Intecap

CONTRATO NÚMERO GE GUION AL GUION DIECISIETE GUION DOS MIL VEINTISÉIS (GE-AL-17-2026). En la ciudad de Guatemala, el veinticinco de marzo de dos mil veintiséis. NOSOTROS: Por una parte, **ARNALDO ADEMAR ALVARADO CIFUENTES,** de cincuenta y cuatro años, casado, guatemalteco, Ingeniero, de este domicilio, me identifico con Documento Personal de Identificación (DPI), Código Único de Identificación (CUI) dos mil quinientos noventa y ocho espacio sesenta y seis mil cuatrocientos treinta y uno espacio mil seiscientos uno (2598 66431 1601), extendido por el Registro Nacional de las Personas de la República de Guatemala; actúo en mi calidad de Sub Gerente del Instituto Técnico de Capacitación y Productividad "INTECAP", con cuentadancia número dos mil veintidós guion cien guion ciento uno guion diecinueve guion cero veintinueve (2022-100-101-19-029); acredito mi personería con: a) Certificación del punto Quinto del acta número treinta y seis guion dos mil dieciséis (36-2016), de la Honorable Junta Directiva del "INTECAP"; y b) Certificación del Acta de toma de posesión del cargo número ochenta y cuatro guion dos mil dieciséis (84-2016), de fecha veintiocho de octubre de dos mil dieciséis, extendida por la División de Recursos Humanos del "INTECAP", en lo sucesivo denominado "INTECAP"; y por la otra parte, **ESTUARDO JOAQUÍN OLIVARES RUIZ,** de cincuenta y nueve años, casado, empresario, guatemalteco, de este domicilio, me identifico con Documento Personal de Identificación (DPI), Código Único de Identificación (CUI) dos mil ciento setenta y seis espacio cuarenta mil sesenta espacio cero ciento uno (2176 40060 0101), extendido por el Registro Nacional de las Personas de la República de Guatemala; actúo en mi calidad de Administrador Único y Representante Legal de la entidad "Red Óptima, Sociedad Anónima", inscrita en el Registro

Mercantil General de la República de Guatemala, al número ciento diecisiete mil trescientos treinta (117330) folio veintinueve (29) libro doscientos once (211) de Sociedades; propietaria de la empresa de nombre comercial "Red Optima", inscrita en el Registro Mercantil General de la República de Guatemala, al número seiscientos setenta y cinco mil cuatrocientos sesenta y cuatro (675464) folio seiscientos cuarenta y uno (641) del libro seiscientos treinta y siete (637) de Empresas Mercantiles, calidad que acredito con el acta notarial de fecha dos de junio de dos mil veintitrés, autorizada en esta ciudad por el Notario Jorge Luis Molina Del Cid, debidamente inscrita en el Registro Mercantil General de la República de Guatemala, bajo el número setecientos un mil quinientos doce (701512), folio treinta y uno (31), libro ochocientos dieciocho (818) de Auxiliares de Comercio; señalo como lugar para recibir notificaciones en la sexta (6ta) avenida uno guion treinta y seis (1-36) zona catorce (14), Edificio Plaza Los Arcos, Oficina cuatro A (4A) de esta ciudad, en lo sucesivo seré denominado "Red Optima". Ambos comparecientes manifestamos hallarnos en el libre ejercicio de nuestros derechos civiles y que la representación que se ejercita es suficiente conforme a la Ley para la celebración del presente **CONTRATO DE COMPRAVENTA** contenido en las cláusulas siguientes:

PRIMERA: BASE LEGAL: El presente contrato se suscribe con fundamento en lo que prescribe la Ley de Contrataciones del Estado, Decreto cincuenta y siete guion noventa y dos (57-92) del Congreso de la República de Guatemala y su Reglamento contenido en el Acuerdo Gubernativo ciento veintidós guion dos mil dieciséis (122-2016); Bases de Cotización número setenta y seis guion dos mil veintiséis (76-2026), cuyo objeto es la adquisición de licencia de herramienta de concientización en ciberseguridad; bajo el número de operación Guatecompras

/veinticinco/ /2025/

veintiocho millones trescientos setenta y ocho mil trescientos veintiséis (NOG 28378326); Acta número SC guion cero doce guion dos mil veintiséis (SC-012-2026), de fecha veintisiete de enero de dos mil veintiséis; Acta número SC guion cero treinta y cinco guion dos mil veintiséis (SC-035-2026), de fecha doce de febrero de dos mil veintiséis, de recepción y apertura de plicas; Acta número SC guion cero treinta y siete guion dos mil veintiséis (SC-037-2026), de fecha dieciocho de febrero de dos mil veintiséis, de calificación y adjudicación de oferta; cotización contenida en formulario electrónico COT guion dos mil veintiséis guion veintiocho millones trescientos setenta y ocho mil trescientos veintiséis guion ochenta y ocho millones ciento noventa y seis mil seiscientos sesenta y seis (COT-2026-28378326-88196666), código de autenticidad doscientos noventa y tres B treinta y seis F uno (293B36F1), de fecha once de febrero de dos mil veintiséis; oferta de "Red Optima", de fecha once de febrero de dos mil veintiséis; Acuerdo de aprobación de la adjudicación número GE guion ciento cincuenta y uno guion dos mil veintiséis (GE-151-2026), de fecha veintisiete de febrero de dos mil veintiséis; y Memorando número SS guion veintisiete guion dos mil veintiséis (SS-27-2026), de fecha dos de marzo de dos mil veintiséis. Se tiene por incorporada al presente contrato la documentación anteriormente citada.

SEGUNDA: OBJETO DEL CONTRATO: Adquisición de licencia de herramienta de concientización en Ciberseguridad; para el efecto "Red Optima" vende al "INTECAP" lo siguiente**: un (1) Licenciamiento para concientización de usuarios**; marca KnowBe cuatro (KnowBe4); país de origen Estados Unidos; para mil quinientos (1,500) colaboradores, por un plazo de doce (12) meses, con las siguientes características: **CONSOLA DE ADMINISTRACIÓN:** es agnóstica

al sistema operativo y funciona exclusivamente a través de la web mediante protocolos estándar (HTTPS), no requiere la instalación de software cliente, complementos como Java, ni extensiones propietarias para que los administradores gestionen la herramienta o los usuarios consuman el contenido; la consola de administración de KnowBe4 está diseñada bajo una arquitectura web responsive, optimizada para funcionar en navegadores modernos de escritorio y tabletas, esto permite gestionar campañas, revisar reportes y administrar usuarios sin depender de una aplicación dedicada, adaptándose a diferentes resoluciones de pantalla; incluye un (1) dashboard dinámico que visualiza en tiempo real el Phish-prone Percentage (tasa de propensión) y el Virtual Risk Officer (VRO), este último utiliza algoritmos para calcular el puntaje de riesgo individual y grupal, permitiendo identificar brechas de seguridad mediante métricas de comportamiento comparadas con el estándar de la industria. **GESTIÓN DE USUARIOS:** soporta la automatización de usuarios mediante Active Directory Integration (ADI) para entornos on-premise y el estándar SCIM para entornos de nube como Azure AD (Entra ID) y Google Workspace, esto permite la sincronización automática de altas, bajas y pertenencia a grupos sin intervención manual; permite la automatización total de la base de usuarios y su estructura organizacional, utiliza la herramienta ADI (Active Directory integration) para entornos locales y el protocolo SCIM para directorios en la nube, esta sincronización asegura que cualquier cambio en los grupos de seguridad o unidades organizativas del cliente se refleje automáticamente en la consola, facilitando la asignación de cursos y campañas de phishing basadas en la pertenencia a grupos específicos; permite la segmentación granular de la audiencia mediante la selección de Grupos

Específicos o Unidades Organizativas al momento de configurar cualquier campaña de Phishing o Entrenamiento, gracias a la sincronización con el directorio corporativo, un administrador puede dirigir ataques simulados de alta complejidad exclusivamente al departamento de Finanzas o asignar cursos de codificación segura solo al grupo de Desarrolladores, permitiendo una gestión de riesgos diferenciada por perfil de puesto; cumple mediante su motor de Simulación de Ingeniería Social (Phishing, Vishing y Smishing), permite a los administradores enviar ataques simulados que imitan amenazas reales para evaluar la vulnerabilidad de los usuarios; cumple mediante un motor de Simulación de Phishing (PST - Phishing Security Test) totalmente automatizable, este motor permite ejecutar campañas masivas o dirigidas (Spear Phishing) utilizando una biblioteca de miles de plantillas basadas en amenazas reales; cumple mediante el módulo Phishing Templates, que ofrece acceso a una biblioteca de miles de plantillas preconfiguradas basadas en ataques reales, categorizadas por industria y nivel de dificultad, el sistema incluye un Editor de Plantillas "WYSIWYG" (lo que ves es lo que obtienes) que permite personalizar completamente el remitente, el cuerpo del mensaje y el dominio de envío; cumple mediante la función de Phishing Campaigns, que permite una automatización completa bajo el concepto "configurar y olvidar", el motor permite una programación flexible donde el administrador define la frecuencia (una vez, semanal, mensual o trimestral) y el periodo de envío (ej. de lunes a viernes en horario laboral). **GESTIÓN DE CONTENIDO DE CAPACITACIÓN:** mediante su módulo ModStore, que es la biblioteca de contenido de concienciación en seguridad más grande del mundo, los administradores y usuarios tienen acceso a un catálogo centralizado que incluye módulos de capacitación interactivos,

videos de calidad cinematográfica; cumple mediante la funcionalidad de Smart Groups y campañas de capacitación dirigidas, permite la asignación manual de cursos a individuos o grupos específicos, pero su mayor fortaleza es la automatización basada en el comportamiento; cumple mediante su motor de Reportes Dinámicos, que permite un monitoreo detallado y en tiempo real del avance en las capacitaciones. **REPORTES Y ANALÍTICA:** se desarrolla mediante un robusto motor de reportes y analíticas que transforma los datos de las campañas en inteligencia de seguridad; ofrece más de sesenta (60) tipos de reportes diferentes que permiten analizar el comportamiento de los usuarios desde múltiples dimensiones; mediante su motor de reportes avanzados, que permite a los administradores filtrar y segmentar datos para crear vistas personalizadas según las necesidades de la organización; mediante la generación de métricas avanzadas centradas en el comportamiento humano ante amenazas; rastrea y visualiza automáticamente mediante su motor de Análisis de Tendencias y Segmentación Jerárquica, visualiza el progreso de la cultura de seguridad a lo largo del tiempo y desglosa por cualquier atributo importado desde el directorio corporativo. **GESTIÓN DE ALERTAS:** permite mediante un sistema robusto de Notificaciones de Consola y Alertas por Correo, configurar alertas automáticas para administradores ante eventos críticos y recordatorios personalizados para los usuarios finales; mediante la función de Reportes Programados (Scheduled Reports) y el resumen ejecutivo, los administradores pueden configurar el sistema para que genere y envíe automáticamente un resumen periódico (semanal, mensual o trimestral) directamente a su bandeja de entrada o a la de los interesados (CISO, Gerencia, Auditores); mediante la funcionalidad Virtual Risk Officer (VRO), un motor de

