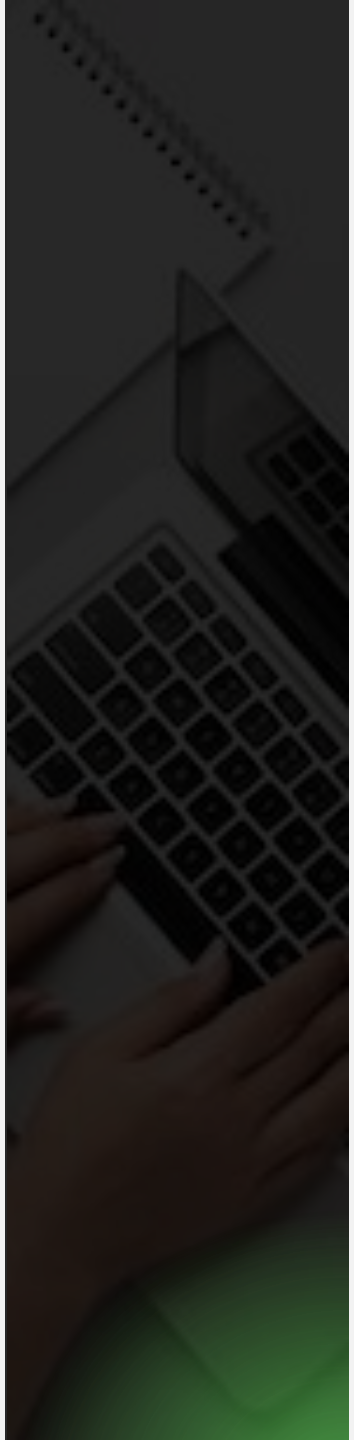
Cliente

TOKIOTA

Responsable de Proyecto

Arquitectura

Arquitecto infraestructura



Tareas

- Análisis de las recomendaciones de seguridad y buenas practicas
- Realizar pruebas de seguridad e introducir los controles mitigatorios en base a los resultados obtenidos
- **Zero Trust** de Microsoft
  - Análisis de servicios de administración de identidad y acceso, aportando los procedimientos recomendados, planos de control y listas de comprobación
  - Análisis de seguridad de la red, aportando los procedimientos recomendados, protecciones ante ataques, segmentación de red, flujo de datos y conectividad.
  - Análisis de seguridad, cifrado y almacenamiento de datos, aportando listas de comprobación y administración de claves de seguridad y encriptación.
  - Análisis de seguridad en plataformas de infraestructura, revisando los servicios antimalware y las políticas de seguridad de máquinas virtuales
  - Análisis y clasificación de seguridad en aplicaciones, planeando dependencias y configuraciones, usando servicios de supervisión, auditoria y operaciones.
- Incluir en el plan de acción las técnicas para alcanzar los objetivos.
- Elaborar un presupuesto acorde a las acciones técnicas definidas.

Entregables

- Zero Trust Maturity assessment
  - Recomendaciones de seguridad Identidades y accesos
  - Recomendaciones de seguridad en Redes
  - Recomendaciones de seguridad en cifrado y almacenamiento de datos
  - Recomendaciones de seguridad en servicios IaaS
  - Recomendaciones de seguridad en aplicaciones
- Plan de acción y presupuesto asociado.

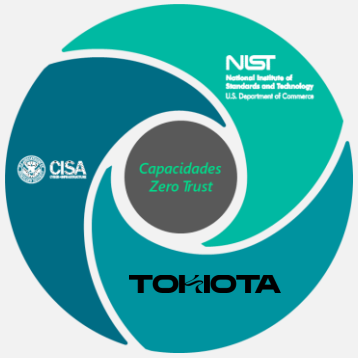
Assessment Semiautomático

Cyber Assessment Zero Trust

Se realizará un **Cyber Assessment** con el objetivo de evaluar y establecer el nivel de madurez de ciberseguridad del Cliente, éste se basará en frameworks de seguridad contrastados internacionalmente (CSA, NIST, CIS).

