Gobierno de Chile

Informe Mensual de Desempeño de Honorarios a Suma Alzada

Mes	Septiembre		
Año:	2024		
Datos Personales			
Nombre y Apellidos	Erik Rodrigo Atenas Chamblás		
Monto Honorario Bruto Mensual	2.607.500.-	Monto Honorario Líquido Mensual	$2.248.969.-
Fecha Inicio Asesoría	01-01-2024	Fecha Termino Asesoría	31-12-2024
N° Decreto (Ex.) y/o Resolución (Ex.)	410	Fecha Decreto (Ex.) y/o Resolución (Ex.)	31/01/2024
Agente Público			

Asesoría o Trabajo Encomendado, Descripción

a) Definir los estándares básicos para la plataforma de servidores, en lo que respecta a software y hardware para cumplir con los estándares de ciberseguridad
b) Proponer la adquisición de hardware y software para la plataforma tecnológica destinada a dar seguridad de infraestructura.
c) Asesorar y mantener coordinadores informáticos regionales en materia de ciberseguridad.
d) Participar como miembro activo en el Comité de Seguridad de la División de Informática.
e) Relacionarse con empresas externas y controlar que se cumplan las planificaciones establecidas en cada proyecto de ciberseguridad.
f) Asistir a las jefaturas de División y unidades ministeriales en la evaluación de seguridad informática.
g) Reportar los incidentes de ciberseguridad al Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior y Seguridad Pública, de acuerdo a lo establecido en el Procedimiento de Gestión de Incidentes Institucional y el Decreto 273/2022, del Ministerio del Interior.
h) Implementar procesos de administración de la seguridad y comprobar que todas las solicitudes de soporte sean tratadas conforme a procedimientos acordados
i) Implementar políticas, procedimientos, guías, protocolos, estándares, procesos y directrices en el ámbito informático.
j) Resguardar la integridad, disponibilidad y confidencialidad de los activos de información de los procesos a su cargo, de acuerdo con lo establecido en la Política General de Seguridad de la Información, políticas específicas, procedimientos y otros documentos de este Sistema, como, asimismo, según las competencias asociadas al cargo participar en la implementación y mejora del sistema. k) Fomentar el trabajo en equipo a su cargo y la comunicación de los lineamientos definidos con las jefaturas de la División de Informática.

Actividades Realizadas

22/08/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Elaboración de procedimiento para bloqueo inmediato de cuenta de usuario y dispositivos utilizados para conexión a servicios On Premises y Azure.

- Asignación de roles adecuados para cuenta ADConnec que permite la conexión entre AD On Premises y Azure Entra ID. Se remueve rol de Global Administrator. Se verifica correcto funcionamiento. Se da por cerrado el caso.
- Preparación de procedimientos asociados a TI para formalización de operaciones. Clusterización de alcance.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.

23/08/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Adecuación de perfil de cargo y requerimientos a solicitar para cubrir el cargo de Administrador/Operador TI (especialización plataforma Exchange On premises y en la nube) ID 117909.
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender: https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files
- Revisión y catalogación de procedimientos. Catalogación por alcance. Separación de procedimientos de acuerdo al objetivo. Se busca reducir el número de procedimientos existentes y generar nuevos procedimientos por alcance.

26/08/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para el usuario Ivan Carmona Vidal, a partir del 25/08/2024 se hacen inicio de sesión desde Hong Kong y el mismo día desde Dinamarca, como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.

- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Reunión DINFO. Revisión estado de avance - Plataforma Exchange On premises - estrategia de parchado y otros. Puntos tratados:
    - Respaldo SQL: Se disponibiliza descarga y se instala en la medida que sea menos impactante. Se definiría día de la semana en la cual se realizará esta tarea. La instalación se deberá realizar a la semana siguiente de liberado el parche MS y no deberá pasar de una semana en su aplicación para todos los servidores SQL. Se seguirán las pruebas para determinar la mejor forma de hacerlo (BEA)
    - Plan de actualización Exchange: Para el parchado de esta semana se aplicará en forma manual @Carlos Valdés España definirá día de la semana vigente y el horario en que se aplicará. OK
    - Se define que la instalación de los parches MS deben comenzar una semana después de que son liberados por Microsoft y no debería pasar de una semana para su instalación en todos los servidores.
    - @Carlos Valdés España generar manual paso-a-paso para aplicar en la actualización de los servidores Exchange On premises. Documento será publicado en OneNote.
    - @Waldo Gonzalez Armani analizará la factibilidad de configurar una tarea en SCCM que permita automatizar el proceso de parchado de los servidores Exchange On Premises.
    - @Daniel Varela González retomará caso con Microsoft para revisar el proceso de descarga de casillas de correo desde Exchange Online a servidores Exchange On Premises en Liray, se establece plazo de 2 semanas para retomar el caso.

27/08/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de boletín de seguridad emitido por el CSIRT de Gobierno N°268 – del 17/08/2024 al 23/08/2024. Recopilación de información, envío de correo solicitando bloqueos a nivel de IP y ULR en firewall corporativo para sitios identificados como fraudulentos, phishing y malware.
- En base al reporte generado por CSIRT N°268 (17/08/2024 al 23/08/2024) se incluyen el bloqueo EndPoint de Defender los siguientes Hash SHA256:

  Nombre asociado: TGR - Suplantación con malware - CSIRT - 26082024
  1e74435045984691a9d8bce58101b8e3509c1031142b8aedd8f81d1c67eedbd2 --> DevolucionImpuestopiendenteTGR_b1Gz5R2UBS.cmd
  28225c5622637cdaed8342e14560e8de7b53dd6ba145d973643fc4b5bdd67b75 --> - dc626f8f3b32c1e751d02c3e881bdfdc701a8db9dcb11a424b68f69fd7c4ce5c --> DevolucionImpuestopiendenteTGR_16081.zip

- Defender EndPoint:
  https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files

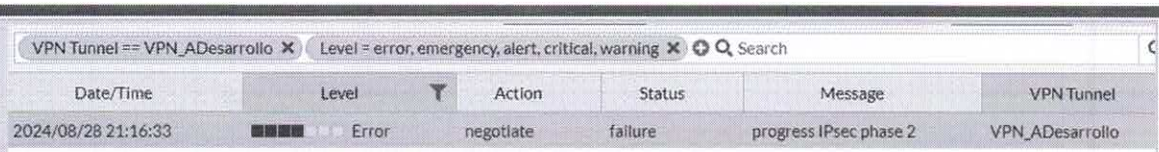
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para el usuario Matías Carvacho Pérez, el día 26/08/2024, viaje imposible, se hacen inicio de sesión desde Oslo (Noruega) y el mismo día desde Boydton (USA), como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de documento "Solicitud de información AP001T0005540" desde la perspectiva de la seguridad, se tachan nombres de servidores, tablas y accesos en las querys entregadas, Se elimina columna en el Anexo en dónde se explica el requerimiento original más el resultado de la ejecución realizada.

28/08/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Reunión Minvu: Herramienta eaFlow - levantamiento arquitectura empresarial. Presentación de la herramienta, alcances, integraciones, pilares de control y otros. Se realizará una nueva reunión para entrar en detalle.
- Reunión Minvu – Microsoft. Configuración de Azure Firewall. Se despliega firewall en tenant. Se genera IP pública para navegación en internet. Próxima reunión para definir rutas, reglas, subredes y table routes. Falta configurar, para lograr que el tráfico pase por el Firewall, tiene que haber conectividad entre las VNETs spoke y la VNET Hub, por medio de un peering.

29/08/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas en la VPN VPN_Aprod_QA. Para la VPN VPN_ADesarrollo se detectó el siguiente error: A las 21:16:33 del 28/08/2024 se registró un error de negociación, el cual fue recuperado.