análisis de datos que utiliza aprendizaje automático para calcular y monitorear la postura de riesgo de la organización, el VRO asigna un Puntaje de Riesgo (Risk Score) dinámico tanto a usuarios individuales como a grupos y a la empresa en su totalidad; mediante su motor de Plantillas de Phishing Dinámicas que utilizan marcadores de posición (placeholders) y lógica condicional para personalizar el contenido automáticamente; por medio de su equipo de investigación KnowBe4 Research y la integración de Inteligencia de Amenazas (Threat Intelligence) en tiempo real, actualiza semanalmente su biblioteca de simulaciones basándose en ataques reales detectados "en la naturaleza"; mediante su motor de Landing Pages (Páginas de Aterrizaje), las cuales están diseñadas con tecnología HTML5 y CSS responsive, esto garantiza que, cuando un usuario hace clic en un enlace de phishing simulado desde cualquier dispositivo (smartphone, tablet o PC), la página de error o de retroalimentación se adapte perfectamente al tamaño de la pantalla; mediante el uso de Landing Pages (Páginas de Aterrizaje) de Retroalimentación Inmediata, en el momento exacto en que un usuario hace clic en el enlace simulado, es redirigido a una página que debe ser personalizada al cien por ciento (100%) con los logos y el tono de comunicación del INTECAP; cumple mediante una arquitectura de plataforma única, donde la gestión de las simulaciones de phishing y la administración del sistema de gestión de aprendizaje (LMS) residen en la misma consola; permite la creación y envío de simulaciones de phishing que incluyen archivos adjuntos maliciosos simulados, el administrador puede elegir entre plantillas predefinidas o crear una personalizada utilizando el Attachment Manager; permite la gestión y carga masiva de usuarios mediante múltiples métodos adaptables a la infraestructura del cliente, garantizando que la base de

datos de empleados esté siempre actualizada para las campañas de simulación; mediante una Consola de Administración Multilingüe diseñada bajo principios de usabilidad moderna (UX/UI), la interfaz permite a los administradores configurar su entorno de trabajo completamente en español, facilitando la gestión de campañas, la lectura de reportes y la configuración de usuarios sin barreras idiomáticas; por medio del Executive Dashboard (Tablero de Control Ejecutivo), que proporciona una visión consolidada y de alto nivel sobre la postura de seguridad; cumple mediante la herramienta ASAP (Automated Security Awareness Program), este es un generador inteligente que crea un programa de capacitación personalizado y listo para ejecutar en pocos minutos, mediante la potente funcionalidad de Smart Groups (Grupos Inteligentes), a diferencia de los grupos estáticos tradicionales, los Smart Groups funcionan basados en reglas lógicas condicionales que evalúan los atributos y el comportamiento de los usuarios en tiempo real; cumple mediante el uso de Smart Groups combinado con Campañas Automatizadas, lo que permite crear flujos de trabajo de ciclo de vida completo para el usuario sin intervención manual. **LA HERRAMIENTA CUBRE LO SIGUIENTE:** el ModStore, que es reconocido como el mercado de contenido de concientización de seguridad más grande del mundo, no se limita a videos estáticos, sino que ofrece una biblioteca masiva y en constante crecimiento; cumple mediante su enfoque de Simulación Multicanal, que permite a los administradores replicar ataques de ingeniería social que van más atlá del correo electrónico tradicional, utilizando vectores que los ciberdelincuentes reales emplean para evadir perímetros de seguridad; la solución cumple mediante una arquitectura de SaaS (Software as a Service) que centraliza todas las operaciones en un único punto de control accesible desde cualquier

navegador moderno, eliminando la necesidad de instalaciones locales de pesados clientes de administración; mediante herramientas diagnósticas y predictivas que van más allá del simple reporte de clics, permitiendo medir la madurez real de la organización; mediante la combinación de Smart Groups y Event-Driven Training (Capacitación basada en eventos). Este motor permite diseñar flujos de trabajo que reaccionan de manera autónoma al comportamiento específico de cada usuario, eliminando la necesidad de intervención manual por parte del administrador; está diseñado para operar de forma integrada con el ecosistema de TI corporativo, permitiendo la automatización de la identidad, la seguridad y la respuesta a incidentes; mediante la aplicación móvil KnowBe4 Learner App, diseñada específicamente para facilitar el acceso a la capacitación en ciberseguridad sin depender de una computadora de escritorio. Esta aplicación está disponible tanto para iOS como para Android; mediante una arquitectura Cross-Browser (Navegación cruzada), garantizando que tanto la consola de administración como el portal de capacitación del usuario (Learner Experience) funcionen de manera óptima en las versiones modernas de los navegadores más utilizados en entornos corporativos. Google Chrome: compatibilidad total tanto en Windows, macOS como en dispositivos móviles, Mozilla Firefox: soporte completo para todas las funciones interactivas y visualización de módulos SCORM. Microsoft Edge: Optimizado para el motor Chromium de Edge, asegurando una integración fluida en ecosistemas Microsoft, Safari: soporte oficial para usuarios de macOS e iOS. **PROGRAMA DE CONCIENTIZACIÓN**: se proporciona el ModStore, que ofrece acceso a la biblioteca de concientización en seguridad más grande y diversa del mundo, al superar ampliamente el requisito de mil trescientos (1,300) contenidos, permite