METODOLOGÍA

El Cyber Assessment Cloud está **compuesto por los mejores estándares** en materia de ciberseguridad aportando una **visión unificada** de todos ellos, así como la incorporación de las mejores prácticas definidas por el framework CIS de Microsoft



CAPACIDADES

Está diseñado para ayudar a los negocios a evaluar su nivel de madurez en cuanto a seguridad de la información de su infraestructura y AD, donde en cada uno de ellos se identifican tanto las **capacidades como las opciones de mejora**.

Microsoft 365, SharePoint and Azure

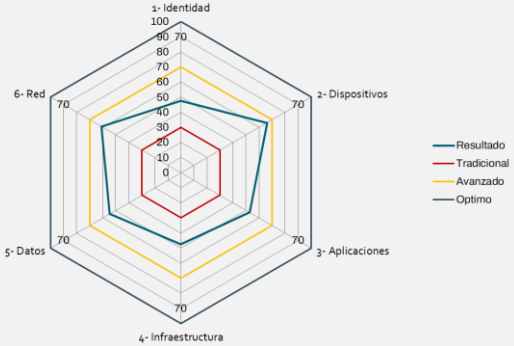
Active Directory Microsoft Entra ID

GRADO MADUREZ

Como resultado de este modelo se obtendrá un **scoring de seguridad**, el cuál marcará el punto de partida de cara a realizar este ejercicio una vez aplicadas las medidas mitigatorias recomendadas en el **Plan de Acción** y, comparar así, la **evolución del grado de madurez**

EVOLUCIÓN

El modelo permite la **comparativa del nivel de madurez** actual con el nivel de agentes externos, tanto a **nivel sectorial**, como en base **a buenas prácticas** del mercado.



Assessment Semiautomático

Preparación

- Kick-off
- Info prerrequisitos

Descubrimiento

- Despliegue herramienta
- Escaneo alcance
- Rellenar cuestionario

Análisis

- Revisión resultados
- Generación entregables

Entrega

- Presentación resultados
  - *CSAT - Cloud Security Assessment*
  - *Doc Findings*
  - *Resum Executive*
- Recomendaciones
- Siguientes pasos

2 horas | 5 días | 1 hora

1 hora | Tiempo estimado de ejecución: 2 semanas

Total de tiempo estimado: 2-3 semanas

Detección y Respuesta

Objetivo

Realizar una evaluación exhaustiva de la plataforma Azure del Cliente para identificar amenazas, vulnerabilidades y riesgos. Con base en los hallazgos, se definirán contramedidas y recomendaciones que fortalezcan la seguridad de las aplicaciones e infraestructuras, mitigando riesgos técnicos y de negocio.

El proceso incluye:

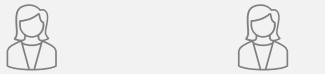
- **Evaluación inicial**: Cuestionario estructurado para identificar riesgos.
- **Análisis técnico avanzado**: Modelado de amenazas y priorización de riesgos.

Este enfoque garantiza una comprensión clara de los riesgos y una base sólida para implementar medidas de seguridad proactivas.

Responsables Principales:

Cliente

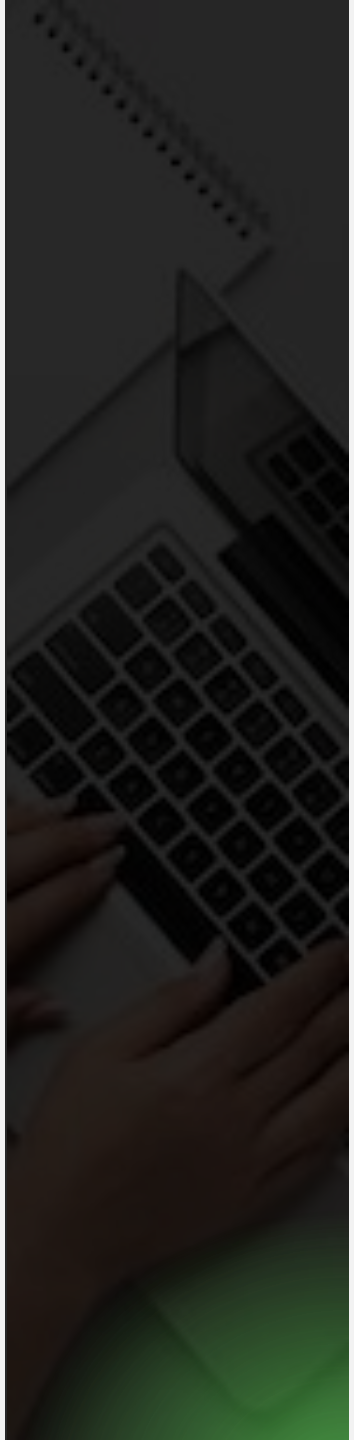
TOYOTA



Responsable de Proyecto

Arquitectura

Arquitecto Cyber



Tareas

- **Análisis de recursos y entornos**: Evaluación de los recursos, aplicaciones y entornos existentes para identificar posibles amenazas y vulnerabilidades.
- **Protección contra ransomware y extorsión**: Revisión de las medidas actuales de protección contra ransomware, extorsión y otras amenazas críticas.
- **Identificación de puntos críticos**: Análisis de los aspectos clave de seguridad:
  - Identidad
  - Dispositivos
  - Datos
  - Aplicaciones
  - Infraestructura
- **Cuestionario inicial**: Recopilación de información mediante preguntas sencillas para entender el estado actual de la seguridad.
- **Evaluación progresiva**: Revisión detallada del diseño de recursos, aplicaciones entornos para detectar riesgos técnicos.
- **Detección y mitigación**: Análisis de las plataformas de detección y mitigación existentes.
- **Plan de acción**: Definición de técnicas y acciones para alcanzar los objetivos de seguridad.
- **Presupuesto**: Elaboración de un presupuesto alineado con las acciones técnica propuestas.

Entregables

- Resultado de detecciones
- Recomendaciones
- Plan de acción y presupuesto asociado.

Assessment Manual

Assessment Cloud

Identidades

- Active Directory
- Entra ID
- Azure AD Connect
- Identity Protection
- Multi Factor Authentication
- Acceso Condicional
- Privileged Identity Management
- Endpoints: Intune
- RBAC
- SSO
- Azure Business to Consumer
- Informes de Azure AD
- Revisión de accesos en Entra
- Purview: Cumplimiento
- Purview: Seguridad
- Revisión de usuarios administradores

General

- Suscripciones

Networking

- Segmentación de red
- Posibilidad de permitir y denegar trafico
- Azure Front Door
- Application Gateway
- Azure Firewall
- Azure DDoS Protection
- Máquinas virtuales privadas
- Control de trafico
- NSG

Aplicaciones

- Detección de apps criticas
- Detección de servicios críticos

Recursos específicos

- Máquinas Virtuales
- Contenedores
- VNETe
- Microsoft Defender for cloud

Auditoria

Objetivo

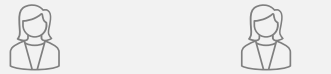
Azure proporciona herramientas integradas para registrar, auditar y evaluar la seguridad de la plataforma, generando métricas y puntuaciones de seguridad. Sin embargo, el uso intensivo de estas herramientas puede incrementar el volumen de datos y comunicaciones, lo que, dependiendo del tamaño de la infraestructura, podría generar sobrecostes en las suscripciones de Azure.

Este assessment tiene como objetivo evaluar el diseño e implementación de seguridad mediante casos de prueba basados en ataques reales, identificando áreas de mejora y oportunidades para fortalecer la protección de la plataforma. Los resultados servirán como base para definir proyectos futuros y estrategias de seguridad proactivas, complementados con auditorías externas y la revisión de puntuaciones de seguridad.

