**CLAUSULA DE CONFIDENCIALIDAD**

Esta propuesta es propiedad de GRUPO MICROSYSCOM, S.L. No podrá ser duplicada, duplicada o enviada en su totalidad o en parte para otro propósito que su evaluación. Si un pedido o contrato le es adjudicado a MICROSYSCOM como resultado o en conexión con esta propuesta, el cliente no tiene el derecho a copiar, usar o revelar los datos en los términos estipulados en el contrato. Esta cláusula no limita el derecho del cliente a usar la información contenida en la propuesta si ésta ha sido obtenida de otras fuentes. Toda la información de esta propuesta está sujeta a dicha cláusula.

**Versionado**

Versión: 0.0. Fecha: 26 de noviembre 2024

La información contenida en este documento puede estar sujeta a cambios, previo aviso, convenidos conjuntamente con el cliente. Tales cambios se incluirían en posteriores versiones de la presente propuesta.

**ÍNDICE**

**1.Seguridad Perimetral ………………………………………………………………………….……………………....3**

**1.1 Firewalls**

**1.2 Switch**

**1.3 Acces Point**

**1.4 XDR**

**1.5 SIEM**

**2.Continuidad de negocio……………………………………………………………………………………….….3,4**

**2.1 Router**

**2.2 Copias de Seguridad**

**2.3 Servidores de Respaldo**

**2.4 SAI**

**3.Protección de la información……………………………………………………………………………...4**

* **Seguridad Perimetral de la Empresa.**
* **Firewalls.**

**Problema detectado:** Actualmente todas las sedes menos Félix Boix y Fuenlabrada, carecen de firewalls con licencia, además de no figurar en el Catálogo de Productos y Servicios de Seguridad emitido por el Centro Criptológico Nacional.

**Impacto**: No tener un firewall con licencia activa y que no figure en el **CCN-STIC** tiene impactos importantes:

* **Seguridad reducida**: Sin licencia, el firewall no recibe actualizaciones ni soporte técnico, lo que lo hace vulnerable a ataques y limita sus funcionalidades avanzadas.
* **Incumplimiento normativo**: En sectores regulados (como el público), esto podría infringir el **Esquema Nacional de Seguridad (ENS)**, exponiendo a sanciones y problemas en auditorías.
* **Pérdida de confianza**: Puede generar desconfianza en clientes y afectar contratos, especialmente en sectores que exigen estándares certificados.
* **Costos a largo plazo**: Mayor riesgo de ciberataques, costos de recuperación y necesidad de reemplazo por un equipo certificado.

Contar con un firewall certificado y con licencia activa garantiza mayor seguridad, cumplimiento legal y protección de la red.

**Recomendación**: Recomendamos el despliegue de dispositivos que cumplan con los requerimientos de seguridad exigidos por la NIST 2.0.

**Costo:**

* Adjuntar presupuestos de los Firewalls
* **Switch.**

**Problema detectado:** Ninguna sede tienen los segmentada la red, el Anti-Storm configurado. Además, hay sedes que ni siquiera tienen switches gestionables, que puedan cumplir con los requerimientos de seguridad.

**Impacto**: La falta de segmentación, el Anti-Storm sin configurar y la ausencia de switches gestionables tienen impactos críticos:

* **Seguridad comprometida**: Facilita la propagación de ataques (como ransomware) y expone datos sensibles al no controlar accesos.
* **Problemas de rendimiento**: Sobrecarga la red con tráfico innecesario y afecta aplicaciones críticas al no priorizar el tráfico.
* **Incumplimiento normativo**: Puede violar estándares como el **ENS** o **ISO 27001**, exponiendo a sanciones y problemas en auditorías.

Estas carencias aumentan riesgos, afectan la operatividad y dejan a la red vulnerable.

**Recomendación**: Recomendamos el despliegue de dispositivos que cumplan con los requerimientos de seguridad exigidos por la NIST 2.0, además de las configuraciones oportunas.

