Gobierno de Chile

Informe Mensual de Desempeño de Honorarios a Suma Alzada

Mes	Agosto		
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

22/07/2024:

- 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). Usuario Jair Pereira Abrigo presenta un estado en riesgo de inicio de sesión, el usuario presenta un viaje sospechoso el 20/07/2024 entre Chile y USA, se fuerza el cambio de contraseña en el próximo inicio de sesión. 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 escenarios para resolver problema con red MPLS a nivel nacional.
- Revisión de boletín de seguridad emitido por el CSIRT de Gobierno N°262 – del 06/07/2024 al 12/07/2024. 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°262 (06 al 12/07/2024) se incluyen el bloqueo EndPoint de Defender los siguientes Hash SHA256:

Nombre asociado: SII CMV24-00476 - Suplantación con Malware - CSIRT
36a9e7f1c95b82ffb99743e0c5c4ce95d83c9a430aac59f84ef3cbfab6145068 -> b.txt
5d5100480985f7cb1f2bf0ad8d104325a75d511b8af6c8e87e6081e6f43194e6 -> MSIB8A5.tmp
7e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910a -> ssleay32.dll
8cea66c4bd7b03666a88e80791edb015df847381702a356eae0c2f8b6dd08e71 -> MSIACAA.tmp
ca763693cc25d316f14a9ebad80ebf00590329550c45adb7e5205486533c2504e -> MSIAC0B.tmp
d2ea96db9ddfa369200ebb5fd30c6b884acabdc39de8704a1ec934488cd86a09 -> SiiFacturaMayonopagada.msi
d2ea96db9ddfa369200ebb5fd30c6b884acabdc39de8704a1ec934488cd86a09 -> SiiFacturaMayonopagada.zip
e28e34fbdaff077669586dcdb4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7 -> libeay32.dll

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

23/07/2024:

- 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). Usuario Celinda Castro Cardenas presenta un estado en riesgo de inicio de sesión, el usuario presenta un viaje imposible el 23/07/2024 entre Chile y Brasil, se fuerza el cambio de contraseña en el próximo inicio de sesión. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Comunicado a todos los funcionarios para que no conecten equipos de comunicaciones no autorizados a la red institucional.
- 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 – Cunix. Revisión publicación DSpace. Documentos faltantes, mal nombrados y definición de cuenta de acceso para SMTP Gateway de O365 (smtp.office365.com), cuenta generada por Daniel Varela, UserDocMail (AD).

24/07/2024:

- 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.

25/07/2024:

- 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. Se detectan errores de negociación en la fase 2 para la VPN_AProd_QA entre las 9:18 y las 10:16. Para la VPN_ADesarrollo no se detectaron problemas.
- Comunicado a los Coordinares Informáticos en regiones para explicar lo sucedido en el incidente del viernes 19 y lunes 22 de julio (corte de servicios por bloqueo de puertas a nivel de protocolo Spanning Tree en switch de Claro y de Entel), pasos a seguir e implementar para minimizar una nueva ocurrencia. Se citará a todos los coordinadores para sesión Teams para analizar las causas y los pasos a seguir.
- Reunión Minvu – Microsoft. Problema DNS. El problema esta fuera de la infraestructura interna. Los logs reflejan los problemas de resolución DNS a servidores externos. Internamente funciona sin problemas. Los registros DNS cacheados indican que el servicio en internet no está disponible.

26/07/2024:

- 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, solo las detectadas el día anterior que fueron explicadas por Novared (habilitación de un nuevo segmento en la VPN).
- Reunión interna. Presentación de la arquitectura Exchange 2016 On Premises al equipo de administración de plataforma. Objetivo: Definir una estrategia de parchado para los servidores Windows involucrados. Se toman acuerdos y se cita a reunión el próximo viernes para revisar avances.

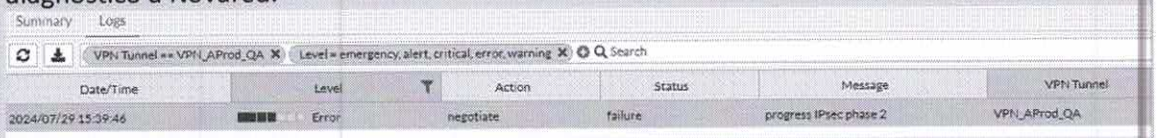
29/07/2024:

- 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). 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. Parchado Servidores estado actual, pasos a seguir.
- 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

30/07/2024:

- 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 y propuesta de nueva versión para formulario de Postulación al Teletrabajo. Se agregan escenarios disponibles para acceder a VPN
- 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 propuesta Procedimiento para la Gestión de Incidentes V7.

- Se detectan problemas con la VPN VPN_AProd_QA. Error de negociación en la fase 2. Se solicita diagnóstico a Novared.



-
- Para la VPN_ADesarrollo, no se detectan errores en las últimas 24 horas.
- Reunión Minvu – 8Layer/PRTG. Ronda de consultas por dudas con respecto al alcance de los sensores que se pueden aplicar, licenciamiento necesario, forma de configurar PRTG (Cluster por ejemplo).
- 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.

31/072024:

- 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). 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. Presentación de los códigos y valores del nuevo contrato de licenciamiento y soporte para los próximos años.
- Verificación de acceso a WS de Transbank para aplicación de pago en Minvu. Sin conexión, solo se habilita para IP puntual, pero no para otros servicios, aun en investigación, se hacen consultas a Novared.

01/08/2024:

- 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.
- Preparación de PPT por incidente asociado a falla de comunicaciones los días 19 y 22 de junio, SpanningTree y Red MPLS. Para ser presentada en la reunión de coordinadores informáticos del miércoles 07/08/2024.