Responsables Principales:

Cliente

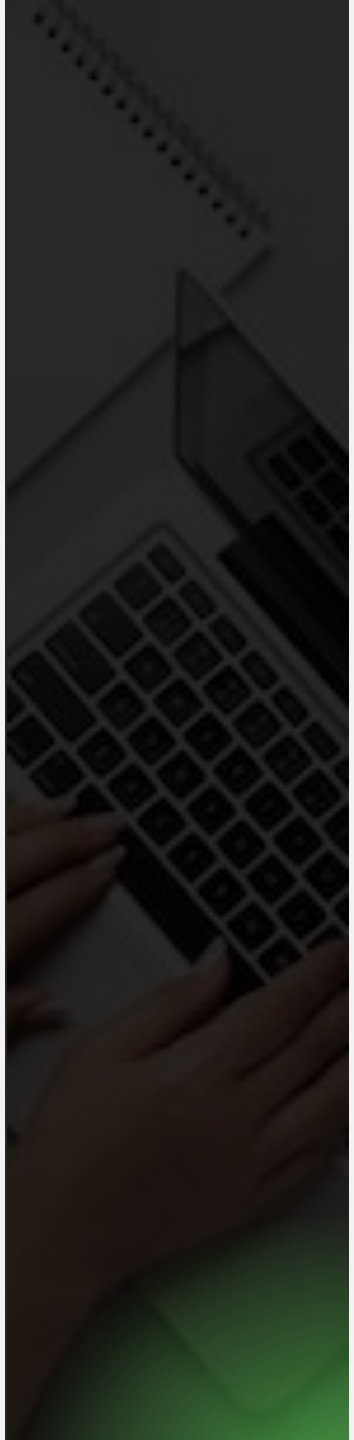
TOYOTA



Responsable de Proyecto

Arquitectura

Arquitecto Cyber



Tareas

- Supervisión de la puntuación de seguridad: Evaluación de las métricas de seguridad en las diferentes plataformas de Azure para identificar áreas de mejora.
- Revisión de consolas y responsables: Análisis de las consolas de administración y asignación de responsabilidades para fomentar una revisión proactiva de actividades sospechosas.
- Simulación de ataques reales: Investigación de posibles brechas de seguridad mediante la simulación de escenarios de ataque basados en amenazas reales.
- Plan de investigación y proactividad: Desarrollo de un plan que priorice la detección temprana y la respuesta rápida ante incidentes.
- Definición de técnicas y acciones: Inclusión en el plan de acción de las técnicas necesarias para alcanzar los objetivos de seguridad.
- Elaboración de presupuesto: Creación de un presupuesto alineado con las acciones técnicas y estratégicas definidas.

Entregables

- Estrategia de investigación y proactividad
- Plan de ejecución de tareas
- Recomendaciones
- Plan de acción y presupuesto asociado.

Plan de acción y control de costes

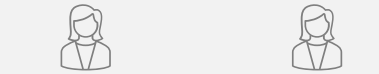
Objetivo

A partir de las tareas realizadas en los ámbitos humano y técnico, se elaborará un plan de acción detallado para abordar carencias, vulnerabilidades y recomendaciones de seguridad identificadas. Este plan incluirá propuestas de solución y una estimación de costes aproximados, asegurando una implementación eficiente y alineada con los objetivos de seguridad.

Responsables Principales:

Cliente

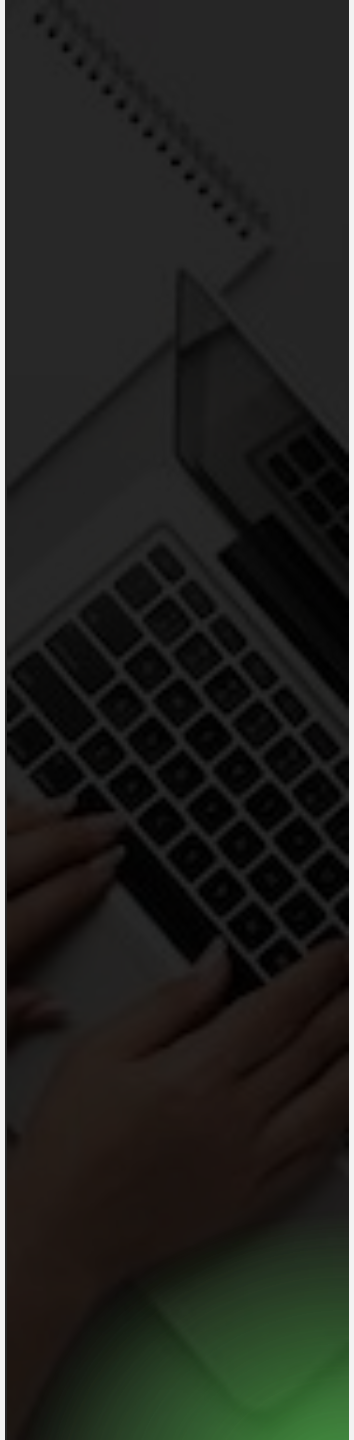
TOYOTA



Responsable de Proyecto

Arquitectura

Arquitecto Cyber



Tareas

- **Definición del plan de acción**: Establecimiento de tareas y soluciones para abordar carencias y vulnerabilidades identificadas.
- **Evaluación de costes**: Análisis de precios y costes asociados a las soluciones propuestas.
- **Control de costes**: Definición de un plan de acción que incluya el control y seguimiento de los costes de cada tarea y solución.
- **Priorización de acciones**: Clasificación de las acciones en:
  - Quick Wins (beneficios inmediatos)
  - Corto plazo
  - Mediano plazo
  - Largo plazo
- **Comparativa de madurez**: Evaluación del nivel de madurez en seguridad respecto al sector, identificando brechas y oportunidades de mejora.

Entregables

- Plan de acción y presupuesto asociado.

Entregable: Informe Final

1. **Introducción**
    1. Contexto
    2. Situación Inicial
2. **Memoria del análisis del plan de seguridad**
    1. Definición del Plan de Acciones tecnológicas
        a. Elementos para la Seguridad y Protección
        b. Elementos para la detección y mitigación
        c. Estrategia de investigación de actividad sospechosa y proactividad
3. **Diseño de plan de Seguridad**
    1. Diseño de las acciones implementables
    2. Plan maestro de acciones priorizadas (Quickwins, Short, Medium y Long Term).
4. **Análisis del coste de implementación**
    1. Coste de implementación de proyecto técnico definido.
    2. Coste de implementación servicio operativo.

03

Servicios Remediación

Servicios Remediación

A continuación, se muestran algunas de las tareas que suelen ir vinculadas al servicio de remediación.

Defender

Cloud Security Posture Management (CSPM)
- Discovery de asignación de identidades y roles
- Detección de exposición de red
- Análisis y remediación de rutas de ataque
- Escaneo de vulnerabilidades y secretos
- Reglas de gobierno para impulsar la remediación
- Cumplimiento normativo y mejores prácticas de la industria

Defender for Cloud
- Análisis y remediación de servidores Cloud y OnPrem
- Análisis y remediación de bases de datos SQL
- Análisis y remediación de Apps Services
- Análisis y remediación de Storage Accounts

Defender for Endpoint
- Análisis y remediación de puestos de trabajo
- Investigación y respuesta automatizadas (AIR)
- Ejecutar escaneo AV en dispositivo remoto
- Aislamiento de dispositivo

Microsoft 365

Directivas y políticas:
- Directivas de seguridad (protección de identidad)
- Gestión de directivas, políticas, alertas de seguridad
- Gestión y control de Microsoft Secure Score (Puntuación y cumplimiento)

Protección de la información:
- Administración de Data Loss Prevention (DLP)
- Administración de registros, ciclo de vida de datos y perdida de información

Roles:
- Gestión y administración de roles de O365 (Exchange online)

Buzones y Exchange:
- Auditoria de buzones
- Sincronización de atributos de Exchange Online

Gobierno y Seguimiento

Procedimientos y estándares:
- Definición de procedimientos y estándares para la gestión de usuarios (alta, baja y modificación).

Seguimiento e informes:
- Consultas e informes a medida sobre estado de usuarios, departamentos, permisos.
- Generación de informes, supervisión, recomendaciones

Seguimiento y gestión del servicio:
- Seguimiento de indicadores y calidad del servicio
- Gestión y resolución de incidencias críticas y escalados
- Planificación de intervenciones, configuraciones y mejoras

IMPORTANTE: *tómense estas tareas como ejemplo, ya que hasta el resultado de la evaluación se desconocerán los ámbitos a remediar.*

Nuestras capacidades en Infraestructura y Seguridad:

Centro de operaciones de Excelencia

MODELO INDUSTRIALIZADO

Somos disciplinados en la definición y aplicación de procesos que nos permitan automatizar parte de las tareas recurrentes y dedicar a nuestras personas a tareas de mayor valor añadido

ACTIVOS PROBADOS

Nuestra especialización nos permite identificar y estandarizar configuraciones, soluciones y formas de hacer, que luego reutilizamos siempre que sea posible en todos nuestros clientes del CoE

EQUIPO MULTIDISCIPLINAR

Nuestro CoE no sólo está formado por técnicos. Contamos con arquitectos, consultores y expertos de otras áreas (Infra, seguridad, datos, desarrollo, etc.) que involucramos siempre que sea necesario

HABILITADORES DE NEGOCIO

Nos gusta entender los negocios para los que trabajamos y ser proactivos a la hora de identificar casos de uso y soluciones.

"Somos cabezas, no sólo manos"

EVOLUCIÓN CONSTANTE

Adaptamos nuestra forma de trabajo, ideas y capacidades al status de las tecnologías y las nuevas capacidades que esta ofrece

GOBIERNO Y MEDICIÓN

Medimos el uso de los casos de uso y soluciones implementadas y evaluamos su retorno con las áreas de negocio que los utilizan

CAPACITACIÓN Y AUTONOMÍA

No queremos estar donde no aportamos valor. Formamos a las áreas para que sean autónomas en el uso y extensión de la plataforma si lo consideran

PARTNERSHIP MICROSOFT

Estamos en contacto directo con arquitectos y equipos de producto de Microsoft nacionales e internacionales, lo que nos permite ir un par de pasos por delante del resto

Alcance de nuestro CoE

UN MODELO END TO END QUE CUBRA LAS NECESIDADES DIARIAS DE NUESTROS CLIENTES

Gobierno, seguimiento y eficiencia

- Garantizamos una correcta organización de los recursos.
- Seguimiento de SLAs y mejora de eficiencias
- Seguimiento del consumo y costes

Equipo Infraestructuras

- Asesoramiento a proyectos
- Diseño y estandarización de arquitecturas
- Participación en el despliegue de soluciones

Equipo Seguridad

- Evaluación nivel madurez seguridad
- Definición de políticas y controles de seguridad
- Formación y Concienciación de usuarios y equipos

Equipo Operaciones

- Monitorización del servicio y respuesta en caso de incidencia
- Gestión de los entornos definidos
- Operación de infraestructuras productivas

Equipo Automatizaciones

- Automatización de las soluciones para mejorar el servicio y reducir costes
- Optimización de tareas recurrentes
- Generación de activos reutilizables

Mejora continua del servicio

- Hacemos revisiones cada tres meses que incorporamos a un plan de mejora
- Revisamos y ajustamos la capacidad a las necesidades reales
- Identificamos nuevas tecnologías que puedan suponer mejoras

RECURSOS DE PRIMER NIVEL ORIENTADOS A CALIDAD, FLEXIBLIDIDAD Y MEJORA CONTINUA

Equipo Soporte

- Desarrollo
- Data & IA
- Moderm work

Stack tecnológico de referencia

Activos en constante evolución

- Procesos y modelos
- Soluciones reutilizables
- Configuraciones estándar

4 especializaciones avanzadas en Seguridad

- Cloud Security
- Threat Protection
- Identity and Access Management
- Info. Protection and Governance