a las organizaciones mantener sus programas frescos y atractivos, evitando la "fatiga de capacitación" de los empleados; mediante una flexibilidad total en la gestión de contenidos y personalización de la experiencia del usuario, asegurando que el material educativo se sienta como una parte integral de la cultura organizacional. Contenidos SCORM Descargables: permite a los clientes con niveles de suscripción específicos descargar los módulos de capacitación en formato SCORM para ser cargados en un Sistema de Gestión de Aprendizaje (LMS) externo propio, esto permite centralizar el entrenamiento si la empresa ya cuenta con una plataforma corporativa. Enfoque Mobile-First: todo el contenido moderno del ModStore está desarrollado en HTML cinco (HTML5), lo que garantiza que los cursos sean responsivos y funcionen perfectamente en smartphones y tablets a través de un navegador o de la KnowBe cuatro (KnowBe4) Learner App. Personalización de Marca (Branding), Logo e Imagen: carga el logotipo de la entidad y colores institucionales para que aparezcan en el portal de capacitación del empleado (Learner Experience). Páginas de Destino y Correos: Tanto las plantillas de phishing como las páginas de aterrizaje tras un fallo pueden personalizarse con la imagen corporativa para aumentar la credibilidad o reforzar el mensaje de que es una iniciativa interna oficial; permite una gestión total del ciclo de vida educativo, ofreciendo flexibilidad absoluta en la ejecución y el reconocimiento del aprendizaje. Campañas Ilimitadas: No existen restricciones en el número de campañas de capacitación o phishing que se puede lanzar durante el periodo de suscripción, se puede segmentar por departamentos, niveles de riesgo o regiones geográficas sin costos adicionales por campaña. Certificados Corporativos: Al completar con éxito los módulos, el sistema puede generar automáticamente certificados de finalización, estos

certificados son personalizables, puede incluir la firma del responsable de seguridad (CISO) o el logo de la entidad para darles validez formal dentro del plan de carrera del empleado. Cadencia Variable: puede programar la frecuencia de los cursos según las necesidades, desde campañas intensivas semanales hasta refuerzos trimestrales o anuales. Gracias a los Smart Groups, la cadencia puede ser dinámica; los usuarios de "Alto Riesgo" pueden recibir capacitación con mayor frecuencia que el resto; utiliza mecánicas de juego avanzadas para aumentar el compromiso (engagement) de los empleados, transformando la capacitación obligatoria en una experiencia competitiva y motivadora mediante el Learner Dashboard; incluye AI-Driven Recommendations (Motor de Recomendaciones impulsado por IA), una funcionalidad integrada en el portal del usuario (Learner Experience) que utiliza aprendizaje automático para personalizar la ruta de aprendizaje de cada empleado. Aprendizaje Automático (ML): el algoritmo analiza los cursos que el usuario ya ha completado, sus intereses declarados (si se habilitan) y las tendencias de aprendizaje de otros usuarios con perfiles similares dentro de la organización o industria. Contenido Relevante y Opcional: los módulos recomendados aparecen en una sección dedicada llamada "Recomendado para ti" dentro del tablero del usuario, este contenido es totalmente opcional y permite que el empleado explore temas de su interés sin que el administrador tenga que crear, asignar o gestionar una campaña formal para ello; a través de la KnowBe4 Learner App, una aplicación nativa diseñada específicarnente para llevar la formación en ciberseguridad a los dispositivos móviles de los empleados, optimizando la accesibilidad y las tasas de finalización; mediante la funcionalidad AITP (AI-Driven Phishing) o Adaptive AI Phishing, este motor utiliza algoritmos de aprendizaje automático

para seleccionar y enviar automáticamente la plantilla de simulación más adecuada para cada individuo en lugar de enviar la misma prueba a toda la organización; permite la integración con Sistemas de Gestión de Aprendizaje (LMS) externos de dos maneras principales, asegurando que la inversión en contenido sea aprovechable en cualquier infraestructura previa. Descarga de Módulos SCORM/AICC: los clientes pueden descargar los módulos de capacitación desde el ModStore en formatos estándar de la industria (SCORM 1.2, SCORM 2004 o AICC), esto permite cargar los cursos directamente en su propio LMS (como Moodle, Blackboard, Cornerstone, etc.), sin Costos Adicionales por Integración, lo que significa que no hay un "cobro por conector" o una tarifa de licencia extra por cada vez que se sube un curso a su LMS interno, el motor de IA (AITP) actúa como un tutor personalizado que gestiona el "techo de dificultad" de cada usuario. Para usuarios de Alta Madurez: la IA selecciona plantíllas categorizadas con Nivel de Dificultad cuatro o cinco (4 o 5), que incluyen señales de phishing mucho más sutiles, remitentes altamente realistas y ganchos de ingeniería social complejos (como facturas de proveedores reales o notificaciones de TI urgentes). Para usuarios en Remediación: la IA prioriza plantillas de nivel de dificultad uno o dos (1 o 2), donde las señales de alerta (red flags) son más evidentes (errores gramaticales, remitentes extraños), asegurando que el usuario pueda aplicar lo aprendido en sus módulos de refuerzo y gane confianza antes de enfrentar retos mayores. **PHISING SIMULADO:** KnowBe cuatro (KnowBe4), ofrece un modelo que permite realizar simulaciones ilimitadas a través de múltiples vectores de ataque, no existe un costo por campaña o por correo enviado, lo que permite una experimentación constante y un entrenamiento continuo; supera ampliamente este requisito

