ANEXO4

		SISTEMA INTEGRADO DE GESTIÓN	**Código:**	
	PROCESO	GESTION DE LA INFORMACION Y COMUNICACIONES	**Versión:**	
	FORMATO	REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	**Fecha:**	1/06/2021

REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

FECHA Y HORA REPORTE DE INCIDENTE DE SI	3/8/2021 8:00AM
LUGAR DEL INCIDENTE DE SI	GOBERNACIÓN - Tesoreria
CONSECUTIVO ASIGNADO A INCIDENTE	001

DETALLES DE PERSONA QUE REPORTA/IDENTIFICA INCIDENTE DE SI :

NOMBRE	CARGO
WILT ASBEL ONEILL CORPUS	Secretaria de ServiciosPúblicos y Medio Ambiente

DESCRIPCION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION:

¿Qué Sucedió?: El pasado 3 de agosto el funcionario WILT ASBEL ONEILL CORPUS reportó que recibió un correo donde se le pedía la transferencia de un dinero a cambio de no divulgar videos privados y se le presionaba escribiéndole desde su misma cuenta de correo para mostrar que si tenían acceso a sus cuentas.

¿Cómo Sucedió?: Correo electrónico

Por qué Sucedió?: El diagnóstico realizado arrojó que en los cambios de dominio que se hicieron en la entidad puede haber causado que este correo no fuera detectado como spam por el servidor de correo.

Consideraciones Iniciales sobre componente(s) / Activo(s) de información afectados?: Ninguno

Impactos adversos para la Entidad?:	SI	☐	NO	☑	Cual?
Se identifica Vulnerabilidad alguna?:	SI	☐	NO	☑	Cual?
Se identifica responsable del Incidente?:	SI	☐	NO	☑	Cual?

ESTADO DEL INCIDENTE Sucediendo : ☑ Sucedió : ☑ Sucede Nuevamente : ☐

DETALLE DEL INCIDENTE DE SEGURIDAD DE LA INFORMACION:

Fecha y Hora en la que sucedió el incidente?:	3/08/2021 9:42
Fecha y Hora en la que se descubrió el incidente?:	3/08/2021 9:42
Fecha y Hora en la que se reportó el incidente?:	3/08/2021 9:42

La respuesta a este incidente ya ha finalizado?: SI ☐ NO ☑

En caso afirmativo, especifique cuánto tiempo duró el incidente (Días / Horas / Minutos)?: Una hora Aprox.

CATEGORIA DEL INCIDENTE SE SEGURIDAD DE INFORMACION:

Presione Click en el recuadro que aplique de acuerdo al incidente a reportar

Incidente de Seguridad de la Información **Real**?	☑	Incidente de Seg. Información **Sospechado**?	☐

Desastre natural:

Terremoto	☐	Inundación	☐
Descarga Electromagnética	☐	Otro? Especifique_____	☐
Conflicto social:			
Disturbio	☐	Ataque Terrorista	☐
Guerra	☐	Otro? Especifique_____	☐
Daño físico:			
Incendio	☐	Agua	☐
Electrostática	☐	Ambiente Nefasto (Contaminación, polvo, corrosión	☐
Destrucción de Equipo	☐	Destrucción de Medios	☐
Robo de Equipos	☐	Pérdida de Medios	☐
Alteración de Equipo	☐	Alteración de Medios	☐
Otro? Especifique_____	☐	Otro? Especifique_____	☐
Falla en la infraestructura:			
Fallas en la Alimentación Eléctrica	☐	Falles en las Redes	☐
Fallas en el Aire Acondicionado	☐	Fallas en el suministro de Agua	☐
Otro? Especifique_____	☐	Otro? Especifique_____	☐
Perturbación por radiación:			
Radiación Electromagnética	☐	Pulsos Electromagnéticos	☐
Interferencia Electrónica	☐	Fluctuación de Tensión	☐
Radicación Térmica	☐	Otro? Especifique_____	☐
Falla técnica:			
Falla en el Hardware	☐	Mal Funcionamiento del Software	☐
Sobrecarga (saturación de capacidad de los sistemas)	☐	Violación de Mantenibilidad	☐
Otro? Especifique_____	☐	Otro? Especifique_____	☐
Malware:			
Gusano de Red	☐	Troyano	☐
Botnet	☑	Ataques combinados	☐
Página WEB con código malicioso incrustado	☐	Sitio de alojamiento con código malicioso	☐
Otro? Especifique_____	☐	Otro? Especifique___spoofing_____	☑
Ataque técnico:			
Escaneo de Redes	☐	Aprovechamiento de Vulnerabilidades	☐
Aprovechamiento de Puertas traseras	☐	Intentos de acceso	☐
Interferencia	☐	Denegación de Servicio	☐
Otro? Especifique_____spoofing_____	☐	Otro? Especifique_____	☐
Violación de reglas:			
Uso no autorizado de recursos	☐	Violación a los Derechos de Autor	☐
Otro? Especifique_____	☐	Otro? Especifique_____	☐
Puesta en peligro de las funciones:			
Abuso de Derechos	☐	Falsificación de Derechos, denegación de acciones	☐
Operaciones Incorrectas	☐	Violación de la Disponibilidad del Personal	☐

Otro? Especifique_____	☐	Otro? Especifique_____	☐
Puesta en peligro de la información:			
Interceptación	☐	Espionaje	☐
Chuzada de Teléfonos	☐	Divulgación	☐
Enmascaramiento	☐	Ingeniería Social	☐
Phishing de Redes	☐	Robo de Datos	☐
Pérdida de Datos	☐	Alteración de Datos	☐
Error de Datos	☐	Análisis de Flujo de Datos	☐
Detección de posición	☐	Otro? Especifique_____	☐
Contenidos peligrosos:			
Contenido Ilegal	☐	Contenido que provoca pánico	☐
Contenido Malicioso	☐	Contenido Abusivo	☑
Otro? Especifique_____	☐	Otro? Especifique_____	☐

DETALLE DE LA SOLUCION DEL INCIDENTE DE SEGURIDAD DE LA INFORMACION:	
Fecha y Hora de la investigación del incidente?:	4/08/2021 8:00
Nombre(s) del(los) investigador(es) del incidente?:	Shary Llanos
Fecha y Hora de la Finalización del incidente?	05/08/2021 06:00pm
Fecha y Hora de la Finalización del impacto?	05/08/2021 06:00pm

Descripción de las acciones tomadas para resolver el incidente de SI:

1. Validación de los encabezados del correo para identificar de donde proviene el correo y posibles causas por las cuales no fue filtrado como spam.
2. Verificación de la configuración dkim dmarc y spf.

Descripción de las acciones planeadas para resolver el incidente de SI:

1. Realizar validaciones de configuración dkim, demarc y spf.
2. Sensibilizar a los funcionarios sobre ese tipo incidentes.

Acciones pendientes para resolver el incidente de SI:

1. Actualizacion de la configuración de firmas digitales

Conclusiones:

Se describe claramente que técnica fue utilizada para el ataque y se identifica la importancia de realizar validaciones a la configuración de las firmas digitales de los correos electrónicos.

Lecciones aprendidas del incidente de SI:

1. Investigar problemas de correo con la herramienta de Google Messageheader.
2. Lo importante de hacer campañas de formación para los funcionarios y contratistas para que identifiquen las amenazas de seguridad de la información.

DETALLES DE PERSONA DEL ISIRT (Equipo de Respuesta a Incidentes de SI)**:**	
Nombre :	**Sede :**
Área :	**Dirección :**
Teléfono de Contacto :	**Correo Electrónico :**

FIRMAS	
Originador (Nombre y apellido):	**Revisor (Nombre y Apellido)**

Firma Digital	**Firma Digital:**
Rol:	**Rol:**
Fecha:	**Fecha:**