Proveedor Tier 1 CSP

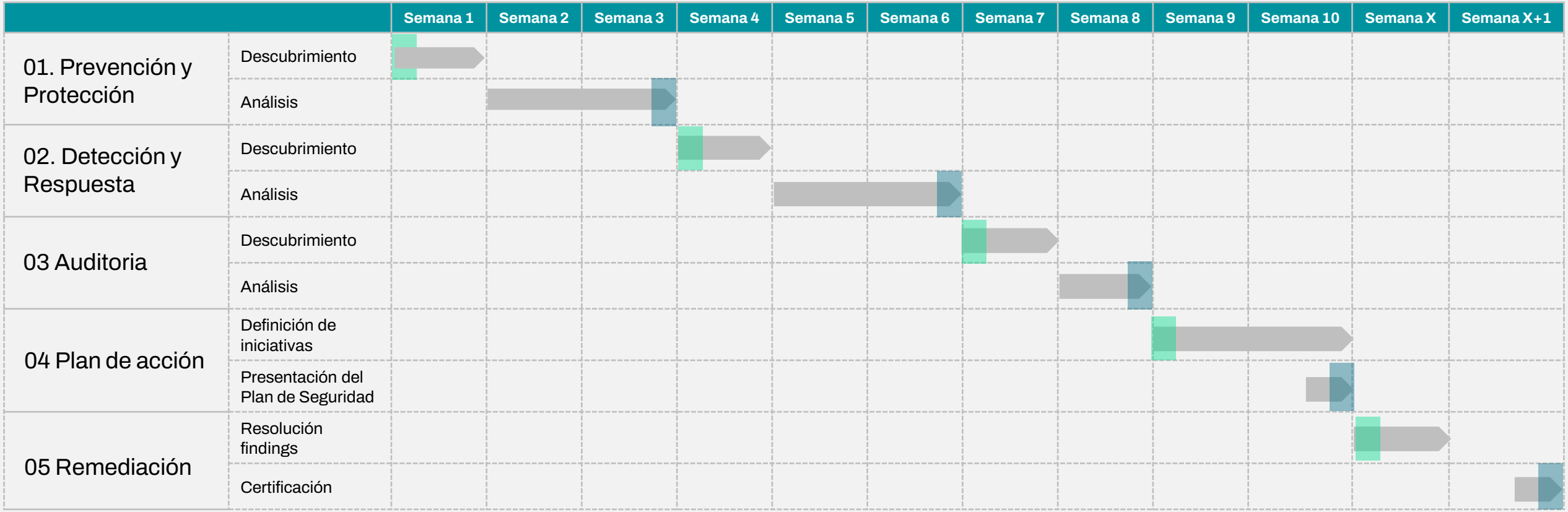
04

Planificación y Equipo de trabajo

Calendario

Inicio

Sesiones de control



ENTREGABLE

- Documento v0.0
- Documento v0.1
- Documento v0.2
  - Zero Trust Maturity assessment Power BI ZT
  - Tabla findings
  - Plan de Seguridad

Equipo

TOKIOTA

Squad de ejecución

Tokiota propone un equipo cuyas capacidades puedan cubrir ambas actividades:

Project Manager

Responsable de Proyecto

Assessment ZeroTrust:

Consultor de Negocio

Proyecto Técnico:

Arq. Ciber y Cloud

Servicio Remediación

Arq. Ciberseguridad

Es necesario que exista un consultor que entienda el problema, sea capaz de entender los riesgos que puede tener el negocio y el impacto con un fallo en la seguridad y que pueda sugerir procesos operativos acordes a la necesidad.

Tokiota presenta en este documento un equipo de especialistas del más alto nivel del mercado (técnicos y consultores) con mucha experiencia en definición de sistemas complejos y acciones de planteamientos de marcos de seguridad en infraestructuras complejas.

Un equipo compuesto, sólo, por los mejores especialistas ciberseguridad y cloud cuyo único propósito es ayudar a aterrizar la definición de un proyecto crítico para el Cliente y conseguir un plan de seguridad realizable y ajustado a unos objetivos concretos.

Seguimiento y Reporting

SEGUIMIENTO Y GOBIERNO

Para garantizar una ejecución en tiempo y forma y garantizar que la solución implantada cubre las necesidades, planteamos un modelo de seguimiento basado en 3 elementos