ofreciendo la biblioteca de plantillas de phishing más extensa del mercado, diseñada para replicar amenazas reales de manera precisa; mediante su tecnología de Social Engineering Indicators (SEI), la cual transforma un error del usuario en una oportunidad de aprendizaje interactiva y visual de manera inmediata; mediante su motor de AITP (AI-Driven Phishing), esta funcionalidad utiliza algoritmos de aprendizaje automático para transformar la gestión de las simulaciones, pasando de un enfoque masivo y genérico a uno hiper-personalizado basado en el perfil de riesgo individual; ofrece un motor de telemetría avanzado que captura cada interacción del usuario con la simulación de ataque, proporcionando un desglose forense de las vulnerabilidades detectadas en tiempo real. Seguimiento de Clics y Aperturas: Registra no solo quién hizo clic en el enlace malicioso, sino también quién abrió el correo electrónico, en qué dispositivo lo hizo (móvil vs. escritorio), el navegador utilizado y la ubicación geográfica aproximada basada en la IP. Respuestas (Data Entry): Si la simulación incluye una página de destino para captura de datos (phishing de credenciales), el sistema rastrea si el usuario llegó a escribir información en los campos de texto, permitiendo identificar quiénes son propensos a entregar secretos corporativos. Ejecución de Macros y Archivos Adjuntos: La consola monitorea si el usuario descargó un archivo adjunto simulado (como un Word o Excel con macros) y, si habilitó el contenido o ejecutó el archivo, esto es crítico para medir el riesgo de ataques tipo Ransomware; permite una personalización quirúrgica de cada elemento de la simulación, lo que es fundamental para replicar ataques de Spear Phishing (ataques dirigidos) que son mucho más difíciles de detectar que los correos genéricos. Personalización de Dominios: KnowBe cuatro (KnowBe4) pone a la disposición una vasta biblioteca de

dominios que simulan servicios reales (ej. mscrosft.com, facelook.com), además, permite configurar dominios personalizados que pertenezcan a la organización (previa validación de propiedad) para simular correos que parecen venir estrictamente de fuentes internas; mediante la funcionalidad Caltback Phishing, integrada directamente en la consola de administración, este vector de ataque simula una técnica de ingeniería social híbrida muy utilizada en ataques de Ransomware modernos (como el método "BazarCall"), donde el peligro no reside en un enlace, sino en una interacción telefónica iniciada por el usuario; se desarrolla mediante configuraciones específicas de entrega y una sección colaborativa dentro de Knowbe cuatro (Knowbe4) que permite replicar amenazas del mundo real de forma inteligente. Envío Distribuido (Anti-Prairie Dog): Esta funcionalidad, denominada "Spread over" o "Send Period", permite programar que los correos de simulación se entreguen de manera aleatoria durante un período de tiempo determinado (horas, días o incluso semanas). **EVALUACIONES Y CULTURA DE SEGURIDAD**: mediante el SAPA (Security Awareness Proficiency Assessment), una herramienta de evaluación basada en principios científicos que mide el nivel real de conocimientos de los usuarios, a diferencia de un examen estándar al final de un curso, el SAPA está diseñado para establecer una línea base y medir el progreso de las competencias críticas; mediante el SCS (Security Culture Survey), una herramienta diagnóstica desarrollada con rigor académico para medir la madurez de la cultura de seguridad, a diferencia de un examen de conocimientos (que mide lo que el usuario sabe), el SCS mide lo que el usuario siente y hace habitualmente. Proporciona un ecosistema de informes avanzado que transforma los datos brutos en inteligencia accionable, permitiendo visualizar tanto el nivel de

aprendizaje (conocimiento) como la resiliencia real ante ataques (postura de seguridad). **FUNCIÓN DE SEGUNDA OPORTUNIDAD**: incluye la herramienta SecurityCoach a través de su funcionalidad de Real-Time Coaching integrada con los flujos de navegación y correo, además, para el ecosistema de Microsoft, utiliza el Phish Alert Button (PAB) y extensiones de seguridad para el navegador que actúan sobre las URLs. Alerta de "Segunda Oportunidad": Cuando un usuario hace clic en un enlace (URL) dentro de un correo electrónico en Outlook o un documento de Microsoft trescientos sesenta y cinco (365), el sistema interviene antes de que el navegador cargue el sitio final, se presenta una página de advertencia que analiza el riesgo del sitio y pregunta al usuario si está seguro de querer continuar. **REPORTE Y APIs:** se brinda mediante un motor de informes robusto y flexible que permite transformar la actividad de los usuarios en inteligencia de negocios, facilitando la comunicación tanto técnica como gerencial; mediante su motor de análisis Virtual Risk Officer, el cual centraliza múltiples flujos de datos para crear un ecosistema de informes correlacionados, en lugar de ver las métricas de forma aislada; conecta el aprendizaje teórico con la práctica real y el nivel de riesgo resultante; ofrece un robusto ecosistema de interfaces de programación de aplicaciones (APIS) que permiten la automatización y la integración de datos con otras herramientas de seguridad y gestión empresarial. **SEGURIDAD Y CONTRASEÑAS**: se proporciona mediante PasswordIQ, una herramienta especializada que monitoriza y analiza las vulnerabilidades relacionadas con las credenciales de los empleados sin comprometer la seguridad de las contraseñas reales. Detección de Contraseñas Expuestas: PasswordIQ escanea continuamente bases de datos de brechas de seguridad conocidas en la Dark Web, si las credenciales corporativas de un

