

Proceso/área/Recinto: Sistema de Seguridad de la Información – Ciberseguridad

Fecha: 14-07-2020

Objetivo de la reunión
Reunión de planificación actividades monitoreo 24x7 Ciberseguridad 2020

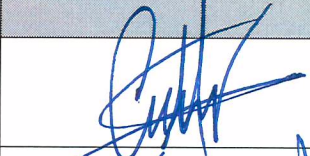
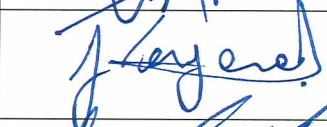
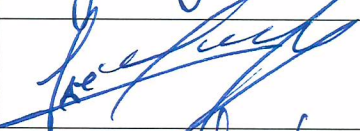
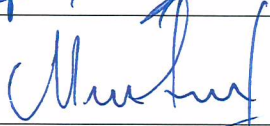
Temas Tratados
<div>1. Se informa que el servicio de monitoreo de Ciberseguridad 24x7 se encuentra activo y en marcha blanca para ajustes de parámetros y procedimientos hasta fines de Julio. El 01 de Agosto se entrará en producción con el servicio y se notificará esta actividad al CSIRT de Gobierno</div> <div>2. Se debe crear una lista de distribución que involucre a los responsables necesarios en la administración de la plataforma tecnológica del IND.</div> <div>3. Se debe definir un contacto telefónico 24x7 en el IND ante incidentes de carácter mayor que requieran su resolución de manera rápida.</div> <div>4. Los incidentes quedarán reflejados en la plataforma MANTIS del IND para históricos. De esta plataforma se seleccionarán aquellos que se informarán al CSIRT de Gobierno.</div> <div>5. Se requiere visibilidad del servidor “Sophos-Central” para gestión de incidentes del tipo “día 0”.</div> <div>6. Se deja constancia que el SIEM tiene la facultad de verificar cuando los respaldos son exitosos, por consiguiente se solicitará la instalación del agente en el servidor de respaldos.</div> <div>7. Se debe generar un vínculo entre 8 Layer y Redinfo de manera de poder generar visibilidad de todos los incidentes o intentos de ataques a las plataformas externas del IND.</div>

Compromisos*		
Detalle del Compromiso	Responsable	Plazo
Crear lista de distribución con integrantes de informática del IND para recepción de incidentes gatillados desde la plataforma MANTIS y recibir comunicados desde 8 Layer. Incluir la casilla mss@measuredsecurity.cl la que da visibilidad al SOC 24x7	IND	22/07/2020
Solicitar a 8 Layer que cada vez que se detecte un incidente, se reporte a la casilla de distribución creada.	IND	22/07/2020
Verificar con 8 Layer la posibilidad de habilitar el protocolo “Netflow” desde el Firewall perimetral Sophos hacia la consola SIEM IND.	IND / REDINFO	31/07/2020
Se deberá instalar agente en servidor Sophos – Central para la visibilidad de posibles ataques de día 0, para esto se generará un agente especial que IND deberá instalar en el servidor.	IND / REDINFO	31/07/2020
Se deberá entregar el nombre y la IP del servidor de respaldos para incorporar el agente directamente desde el SIEM IND	IND	26/08/2020

*En caso de no existir compromisos, ni seguimiento de compromisos, estos campos se deben dejar en blanco

Se debe verificar la posibilidad de aumentar de 2 a 4 cores de CPU a la máquina virtual del SIEM IND de manera de aumentar su nivel de procesamiento.	IND	21/07/2020
---	-----	------------

Seguimiento* de compromisos fijados en reunión anterior		
Detalle del Compromiso	Responsable	Estado (implementado, en desarrollo, pendiente)
Enviar informe ejecutivo del análisis de vulnerabilidades	Redinfo	Implementado
Redactar preguntas para la encuesta a los funcionarios	IND-Redinfo	Implementado
Determinar quiénes y cómo recopilarán los registros de operación	IND	Implementado
Realizar listado de todos los sitios expuestos del IND	IND-Redinfo	Implementado
Crear lista de distribución de correo para la comunicación y coordinación entre IND y Redinfo.	Redinfo	Implementado

N°	Nombre del Participante	Cargo	Firma
1	Cristian Villalobos	Representante Depto. de Informática	
2	Jorge Vergara	Jefe Unidad de Planificación y Control de Gestión	
3	Jaime Bustos	Encargado de Ciberseguridad	
4	Manuel Salas	Jefe Depto. Informática	
5			