

 INFOTEP San Andrés y Providencia		SISTEMA INTEGRADO DE GESTIÓN	Código:		
	PROCESO	GESTION DE LA INFORMACION Y COMUNICACIONES		Versión:	
	FORMATO	REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACION		Fecha:	19/03/2021

REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

FECHA Y HORA REPORTE DE INCIDENTE DE SI	1/4/2019 8:00AM
---	-----------------

LUGAR DEL INCIDENTE DE SI	INFOTEP
---------------------------	---------

CONSECUTIVO ASIGNADO A INCIDENTE	001
----------------------------------	-----

DETALLES DE PERSONA QUE REPORTA/IDENTIFICA INCIDENTE DE SI :

--	--

DESCRIPCION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION:

Qué Sucedió?:

Cómo Sucedió?:

Porqué Sucedió?:

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?:	
---	--

Fecha y Hora en la que se descubrió el incidente?:	
--	--

Fecha y Hora en la que se reportó el incidente?:	
--	--

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 ? <input type="checkbox"/>	Incidente de Seg. Información Sospechado ? <input type="checkbox"/>
---	--

Desastre natural:

Terremoto <input type="checkbox"/>	Inundación <input type="checkbox"/>
------------------------------------	-------------------------------------

Descarga Electromagnética	<input type="checkbox"/>	Otro? Especifique _____	<input type="checkbox"/>
Conflicto social:			
Disturbio	<input type="checkbox"/>	Ataque Terrorista	<input type="checkbox"/>

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

Otro? Especifico_____

Otro? Especifico_____

Puesta en peligro de la información:			
Interceptación	<input type="checkbox"/>	Espionaje	<input type="checkbox"/>
Chuzada de Teléfonos	<input type="checkbox"/>	Divulgación	<input type="checkbox"/>
Enmascaramiento	<input type="checkbox"/>	Ingeniería Social	<input type="checkbox"/>
Phishing de Redes	<input type="checkbox"/>	Robo de Datos	<input type="checkbox"/>
Pérdida de Datos	<input type="checkbox"/>	Alteración de Datos	<input type="checkbox"/>
Error de Datos	<input type="checkbox"/>	Análisis de Flujo de Datos	<input type="checkbox"/>
Detección de posición	<input type="checkbox"/>	Otro? Especifique_____	<input type="checkbox"/>

Contenidos peligrosos:			
Contenido Ilegal	<input type="checkbox"/>	Contenido que provoca pánico	<input type="checkbox"/>
Contenido Malicioso	<input type="checkbox"/>	Contenido Abusivo	<input type="checkbox"/>
Otro? Especifique_____	<input type="checkbox"/>	Otro? Especifique_____	<input type="checkbox"/>

DETALLE DE LA SOLUCION DEL INCIDENTE DE SEGURIDAD DE LA INFORMACION:	
Fecha y Hora de la investigación del incidente?:	
Nombre(s) del(los) investigador(es) del incidente?:	
Fecha y Hora de la Finalización del incidente?	
Fecha y Hora de la Finalización del impacto?	
Descripción de las acciones tomadas para resolver el incidente de SI:	
Descripción de las acciones planeadas para resolver el incidente de SI:	
Acciones pendientes para resolver el incidente de SI:	
Conclusiones:	
Lecciones aprendidas del incidente de SI:	

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:

