Docusign Envelope ID: 825BFC17-EAAC-4425-936B-0B0FC3302EA2

Informe de cierre del Servicio Security & Compliance para IPES.

CO-GWS-IPES-90680-Renovación Workspace 2023-Security & Compliance

Creado por: Hebert Struve
Fecha de creación: 26/08/2024

Docusign Envelope ID: 825BFC17-EAAC-4425-936B-0B0FC3302EA2

Información del Proyecto

Cliente	INSTITUTO PARA LA ECONOMÍA SOCIAL (IPES)
Oportunidad: Servicio:	-IPES-90680-Renovación Workspace 2023 -CO-GWS-IPES-90680-Renovación Workspace 2023-Security & Compliance
Fecha de inicio proyecto / servicio	23 de mayo del 2024.
Fecha de fin del proyecto / servicio	23 de agosto del 2024
Gerente de proyecto Cliente/ Subdirector de Diseño y Análisis Estratégico	William Neil Vargas Contreras wnvargasc@ipes.gov.co
Gerente de Proyecto Xertica	Hebert Struve hebert.struve@xertica.com

Objetivo del proyecto:

Ayudamos a incrementar la seguridad informática en las empresas identificando vulnerabilidades, a través de aseguramiento de Google Workspace, los protocolos de comunicación en correo y garantizando la protección en equipos Windows del usuario final, realizando una formación de cada individuo para mejorar el conocimiento y así puedan identificar los riesgos informáticos y afrontar los mismos

El alcance de esta propuesta es brindar los siguientes servicios para componentes de Datos y Analítica en Google Cloud:

1. Análisis y aseguramiento de la plataforma: Elaboración análisis de seguridad, configuración y optimización DKIM y DMARC, generación e implementación de políticas de seguridad y reglas de cumplimiento de contenido.
2. Generación de Cultura en Seguridad: Ejercicios de Phishing avanzado controlado, simulando casos reales y realizando una transferencia de conocimiento a Equipo TI y sesiones de concientización en Seguridad a usuarios finales.
3. Seguridad mejorada para puntos finales: Identificación, configuración, aplicación de Políticas y mejores prácticas.

Entregables:

Docusign Envelope ID: 825BFC17-EAAC-4425-936B-0B0FC3302EA2

Componentes	
1. Análisis de Seguridad y Aseguramiento de la Plataforma ○ Documento con revisión de todas la configuraciones de consola: ● Aplicar protección contra archivos adjuntos encriptados que provengan de remitentes que no sean de confianza ● Aplicar configuración para protegerse contra los archivos adjuntos que contengan secuencias de comandos y que provengan de remitentes que no sean de confianza ● Habilitar configuración para protegerse contra tipos de archivos adjuntos anómalos en los correos electrónicos ● Habilitar protección de los vínculos en IMAP ● Habilitar mensajes de advertencia cuando se haga clic en vínculos que dirijan a dominios que no sean de confianza ● Habilitar protección contra la falsificación de identidad de dominios basada en nombres similares ● Habilitar protección contra la falsificación de identidad que utiliza nombres de empleados ● Habilitar protección contra los correos electrónicos entrantes que falsifican la identidad de tu dominio ● Aplicar protección contra los correos electrónicos no autenticados ● Habilitar proteger tus Grupos contra los correos electrónicos entrantes que falsifican la identidad de tu dominio ● Deshabilitar Acceso POP/IMAP a los usuarios	✅
2. Configuraciones SPF, DKIM y DMARC ○ Revisión del SPF y DKIM en el DNS ○ Activación de DKIM en consola de ser necesario ○ Generar informe DMARC, Quarentena, 100% para el dominio IPES - Entregable ○ Exposición de informe ○ Informe de IPS	✅
3. Simulacro Phishing (1 envío 500 usuarios) ○ Envío de correo masivo Phishing ○ Recopilación de datos ○ Entrega de documento de simulacro - Entregable	✅

Docusign Envelope ID: 825BFC17-EAAC-4425-936B-0B0FC3302EA2

4. Dos Entrenamiento en Seguridad sobre Google Workspace Equipo TI. ○ Entrenamiento sensibilización de seguridad y recomendaciones ○ ¿Cómo implementar ciberseguridad en la organización? ○ Entregable - Video de capacitación previa ○ Mejores prácticas Seguridad Google Admin ○ Entregable - Video de capacitación previa	2
5. 01 Sensibilización en Seguridad sobre Google Workspace Usuario Final (sesión por Google Meet)	1

Supuestos y Restricciones:

- Xertica prestará el servicio de forma remota incluyendo la plataforma de comunicación y control de proyecto necesaria para la realización del servicio.
- IPES dispondrá del recurso humano para atender el proyecto en tiempo y forma; incluido un gestor del proyecto o líder técnico que sea el canal de comunicación entre la IPES y Xertica.
- IPES proveerá a Xertica de la información requerida en no más de 2 días hábiles desde la solicitud.
- IPES dispondrá de los accesos a sistemas, infraestructura u otros requeridos en el proyecto en tiempo con el fin de no retrasar las actividades.