**Costo:**

* Adjuntar presupuestos de los Switch para las sedes que carecen de él.
* Adjuntar presupuestos de mano de obra para la configuración por sede.
* **Access Points.**

**Problema detectado:** Ningún SSID está oculto, no hay diferencia entre un SSID corporativo y otro para Invitados u dispositivos móviles. además de que los Router tienen el Wifi activado.

**Impacto**: La falta de **ocultación de los SSID** expone innecesariamente las redes a posibles **escaneos y ataques**, facilitando a intrusos identificar las redes disponibles. La **ausencia de separación entre el SSID corporativo y el de invitados o dispositivos móviles** compromete la seguridad al permitir que dispositivos no controlados compartan la misma red, aumentando el riesgo de accesos no autorizados y propagación de malware.

Además, que los **routers tengan Wi-Fi activado** añade más puntos de entrada vulnerables, ya que estas redes suelen carecer de configuraciones avanzadas de seguridad. Esto dificulta el control y la segmentación del tráfico, poniendo en riesgo la confidencialidad de la información corporativa y reduciendo el rendimiento de la red.

**Recomendación**: Ocultar los SSID corporativos, no difundir la contraseña, crear un SSID de invitados para los externos y móviles, además de desactivar el Wifi en los Routers.

**Costo:**

* Adjuntar presupuestos de mano de obra para la configuración por sede.
* **XDR.**

**Problema detectado:** Carencia de XDR en varios dispositivos y la falta de add-ons y configuraciones necesarias para la seguridad de los dispositivos.

**Impacto**: La **carencia de XDR (Extended Detection and Response)** en varios dispositivos limita la capacidad de detectar, correlacionar y responder a amenazas de forma integral, ya que no se obtiene una visión unificada de los eventos de seguridad. Esto aumenta el tiempo de detección y resolución de incidentes, dejando a los dispositivos expuestos a ataques sofisticados.

Por otro lado, la **falta de add-ons y configuraciones necesarias para la seguridad** compromete las capas de protección. Esto incluye la ausencia de funcionalidades críticas como control de acceso, protección contra exploits, y cifrado, lo que abre puertas a vulnerabilidades que pueden ser explotadas fácilmente por atacantes, resultando en un alto riesgo para la integridad de los datos y la continuidad operativa.

**Recomendación**: Recomendamos el despliegue del XDR Vigia Defender es un plan Total Security la cual alberga configuraciones y complementos tales cómo Antimalware, Network Attack Defense, Advanced Threat Control, Cifrado, SandBoxing entre otros.

**Costo:**

* Adjuntar presupuestos de Vigía Defender.
* **SIEM.**

**Problema detectado:** No existe ningún tipo de sistema SIEM, en cargado de recopilar, analizar y gestionar todos los eventos de seguridad.

**Impacto**: La **ausencia de un sistema SIEM (Security Information and Event Management)** impide la centralización, análisis y correlación de los eventos de seguridad, lo que genera una **visión fragmentada del entorno**. Esto dificulta la detección temprana de amenazas y el cumplimiento normativo, además de aumentar el tiempo de respuesta ante incidentes. Sin un SIEM, se pierde la capacidad de identificar patrones de ataque, gestionar alertas de forma eficiente y priorizar acciones críticas, lo que deja a la organización vulnerable frente a ataques complejos y ciberamenazas persistentes.

**Recomendación**: Recomendamos el despliegue de un sistema SIEM conectado a todos los componentes de seguridad y monitoreo para poder gestionar todos los eventos y poder actuar con la mayor rapidez posible.

**Costo:**

* Adjuntar presupuestos del despliegue e implementación de Vigia Monit
* **Continuidad de Negocio.**
* **Routers.**

**Problema detectado:** Ninguna sede cuenta con un sistema de conectividad a internet que forme parte de diferente ISP.

**Impacto**: La falta de conectividad a Internet mediante diferentes ISP (proveedores de servicios de Internet) genera una **dependencia total de un único proveedor**, lo que aumenta la vulnerabilidad ante caídas o interrupciones del servicio. Este único punto de fallo puede llevar a una **pérdida de conectividad completa** en caso de problemas técnicos, afectando la continuidad operativa, la productividad y el acceso a sistemas críticos. Además, esta carencia impide implementar mecanismos de redundancia y balanceo de carga, esenciales para garantizar un acceso confiable y minimizar el impacto de fallos en el servicio.

**Recomendación**: Recomendamos el despliegue de sistemas de conectividad a internet con tecnologías cómo FTTH o 4G de diferentes proveedores en las sedes que alberguen un número considerable de trabajadores o alberguen dispositivos esenciales para los empleados que se encuentren fuera de la sede dónde este dispositivo se aloja.

**Costo:**

* Adjuntar presupuestos de los routers de backup.
* **Copias de Seguridad**

**Problema detectado:** Carencia de copia de seguridad de la información en ninguna sede que no sea la Central, ni de buzones de correo.

**Impacto**: La falta de copias de seguridad tanto en las sedes fuera de la central como de los buzones de correo expone a la organización a una **pérdida irreparable de datos críticos** en caso de fallos técnicos, ciberataques, robos o errores humanos. En las sedes, esto afecta la continuidad operativa local, mientras que la ausencia de respaldos de correo electrónico compromete comunicaciones clave y documentación sensible. Además, sin copias de seguridad, la recuperación de información es prácticamente imposible, lo que aumenta el tiempo de inactividad, los costos asociados y el riesgo de incumplimiento de normativas relacionadas con la protección y conservación de datos.

**Recomendación**: Centralizar toda la información para la facilidad y reducción de costes de las copias de seguridad, despliegue de sistema de copias de seguridad con un sistema cliente servidor, de forma automática y bajo cifrado. Implementación de un sistema de copias de seguridad tanto de los buzones de correo cómo de SharePoint.

Recomendamos contactar con vuestro proveedor de ERP para saber si existe algún sistema de backup aislado del dónde se encuentre lógicamente el servidor.

**Costo:**

* Adjuntar presupuestos de las copias de seguridad.
* **Presupuesta para la migración de la información y restructuración de permisos en el punto 3.3 Control de acceso.**
* **Presupuesta de las copias de seguridad de los correos y de SharePoint en el punto 3.2 Seguridad en el correo.**
* **Servidores de Respaldo.**

**Problema detectado:** Actualmente no existen servidores de respaldo de ningún NAS, ni del DC.

Desconocemos el proveedor del ERP.

**Impacto**: La **ausencia de servidores de respaldo** para los NAS y el controlador de dominio (DC) deja a la organización vulnerable ante fallos catastróficos, ya que no habría forma de recuperar datos críticos o restaurar servicios esenciales, como la autenticación de usuarios o el acceso a archivos. Esto puede paralizar las operaciones, aumentar los tiempos de inactividad y generar costos significativos.

**Recomendación**: Centralizar toda la información para la facilidad para facilitar la replicación entre NAS, Integración del DC con el sistema de Microsoft en Azure. Contactar con el proveedor del ERP para el conocimiento de existencia u carencia de un servidor de respaldo.

**Costo:**

* Adjuntar presupuesto de un servidor de respaldo del NAS.
* Adjuntar presupuesto si procede de un servidor nuevo para hostear un nuevo DC actualmente tienen un EXSI 7, sobre un HPE Proliant ML350 Gen10, 64 de RAM y 8CPUs a 2.10GHz.
* Adjuntar presupuestos de mano de obra para la creación de un servidor en local y licencia de Windows Server 2022 Estándar.
* Adjuntar presupuesto de integración del DC con Azure.
* Adjuntar presupuestos del cambio de 51 licencias de Windows home a pro y la migración de los perfiles.

**2.4 SAI (Sistema de Alimentación Ininterrumpida)**

**Problema detectado:** Actualmente sólo en la sede central cuenta con un SAI que proteja los elementos críticos de la oficina y con una tarjeta de red que permita la gestión de servicios, eventos e informes del estado del mismo.

**Impacto**: La **falta de SAIs (Sistemas de Alimentación Ininterrumpida)** en las sedes expone los elementos críticos a interrupciones eléctricas, lo que puede provocar **pérdida de datos**, daños en el hardware y **caídas inesperadas de servicios esenciales**. Además, la ausencia de una **tarjeta de red para la gestión remota** limita la capacidad de monitorizar y responder proactivamente a eventos relacionados con el SAI, como fallos de batería o sobrecargas. Esto incrementa el riesgo de inactividad prolongada y dificulta la continuidad operativa en todas las sedes.

**Recomendación**: Centralizar toda la información para el ahorro en cuanto a la potencia de SAIs y la implementación de SAI cuya potencia esté relacionada con los dispositivos críticos a los que proporcione alimentación.

**Costo:** Adjuntar presupuestos de los SAI.

* **Protección de la Información**

**3.1 Controlador de Dominio**

**Problema detectado:** Actualmente sólo los equipos de la sede central tienen equipos dentro de un dominio. Además de que este dominio está bajo un DC (Controlador de Dominio) con un sistema operativo obsoleto, cómo lo es Windows Server 2008 R2. También muchos de los equipos tienen un sistema operativo Home, y no uno Pro, que permite la integración de los equipos bajo un controlador de dominio. No existe un sistema de MFA en los inicios de sesión de Windows. Tampoco existen reglas de seguridad mínima según la CIS.

**Impacto** La combinación de estos problemas genera un entorno **altamente vulnerable y difícil de gestionar**. Tener un **dominio centralizado solo en una sede** y con un **Controlador de Dominio obsoleto (Windows Server 2008 R2)** expone a la organización a riesgos graves de seguridad debido a la falta de soporte y actualizaciones, además de posibles incompatibilidades con sistemas modernos.

El uso de **sistemas operativos Home** en lugar de versiones Pro limita la capacidad de integrar equipos en el dominio y aplicar políticas de seguridad centralizadas, dejando dispositivos con configuraciones inconsistentes y vulnerables.

La **falta de MFA** en los inicios de sesión facilita accesos no autorizados, aumentando el riesgo de compromisos por ataques de fuerza bruta, phishing o robo de credenciales. Además, la **ausencia de reglas de seguridad mínimas conforme a estándares como CIS** impide establecer una base sólida de protección, exponiendo los equipos y sistemas a brechas de seguridad y ataques dirigidos.

En conjunto, estas deficiencias ponen en riesgo la **confidencialidad, integridad y disponibilidad** de los sistemas, afectando la continuidad operativa y exponiendo a la organización a sanciones legales y pérdida de reputación.

**Recomendación**: Migración del DC basado en Windows Server 2008 R2 a Windows Server 2022 además de la integración del DC con Azure para una mayor accesibilidad de los equipos que está en otras sedes al DC, además de tener una réplica en el Cloud del DC. Cambio de licencias de todos los dispositivos con Windows Home, a Windows Pro. Implementación de GPOs para cumplir con los estándares CIS en todos los equipos.

**Costo:**

* **Propuesta de la migración de Windows Server 2008 R2 a Windows Server 2022 y de la implementación con Azure en el apartado 2.3 Servidores de respaldo.**
* Adjuntar presupuesto de Vigia MFA para 100 usuarios, 95201.0S1 (Referencia de Also) con los add-ons de 67005.6SPMFA1 (Referencia de Also)
* Adjuntar presupuesto para la implementación de GPOs con los requisitos de seguridad básicos recomendados por la CIS.
* Adjuntar presupuesto para el cambio de licencias Windows Home de 51 licencias.
* **Protección de la Información**

**3.2 Seguridad en el Correo**

**Problema detectado:** Existe una incorrecta configuración del dominio en lo que respecta al DKIM, DMARC, ningún sistema de reportes, ni BIMI. Además, no existe ningún tipo de filtro en la recepción de correo ni un sistema que permita la educación de los empleados ante phishing.

Los usuarios no tienen el MFA activado en sus correos.

**Impacto**: La **incorrecta configuración del dominio** en relación a DKIM, DMARC y la falta de BIMI expone a la organización a un alto riesgo de **suplantación de identidad (spoofing)** y ataques de phishing, ya que no se asegura la autenticidad de los correos enviados ni se aplican políticas claras para manejar mensajes no autorizados.