-
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Reunión Minvu – Microsoft. Continuación configuración Azure Firewall. Se revisan: peering, firewall policy (network rule), route tables (creación de ruta para route table), otros puntos. Se realizó PoC con equipo VM ExpressRoute haciéndolo navegar a internet a través del firewall, resultados exitosos. Hay que hacer la configuración para el resto de los servicios (API) que necesitan salir a navegar hacia internet.
-

30/08/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para los usuarios Yordanka Barrios González y Danitza Roa Santos, el usuario Yordanka Barrios González registra viaje imposible el día 30/08/2024 entre Santiago y USA (Virginia); el usuario Danitza Roa Santos registra viaje a Brasil dentro de los márgenes razonables, como medida preventiva, para el primer caso, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender: https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files.

02/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para el usuario Alvaro Rios Karl, se registran viajes imposibles los días 30/08/2024 y 01/09/2024 entre Santiago, Finlandia (Tuusula), Alemania (Frankfurt y Berlín)

y Marruecos (Rabat); como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de boletín de seguridad emitido por el CSIRT de Gobierno N°269 – del 24/08/2024 al 30/08/2024. Recopilación de información, envío de correo solicitando bloqueos a nivel de IP y ULR en firewall corporativo para sitios identificados como fraudulentos, phishing y malware.

03/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Reunión Minvu. Revisión estado de avance - Plataforma Exchange On premises - estrategia de parchado y otros. Revisión de puntos, estado de avance, próximas metas.
- Reunión Minvu. Estrategia Assessment de Redes. Estado avance. Definiciones tomadas. Siguientes pasos a seguir.
- Configuración para integración Aranda con servidor de correo Exchange 2016 on premises. Integración mediante protocolo IMAP y/o POP3, se detectan problemas de autenticación, no hay disponibilidad de estos protocolos para cuenta de Aranda. Se detectan problemas de permiso para el envío de correo desde esta cuenta. En proceso de revisión.

04/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para el usuario Mario Marcelo Mendez Henríquez, se registran viajes imposibles los días 30/08/2024 y 04/09/2024 entre Santiago, USA, Colombia, Japón, Canada y otros países; como medida preventiva, se bloquea la cuenta y se solicita el cambio de contraseña en forma forzada. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.

- Elaboración de Tips de Ciberseguridad para el periodo septiembre – octubre. Se envían tips para ser difundidos hasta el día 02/10/2024.
- Elaboración de diagrama para integración Azure Firewall, identificación de componentes, integración, identificadores y otros. Lo anterior para hacer pruebas de acceso a internet para plataforma alojada en el tenant de Azure.
- Revisión procedimiento "Acceso a las redes y a los servicios de red".

05/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender: https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para los usuarios Karen Alaluf Skorka, Patricio Sepulveda Turra, Maritza González Fredes, Nerina Paz López, Hermes Montecinos Cuadros, Cristhian González Bazaes, Claudio Díaz Martínez, Adolfo Balboa Monroy, y Eric Pérez Gutiérrez. Se registran viajes imposibles los días 04/09/2024 y 05/09/2024 entre Santiago y otros países; como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Reunión Minvu – Infocorp. Reunión de presentación de la empresa y servicios que presta.
- Reunión Minvu. Tema: consultas Contraloría. Consensuar respuestas a consultas formuladas por la CGR respecto a temas asociados a la seguridad de la información.

06/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas
- Revisión configuración Azure Firewall. Colección de reglas. Definición de reglas.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.

2

- Revisión de usuarios en riesgo – Identity Protection (Entra ID). No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Reunión Minvu – Microsoft. Caso Azure Firewall. Se revisa configuración y problemas detectados (POD no accesibles cuando se incluía el segmento en la tabla de ruteo). Se revisa flujo y probables bloqueos a nivel de firewall. Como prueba se habilita regla any-to-any para verificar si el tráfico no es bloqueado por otro control. Finalmente se descubre que al crear la tabla de ruteo en el "Destination IP Addresses/CIDR ranges" se ingresó erróneamente la máscara aplicada a la IP gresada (Se cambió 10.201.8.242/32 por 10.201.8.0/24) para incluir toda la clase C asociada a la plataforma AKS.
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender: https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files