Docusign Envelope ID: 825BFC17-EAAC-4425-936B-0B0FC3302EA2

Cronograma ejecutado:

Nombre de la tarea	Duración	Inicio	Finalizar	% Comp
Cronograma Security & Compliance 1.0 para IPES	**67d**	**23/05/24**	**23/08/24**	**100%**
Etapa 1: Seguridad Workspace	**66,5d**	**23/05/24**	**23/08/24**	**100%**
Inicio del servicio	**1d**	**23/05/24**	**23/05/24**	**100%**
Revisión de seguridad en GWS	**1d**	**29/05/24**	**29/05/24**	**100%**
Exposición de informe	**1d**	**29/05/24**	**29/05/24**	**100%**
Video de Exposición de informe	**1d**	**29/05/24**	**29/05/24**	**100%**
Verificación de 2 pasos	**2d**	**04/07/24**	**05/07/24**	**100%**
Revisar usuarios a aplicar la 2SV	**4h**	**04/07/24**	**04/07/24**	**100%**
Revisión de Políticas de 2SV	**0,5d**	**04/07/24**	**04/07/24**	**100%**
Aplicar Políticas de 2SV	**0,5d**	**05/07/24**	**05/07/24**	**100%**
Revisión de usuarios con 2SV y reporte de Activación	**0,5d**	**05/07/24**	**05/07/24**	**100%**
Ajustes de Servicios	**4d**	**08/07/24**	**11/07/24**	**100%**
Aplicar protección contra archivos adjuntos encriptados que provengan de remitentes que no sean de confianza	**1d**	**08/07/24**	**08/07/24**	**100%**
Aplicar configuración para protegerse contra los archivos adjuntos que contengan secuencias de comandos y que provengan de remitentes que no sean de confianza	**1d**	**09/07/24**	**09/07/24**	**100%**
Habilitar configuración para protegerse contra tipos de archivos adjuntos anómalos en los correos electrónicos	**1d**	**10/07/24**	**10/07/24**	**100%**
Habilitar protección de los vínculos en IMAP	**1d**	**10/07/24**	**10/07/24**	**100%**
Habilitar mensajes de advertencia cuando se haga clic en vínculos que dirijan a dominios que no sean de confianza	**1d**	**10/07/24**	**10/07/24**	**100%**
Habilitar protección contra la falsificación de identidad de dominios basada en nombres similares	**1d**	**10/07/24**	**10/07/24**	**100%**
Habilitar protección contra la falsificación de identidad que utiliza nombres de empleados	**1d**	**10/07/24**	**10/07/24**	**100%**
Habilitar protección contra los correos electrónicos entrantes que falsifican la identidad de tu dominio	**1d**	**11/07/24**	**11/07/24**	**100%**
Aplicar protección contra los correos electrónicos no autenticados	**1d**	**11/07/24**	**11/07/24**	**100%**
Habilitar proteger tus Grupos contra los correos electrónicos entrantes que falsifican la identidad de tu dominio	**1d**	**11/07/24**	**11/07/24**	**100%**
Deshabilitar Acceso POP/IMAP a los usuarios	**1d**	**11/07/24**	**11/07/24**	**100%**
Configuración DMARC al 100% - Cuarentena - dominio IPES	**9d**	**01/07/24**	**11/07/24**	**100%**
Activar DMARC en el dominio IPES estado "none", 100%	**1d**	**01/07/24**	**01/07/24**	**100%**

Docusign Envelope ID: 825BFC17-EAAC-4425-936B-0B0FC3302EA2

Semana de recepción de informes DMARC	5d	02/07/24	08/07/24	100%
Generar informe DMARC, none, 100% para el dominio - Entregable	3d	09/07/24	11/07/24	100%
Exposición de informe	1d	10/07/24	10/07/24	100%
Validación de Cambios por parte del equipo IPES	1d	11/07/24	11/07/24	100%
Informe de IPS en GWS	4d	29/07/24	01/08/24	100%
Identificar IPS en GWS	1d	29/07/24	29/07/24	100%
Generar informe de seguridad en configuración IPS - Entregable	2d	30/07/24	31/07/24	100%
Exposición de informe	1d	01/08/24	01/08/24	100%
Entrenamientos Seguridad ADMIN	1,5d	22/08/24	23/08/24	100%
¿Cómo implementar ciberseguridad en la organización?	0,5d	22/08/24	22/08/24	100%
Entregable - Video de capacitación previa	0,5d	23/08/24	23/08/24	100%
Mejores prácticas Seguridad Google Admin	0,5d	22/08/24	22/08/24	100%
Entregable - Video de capacitación previa	0,5d	23/08/24	23/08/24	100%
Etapa 2: Ejercicio de Phishing	27d	04/07/24	09/08/24	100%
Simulacro de Phishing	27d	04/07/24	09/08/24	100%
Reunión de Gestión del Cambio para tipo de correo phishing	1d	04/07/24	04/07/24	100%
Definición del correo "Tipo phishing"	1d	05/07/24	05/07/24	100%
Ajustar IPs de aplicación	1d	08/07/24	08/07/24	100%
Envío de correo de prueba	1d	11/07/24	11/07/24	100%
Envío de correo masivo Phishing	1d	22/07/24	22/07/24	100%
Recopilación de datos	5d	22/07/24	26/07/24	100%
Entrega de documento de simulacro - Entregable	1d	30/07/24	30/07/24	100%
Entrenamiento sensibilización de seguridad y recomendaciones	5d	05/08/24	09/08/24	100%
Cierre del servicio	1d	23/08/24	23/08/24	100%
Firma del acta de cierre	1d	23/08/24	23/08/24	100%

Docusign Envelope ID: 825BFC17-EAAC-4425-936B-0B0FC3302EA2

Equipo del proyecto:



Responsables:

Entregado:	Recibido:
Firmado por: HEBERT DARIO STRUVE CARDENAS 61FA29F6EE2C411... Hebert Struve Gerente de Proyecto **XERTICA**	Firmado por: 4C8F62783F55438... William Neil Vargas Contreras Gerente de Proyecto Cliente **IPES**
Fecha:	24 de agosto del 2024