Además, la **ausencia de sistemas de reporte** impide detectar y responder proactivamente a intentos de abuso del dominio.

La **falta de filtros de correo** para bloquear mensajes maliciosos y un **programa de educación sobre phishing** para los empleados aumenta la vulnerabilidad a ciberataques, lo que podría resultar en compromisos de datos sensibles, pérdida de confianza de los clientes y posibles sanciones regulatorias por incumplimientos de seguridad.

La ausencia de un sistema de autentificación mediante múltiples métodos fácil el acceso a los correos y recursos asociados al correo cómo lo son SharePoint a usuarios no autorizados.

**Recomendación**: Cambios de las configuraciones del dominio, implementación de un filtro de correos y de un programa de educación sobre el phishing, activar obligatoriamente un sistema de MFA en los accesos de todos los correos.

**Costo:**

* Adjuntar presupuestos de los cambios correspondientes sobre el dominio.
* Adjuntar presupuestos del Hornet con los add-ons de copia de seguridad de correos y SharePoint y programa de educación al trabajador.

**3.3 Controles de acceso**

**Problema detectado:** El acceso a la información es muy irregular y mucha de la información en varias sedes se puede acceder sin credenciales. El acceso a los dispositivos críticos cómo lo son la electrónica de red, los NAS y el DC no está protegido en muchas sedes.

**Impacto**: El **acceso irregular a la información** y la posibilidad de acceder a datos sin credenciales en varias sedes representan un **grave riesgo de seguridad**. Esto facilita el acceso no autorizado, pudiendo provocar **pérdida, robo o manipulación de datos sensibles**, además de incumplimientos normativos como el RGPD.

La **falta de protección en dispositivos críticos** como la electrónica de red, los NAS y el DC amplifica el riesgo, permitiendo posibles **ciberataques internos o externos**, configuraciones erróneas y caídas de servicios esenciales. Este entorno vulnerable compromete la **confidencialidad, integridad y disponibilidad** de los sistemas, afectando directamente la continuidad operativa y la confianza en la infraestructura de TI.

**Recomendación**: Centralizar toda la información para la facilitar la gestión de accesos tanto a nivel lógico cómo físico. Bloquear el acceso físico a los elementos críticos de la red bajo llave cómo mínimo y tener un control de quién accede a las llaves y durante cuánto tiempo.

Los accesos a la información lógicamente deben de estar bajo credenciales personales con los permisos que realmente necesite, que las contraseñas caduquen cómo máximo a los 90 días. Si el acceso a la información es a través de Wifi o no está la información locamente, deberá de ser mediante una VPN con MFA.

**Costo:**

* Adjuntar presupuestos de la migración de los Datos.
* Adjuntar presupuesto del NAS Core.
* Adjuntar presupuesto de los reacondicionamientos.
* Adjuntar Presupuesto de los RACKS faltantes.

**3.4 XDR**

**Problema detectado:** Los equipos no están encriptados y los que están encriptados están por el anterior soporte de IT, el cuál desconocen las credenciales. Además, las unidades de almacenamiento externas están activadas.

**Impacto**: La **falta de encriptación en los equipos** pone en riesgo la confidencialidad de los datos almacenados, especialmente en caso de pérdida o robo de dispositivos. Los equipos que están encriptados, pero cuyas credenciales son desconocidas, representan un **obstáculo operativo**, ya que la información en ellos no puede recuperarse ni gestionarse, lo que genera ineficiencias y posibles pérdidas de datos importantes.

Además, la **activación de unidades de almacenamiento externas sin control** aumenta significativamente el riesgo de fuga de información confidencial y la introducción de malware. Esto expone a la organización a **violaciones de seguridad**, sanciones regulatorias y pérdida de confianza por parte de clientes y socios.

**Recomendación**: Vigia Defender, permite el bloqueo de las unidades de almacenamientos externas y el encriptado de los equipos.

**Costo:**

* Propuesta para Vigia Defender en el apartado 1.4 XDR.