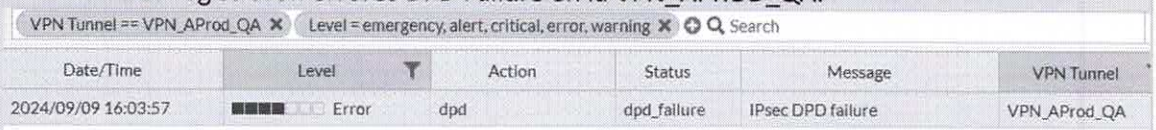
09/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para el usuario Oscar Palacios Soto, se podría presentar viaje imposible entre Chile y Colombia entre los 06 y 07 de septiembre; se está a la espera de comportamiento del usuario en el curso del día para confirmar o descartar.
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender: https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files
- Revisión de boletín de seguridad emitido por el CSIRT de Gobierno N°270 – del 31/08/2024 al 06/09/2024. Recopilación de información, envío de correo solicitando bloqueos a nivel de IP y ULR en firewall corporativo para sitios identificados como fraudulentos, phishing y malware.

10/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.

- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas en la VPN VPN_ADesarrollo. Para la VPN VPN_Aprod_QA se detectaron los siguientes errores:
- A las 16:03 se registraron errores DPD Failure en la VPN_APROD_QA.



-
- La causa se encontraría en internet, en algún punto entre ambos extremos, y no estaría causada por algún problema de comunicación de alguno de los extremos.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se confirma que el comportamiento anómalo detectado el 09/09/2024, en el inicio de sesión para el usuario Oscar Palacios Soto es un falso positivo. No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error).
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender: https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files
- En base al reporte generado por CSIRT N°270 (31/08/2024 al 06/09/2024) se incluyen el bloqueo EndPoint de Defender los siguientes Hash SHA256:

Nombre asociado: Poder Judicial - Suplantación con Malware - CSIRT - CMV24-00484
28225c5622637cdaed8342e14560e8de7b53dd6ba145d973643fc4b5bdd67b75 <-- -
2fcf28af66178424b8b556846eb62f69e46231510bd7d43cb658743171cf03a1 <--
IntimacionPoderJudicial1080706696_48180.zip
da844d08ed86a9531f96645f945cfca5ee24208d52b48874646d2e0a2a175599 <--
IntimacionPoderJudicial1080706696_YODy4Kfc.cmd

Nombre asociado: ALFA TEaM Shell - Comunicado - CSIRT
48a8dfd52e13e4fc8da37b5e682cc32ce2fafb015d4c08c61461fc1c28374f70 <-- db.php
5c2d714f1db9e17c7e3bd8e627115835ec06e4fff1b9e7598d4a02b5d1d7c7f8 <-- alfa-shell-v4.1-tesla-decoded.php
6a4fa6ed62102d67ebb08f7ad73b4c5f31d3e5de59c260d99c11bb606fca3dec <-- lock360.php
9937aec82fd2dd2a2615b6fabce0e3b3664f03dd8b9abd0a2486c509e2a77922 <-- edit.php
ac894fd8fbb673e2b67cd3f2ea3580099152f50e81ac7cda1df3024618e71110 <-- about.php
af02d0590043160393f739598156a0e078563882bb78ea132d92b83db7963863 <-- index.php
b11463f641626666f5659d4bf1f99d5de2889fbea79c879c4105e23d52d723ee <-- up_sc.php
b827cdd9d417abaf9050bc1377aa67127a12f0128f59391714239668c03a011d <-- alfav4.1-tesla.php
d3a5466d936e6fc742f965ae2c76d0d73faca7a9e17321718367afc0b5ac5df5 <-- up.php
e7806d6ee26a8252478bee22a8a39f2f0754f31a993882c55c848e7b4e8de5f9 <-- wp-signin.php
f1c7e62eafe8416501162aed8faf8bc2ee0a3420565fe7396ff78419e52aa18a <-- parbada.php

- Defender EndPoint:
https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files

11/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.

- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para el usuario Gonzalo Gálvez Bobadilla, se registran viajes imposibles el día 10/09/2024 entre Santiago y Valdivia; como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Reunión Minvu – Noventiq. Telefonía IP bajo MS Teams. Ofrecimiento para hacer un análisis de la situación actual en materia telefónica y la migración a Teams. Se informa que por el momento no se tiene la disponibilidad para hacer el estudio.
- Revisión de probables cuentas contaminadas por ransomware asociado a la empres IDOM. Situación informada por CSIRT.
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender: https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files
- Salida anticipada a las 16:00 horas.

12/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas en la VPN VPN_AProd_QA. Para la VPN VPN_ADesarrollo se detectaron los siguientes errores: A las 03:51:03 y 03:53:51 del 12/09/2024 se registraron errores de negociación, los cuales fueron recuperados con una nueva negociación.

Date/Time	Level	Action	Status	Message	VPN Tunnel
2024/09/12 03:53:51	Error	negotiate	failure	progress IPsec phase 2	VPN_ADesarrollo
2024/09/12 03:51:03	Error	negotiate	failure	progress IPsec phase 2	VPN_ADesarrollo

- Revisión de antecedentes de postulantes al cargo de Ejecutivo Técnico para la DINFO (Área Continuidad y Servicios TI).
- Chequeo de vulnerabilidades para la aplicación https://proveedorestecnicos.minvu.gob.cl, para la cual CSIRT informó filtración de información (cuentas de usuario y contraseñas) en la Deep Web. Se analiza información disponible y se aplican las siguientes medidas mitigatorias: 1. Se ha identificado la aplicación y la base de datos que pudiera estar comprometida. 2. Se ha forzado

un cambio de contraseñas explícito para las cuentas informadas. 3. Se ha realizado un análisis de vulnerabilidad de la aplicación informada. 4. Con el resultado del análisis de vulnerabilidad realizado se aplicarán remediaciones en la medida que sea factible aplicarlas.

13/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión de eventos generados por Microsoft 365 Defender. Incidentes y Alertas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). No se detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de informes de vulnerabilidad y recomendaciones OWASP para sitio https://proveedorestecnicos.minvu.gob.cl/inicio-de-sesion/. Se genera correo con las recomendaciones a aplicar para resolver las vulnerabilidades detectadas. Se queda a la espera de comentarios por parte del área de aplicaciones.
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender: https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files

16/09/2024:

- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado por el CSIRT.
- Revisión del estado de la VPN VPN_AProd_QA y VPN_ADesarrollo, chequeo de errores de conexión y/o negociación en la VPN Site-2-Site Minvu-Azure. No se detectan errores en las últimas 24 horas.
- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Se detecta comportamiento anómalo de inicio de sesión para los usuarios Pedro Fernandez Weigert y Eduardo Muñoz Briones. Para el usuario Eduardo Muñoz Briones se detecta viaje imposible entre Santiago y Ámsterdam (Países Bajos) el día 13/09/2024. Para el usuario Pedro Fernandez Weigert se registran viajes imposibles el día 13/09/2024 entre Santiago y Asburn (USA). Como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión de incidentes generados en LUMU (PoC finalizada, funcionamiento en modo Free), manualmente se cierran casos que tienen menos de 8 contactos, se cierran casos de endpoints bloqueados, acá se incorporan los IoC en Defender:

https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files

17/09/2024: Medio día administrativo.
18/09/2024: Feriado.
19/09/2024: Feriado.
20/09/2024: Feriado.

Observaciones

Persona que visa el correcto desempeño de la Asesoría prestada

Nombre	Leonardo Cavieres Córdova
Cargo	Jefe de Continuidad y Servicios TI - División de Informática

MINISTERIO DE VIVIENDA Y URBANISMO
CONTINUIDAD Y SERVICIOS TI

Firma **Firma Honorario**

Lugar	Santiago	Fecha	23/09/2024