empleado (correo y contraseña) aparecen en una filtración externa, el sistema genera una alerta inmediata; está diseñada para entornos empresariales de alta seguridad, integrándose de forma nativa con los estándares de identidad modernos para garantizar un acceso seguro y una administración de usuarios automatizada. **VERIFICACIÓN MENSUAL DE EXPOSICIÓN DEL CORREO ELECTRÓNICO**: se brinda mediante su herramienta especializada Email Exposure Check Pro (EEC Pro), la cual está diseñada específicamente para identificar la superficie de ataque externa de la organización a través de la exposición de correos electrónicos. Búsqueda Profunda y Rastreo: La herramienta realiza un escaneo exhaustivo en la web de superficie (Surtace Web), redes sociales profesionales y empresariales, así como en foros técnicos donde los datos de los empleados suelen estar expuestos involuntariamente. Monitoreo de Filtraciones (Data Breaches): EEC Pro rastrea cientos de bases de datos de filtraciones históricas y recientes (incluyendo la Dark Web), busca cualquier coincidencia con el dominio de correo electrónico de la organización para identificar qué direcciones ya están en manos de ciberdelincuentes. Detección de Usuarios en Riesgo: al encontrar una dirección de correo expuesta, la herramienta identifica al usuario como un "objetivo de alto riesgo", estos usuarios son más propensos a recibir ataques reales de spear phishing, ya que sus datos ya son públicos o han sido vendidos en mercados ilegales. Informes de Exposición: Genera un reporte detallado que muestra exactamente dónde se encontró la información del usuario y qué tipo de datos acompañaban al correo (contraseñas, nombres, cargos), permite al administrador tomar medidas preventivas antes de que ocurra un incidente. **REPORTE Y ANÁLISIS:** dispone de un robusto Centro de Reportes diseñado para satisfacer tanto las

necesidades de auditoría técnica como las de comunicación estratégica con la alta gerencia); mediante su motor de inteligencia de datos Virtual Risk Officer (VRO), el cual utiliza aprendizaje automático (Machine Learning) para transformar el comportamiento pasado en una puntuación de riesgo predictiva a nivel individual, de grupo y organizacional; dispone de un robusto ecosistema de interfaces de programación de aplicaciones (APIS) diseñado para la automatización, la orquestación de seguridad (SOAR) y el análisis de datos a gran escala; ofrece una capacidad de reporte granular y dinámica que permite desglosar los datos desde una visión global hasta el detalle individual, facilitando la auditoría y la toma de decisiones basada en datos. **CONTROLES Y ESTANDARES**: está diseñado bajo un marco de cumplimiento global estricto, operando con estándares internacionales de seguridad y privacidad que garantizan la protección de los datos de los usuarios y la integridad de Knowbe cuatro (Knowbe4); GDPR (General Data Protection Regulation): La solución cumple plenamente con el reglamento europeo, permite la soberanía de datos mediante centros de datos ubicados en la Unión Europea (Irlanda y Alemania) para que los datos personales nunca salgan de la jurisdicción si así se requiere, además, ofrece herramientas para el borrado de datos, anonimización de reportes y gestión de consentimiento de los usuarios. SOC2 Type dos (2): se somete anualmente a auditorías independientes de SOC2 Tipo dos (2), este informe valida que los controles de seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad de los sistemas son efectivos y se mantienen de forma consistente a lo largo del tiempo. ISO veintisiete mil uno (ISO 27001): cuenta con la certificación ISO diagonal IEC veintisiete mil uno dos puntos dos mil trece (ISO/IEC 27001:2013), el estándar de oro internacional para

la Gestión de la Seguridad de la Información (ISMS), esto certifica que aplica un enfoque sistemático para gestionar la seguridad de la información corporativa, protegiendo tanto sus activos como los datos de sus clientes. Incluye Certificaciones adicionales: Además de las solicitadas por la Institución, KnowBe cuatro (Knowbe4) cumple con FedRAMP (para agencias gubernamentales de Estados Unidos), HIPAA (privacidad de datos de salud) y es compatible con marcos de ciberseguridad como NISTy Cyber Essentials; incluye cualquier servicio de instalación y configuración para el correcto funcionamiento; con precio unitario de ciento ochenta y nueve quetzales con cincuenta centavos (Q189.50) y precio total de doscientos ochenta y cuatro mil doscientos cincuenta quetzales (Q284,250.00). La adquisición de la licencia, además de las especificaciones descritas, deben cumplir con las indicadas en la oferta de "Red Óptima" y las bases de contratación relacionadas.

TERCERA: VALOR DEL CONTRATO Y FORMA DE PAGO: El monto a que asciende la adquisición de licencia de herramienta de concientización en ciberseguridad, del presente contrato es de **DOSCIENTOS OCHENTA Y CUATRO MIL DOSCIENTOS CINCUENTA QUETZALES (Q284,250.00);** valor que incluye el Impuesto al Valor Agregado (IVA); para los efectos de pago, "Red Optima" debe presentar la factura electrónica en línea -FEL-, emitida por el proveedor a través de su agencia virtual del Portal de la Superintendencia de Administración Tributaria y copia del acta de recepción en la que conste que la licencia ha sido recibida de conformidad por el "INTECAP". Dicho pago se hará con cargo a la partida presupuestaria número dos mil veintiséis guion once millones doscientos mil treinta y cuatro guion cero cero cero guion cero cero guion once guion cero cero guion cero cero cero guion cero cero uno guion cero

cero cero guion cero ciento uno guion ciento cincuenta y ocho (2026-11200034-000-00-11-00-000-001-000-0101-158), de Administración Institucional, Informática y/o en la que en el futuro corresponda.

CUARTA: LUGAR, FORMA Y PLAZO DE ENTREGA: "Red Optima" se compromete a entregar el documento de acuerdo del licenciamiento de la herramienta, debe ser emitido por el fabricante/propietario del software o casa matriz, que descrita la relación entre el fabricante/propietario y el INTECAP, que contenga la información de la licencia de la herramienta adjudicada y debe ser entregada en Bodega General, Centro de Capacitación Guatemala uno (1), ubicado en la catorce (14) calle treinta y uno guion treinta (31-30), Colonia Ciudad de Plata II, zona siete (7) de esta ciudad, en un plazo de cinco (5) días hábiles, computados a partir del día siguiente de que el "INTECAP" le notifique por escrito, la aprobación del presente contrato.

QUINTA: SEGURO DE CAUCIÓN: a) DE CUMPLIMIENTO: "Red Optima" se obliga a prestar a favor y a entera satisfacción del "INTECAP" previa aprobación del presente contrato un seguro de caución de cumplimiento equivalente al diez por ciento (10%) del valor total del contrato, con una institución aseguradora debidamente autorizada para operar en Guatemala y de reconocida capacidad y solvencia financiera, en tanto dicho seguro no esté aceptado por el "INTECAP", éste no podrá hacerle ningún pago a "Red Optima". En caso de incumplimiento del presente contrato por parte de "Red Optima", el "INTECAP" dará audiencia por diez (10) días a la institución aseguradora, para que se manifieste al respecto, vencido el plazo si no hay oposición manifiesta de la aseguradora, sin más trámite se ordenará el requerimiento respectivo y la institución aseguradora, deberá efectuar el pago dentro del plazo de treinta (30) días contados a partir de

la fecha del requerimiento, circunstancia que se hará constar en la póliza. El seguro deberá mantenerse vigente hasta que el "INTECAP" compruebe que "Red Optima" ha cumplido con las condiciones del contrato, extendiendo la constancia respectiva para la cancelación; la fianza de Cumplimiento deberá ajustarse ante cualquier prórroga, ampliación o modificación del contrato, manteniendo las condiciones de cobertura del contrato original; y b) DE CALIDAD Y FUNCIONAMIENTO: "RED OPTIMA" como requisito previo para la recepción del licenciamiento de la herramienta, objeto del presente contrato deberá otorgar un seguro de calidad y funcionamiento por el equivalente al quince por ciento (15%) del valor total del presente contrato, con el cual garantiza la calidad de la licencia, comprometiéndose a reparar las fallas o desperfectos que le sean imputables. Este seguro es por el plazo de dieciocho (18) meses, computados a partir de la recepción de la misma.

SEXTA: GARANTÍA: "RED OPTIMA" por su parte ofrece una garantía de doce (12) meses para el licenciamiento de la herramienta adjudicada; tiempo durante el cual se compromete a reparar cualquier desperfecto, el cual se computa a partir de la recepción de la misma.

SÉPTIMA: SOPORTE TÉCNICO: "RED OPTIMA", garantiza: a) Que tiene soporte técnico directo del fabricante y que este puede prestarlo localmente de forma presencial y a distancia (chat en línea, correo electrónico y/o vía telefónica mediante número local); b) brindará acompañamiento de la solución a los inconvenientes relacionados con la oferta relacionada; y c) Que tiene la capacidad de cubrir las necesidades de mantenimiento con personal técnico calificado, en un plazo de cinco (5) días, computados a partir del momento en que se le notifique el incidente, por parte del INTECAP.

OCTAVA: INDUCCIÓN: TRANSFERENCIA DE CONOCIMIENTO: "RED OPTIMA", junto con KnowBe cuatro (Knowbe4) realizarán una transferencia de conocimiento para el personal del Departamento de Informática en: a) Uso de Knowbe4 de capacitación de ciberseguridad; b) Generación y creación de reportes básicos y avanzados; y c) Inducción sobre mejores prácticas.

NOVENA: PROHIBICIONES: "Red Optima" tiene la prohibición expresa de ceder, enajenar, traspasar o disponer de cualquier forma, total o parcialmente los derechos provenientes del presente contrato, bajo pena de nulidad de lo pactado.