COMITÉ DE SEGUIMIENTO

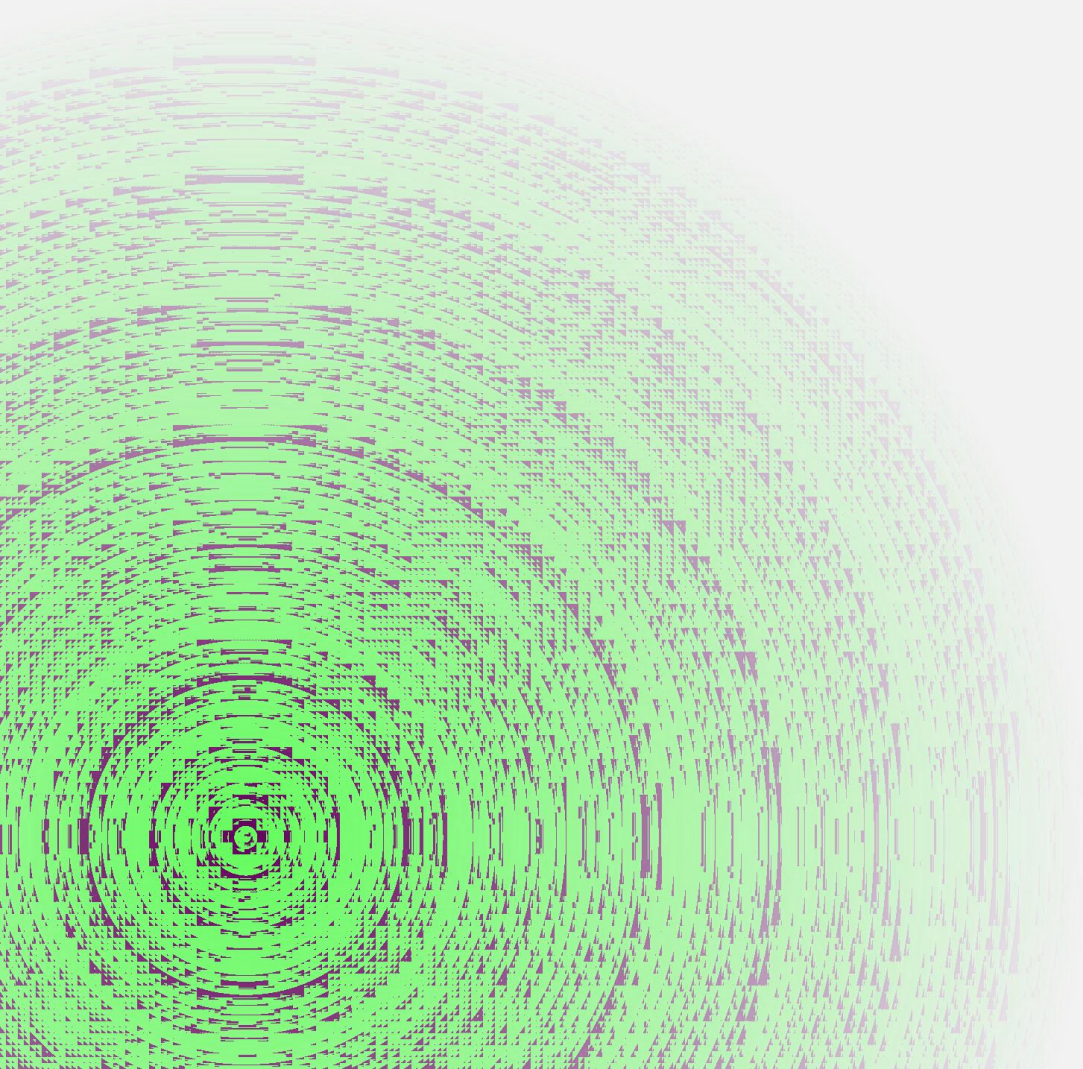
Proponemos que cada 15 días se realice una sesión de seguimiento para compartir el estado de la iniciativa, tareas realizadas, tareas previstas y puntos bloqueantes

PROCEDIMIENTO DE ESCALADO

En cualquier momento, si se produce un problema que se considere bloqueante o afecte al éxito de la migración, se escalará al responsable de la iniciativa por parte de Tokiota, que convocará al Comité de Seguimiento para su análisis, posibles soluciones y toma de decisiones

REPORTING SEMANAL

Al finalizar cada semana, se enviará un informe indicando el avance de la iniciativa, a fin de que todas las partes tengan una visión clara del estado de la iniciativa, tareas realizadas y en curso, puntos bloqueantes y riesgos identificados



C/ Meridional, 9, 08018 Barcelona

Av. del Mediterráneo, 15, 28007, Madrid

C/ Rafael Alberti, 8, 15008, A Coruña