DÉCIMA: DECLARACIÓN JURADA: Yo, **ESTUARDO JOAQUÍN OLIVARES RUIZ,** declaro bajo juramento que ni yo en lo personal ni mi representada nos encontramos comprendidos en las limitaciones contenidas en el Artículo ochenta (80) de la Ley de Contrataciones del Estado; así como no somos deudores morosos del Estado ni de las entidades a que se refiere el Artículo uno (1) de la referida Ley.

DÉCIMA PRIMERA: CLÁUSULA RELATIVA AL COHECHO: Yo, **ESTUARDO JOAQUÍN OLIVARES RUIZ,** manifiesto que conozco las penas relativas al delito de cohecho, así como las disposiciones contenidas en el Capítulo III del Título XIII del Decreto 17-73 del Congreso de la República de Guatemala, Código Penal. Adicionalmente, conozco las normas jurídicas que facultan a la Autoridad Superior del "INTECAP" para aplicar las sanciones administrativas que pudieren corresponderme, incluyendo la inhabilitación en el Sistema de Información de Contrataciones y Adquisiciones del Estado denominado GUATECOMPRAS.

DÉCIMA SEGUNDA: CASO FORTUITO O FUERZA MAYOR: Si surgiere un caso fortuito o de fuerza mayor que impidiera a cualquiera de las partes cumplir

con sus obligaciones contractuales, convienen en dar aviso a la otra parte por escrito dentro del plazo de cinco (5) días de ocurrido el hecho, acompañando las pruebas pertinentes para que si estuviere justificada la causa no se aplique la sanción.

DÉCIMA TERCERA: TERMINACIÓN DEL CONTRATO: El presente contrato se dará por terminado cuando ocurran cualesquiera de las circunstancias siguientes: a) Por vencimiento del plazo siempre que no se haya acordado prórroga alguna; b) Por rescisión unilateral del INTECAP, al determinarse atraso en la entrega de la licencia; con base a la fecha establecida y fijada en el presente contrato, sin perjuicio de aplicar las multas que correspondan de conformidad con los Artículos ochenta y cinco (85) y ochenta y seis (86) de la Ley de Contrataciones del Estado; c) Por rescisión acordada de mutuo acuerdo; y d) Por casos fortuitos o de fuerza mayor que hagan innecesario el contrato o que afecten su cumplimiento.

DÉCIMA CUARTA: CONTROVERSIAS: Los otorgantes convenimos expresamente en que toda controversia, diferencia o reclamación que surgiere como consecuencia del presente contrato, serán resueltas directamente con carácter conciliatorio, pero si no fuera posible llegar a un acuerdo, la cuestión o cuestiones a dilucidarse, se someterán a la jurisdicción del Tribunal de lo Contencioso-Administrativo.

DÉCIMA QUINTA: SANCIONES: a) Retraso en la entrega: El retraso de "RED OPTIMA" en la entrega de las licencias por causa imputable a él, se sancionará con el pago de una multa por cada día de atraso, del valor que represente la parte afectada, conforme al artículo ochenta y cinco (85) de la Ley de Contrataciones del Estado y los porcentajes establecidos en el Reglamento

de la Ley de Contrataciones del Estado; b) Variación en calidad o cantidad: Si, "Red Optima" contraviniendo total o parcialmente el contrato, perjudicare al "INTECAP", variando la calidad o cantidad del objeto del mismo, será sancionado con una multa del cien por ciento (100%) del valor que represente la parte afectada de la negociación, de conformidad con el artículo ochenta y seis (86) de la Ley de Contrataciones del Estado. El "INTECAP" por cualquiera de los conceptos indicados en los literales anteriores, podrá hacer la deducción correspondiente del saldo que hubiere a favor del contratista o hacer efectivo el seguro respectivo.

DÉCIMA SEXTA: RECEPCIÓN Y LIQUIDACIÓN: "RED OPTIMA" al estar preparada para la entrega del documento de la licencia de la herramienta, deberá hacerlo del conocimiento de la Gerencia del "INTECAP", por escrito, quien nombrará la comisión receptora y liquidadora que fundamentándose en el contrato, bases y oferta, verificará cantidad, calidad y demás especificaciones y recibirá el licenciamiento descrito en la cláusula segunda del presente contrato, diligencia en la cual deberá estar presente un representante de "RED OPTIMA", en caso contrario, se entenderá que acepta el contenido de las actas que se levanten, de las cuales se enviará copia certificada a donde corresponde, para los efectos que procedan; la liquidación deberá practicarse dentro de los noventa (90) días subsiguientes a la finalización del servicio.

DÉCIMA SÉPTIMA: APROBACIÓN: Para que el presente contrato surta sus efectos legales y obligue a las partes a su cumplimiento, es indispensable que sea aprobado de conformidad con la Ley.

DÉCIMA OCTAVA: ACEPTACIÓN: Los otorgantes en los términos y condiciones estipuladas aceptamos el presente contrato, el que, leído

íntegramente, por ambas partes y enterados de su contenido, validez y efectos legales, lo ratificamos, aceptamos y firmamos en doce (12) hojas de papel membretado del "INTECAP". Testado: veintiséis, 2026, omítase. Entre líneas: veinticinco, 2025, léase.

Ing. Arnaldo Ademar Alvarado Cifuentes
Sub Gerente

Sr. Estuardo Joaquín Olivares Ruiz
Administrador Único y Representante Legal

Intecap
Subgerencia

RED ÓPTIMA, S.A.