- Revisión de usuarios en riesgo – Identity Protection (Entra ID). Usuario Giselle Andrea Pasten Magna presenta un estado en riesgo de inicio de sesión el 31/07/2024, NO se visualiza viaje imposible, se detecta inicio de sesión desde Miami, Florida, USA, como medida preventiva se fuerza el cambio de contraseña en el próximo inicio de sesión. 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.
- Reconfiguración de dashboard generada por Power BI para la gestión de incidentes informados por CSIRT, se publica en forma temporal para revisión. CSIRT - 2024 - Eventos - v2 - Power BI.
- Revisión de boletín de seguridad emitido por el CSIRT de Gobierno N°264 – del 20/07/2024 al 26/07/2024. 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.

02/08/2024:

- 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.
- En base al reporte generado por CSIRT N°264 (20 al 26/07/2024) se incluyen el bloqueo EndPoint de Defender los siguientes Hash SHA256:

  Nombre asociado: Factura falsa impaga - Suplantación con Malware - CSIRT
  26c75dea56be0a425cd6fe3592fcf52a079a99bce79f8c5f80837268199f71d2
  bfefcee218f14d6730bfec6623b3c0af040e859e16e5a019c8e2b9b6ce352313

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

05/08/2024:

- 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 – Microsoft. Caso DAG Exchange 2016 On Premises. Se require habilitar replicación de bases de datos de casillas de correo entre los servidores Exchange 01, 02, 05, y 06. Se detecta la necesidad de tener espacio disponible en los servidores para soportar las bases de réplica. Se prorroga la actividad hasta que el espacio esté disponible.
- Revisión de boletín de seguridad emitido por el CSIRT de Gobierno N°265 – del 27/07/2024 al 05/08/2024. 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°265 (27/07/2024 al 05/08/2024) se incluyen el bloqueo EndPoint de Defender los siguientes Hash SHA256:

  Nombre asociado: SII - Suplantación con malware - CSIRT
  41421f5c12d966493a33483f6ea460a6162edb01d25ca6f7a07b0cfb5fba4bd7 --> impuestomayonopagoMayo.zip
  4ef45d10ebca266197d7461702a584f661c2b5df40f19f05cf7c56899ee7e2cc --> impuestomayonopagoMayo.bat
  96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7 --> __PSScriptPolicyTest_0fuj5rj1.0v2.ps1

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

06/08/2024:

- 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.
- 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:

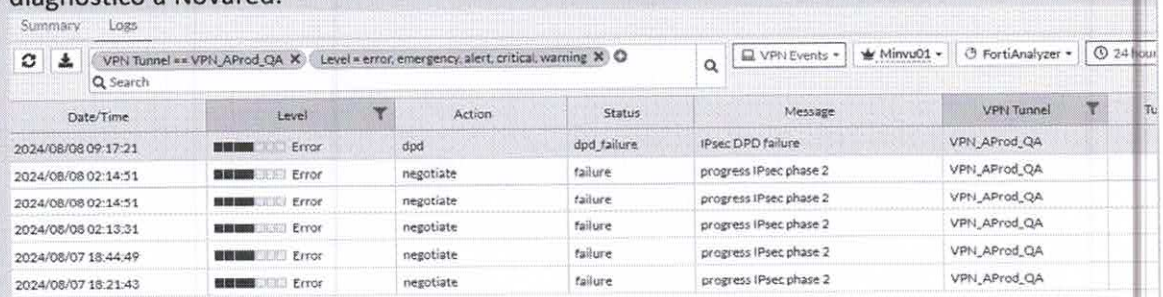
https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?tid=9cacd210-70a9-44ee-826b-f6b7685a01d6&childviewid=files

07/08/2024:

- 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.
- Reunión con Coordinadores Informáticos para analizar el evento suscitado los días 19 y 22 de julio. Presentación de los hechos (contexto), actividades realizadas, resultado de las gestiones. Se presentan actividades a aplicar para mitigar los problemas derivados de la conexión de equipos de comunicación no regulados o aprobados por la DINFO a la red institucional. Inicio 9:00 am, fin 10:00.
- 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.

08/08/2024:

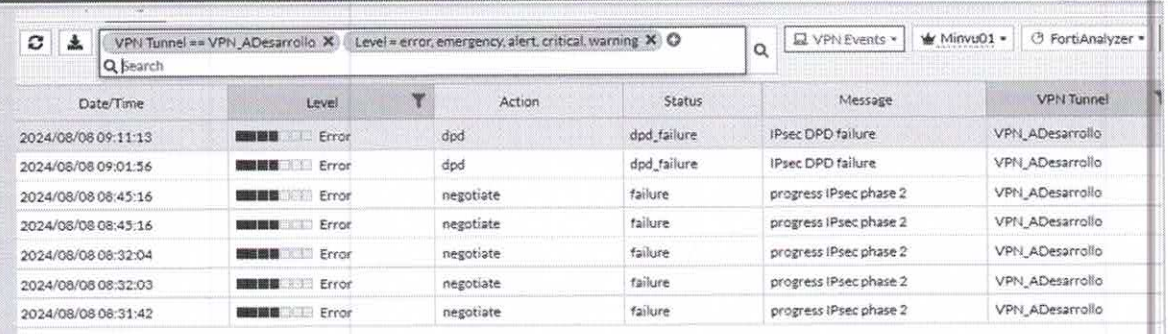
- Revisión de incidentes reportados por Novared en el firewall perimetral. Se registran antecedentes. Se revisa bloqueo si aplica. Se confirma bloqueo si aplica.
- Revisión y actualización de planilla de eventos de seguridad informados por el CSIRT. Derivación de diagnóstico de acuerdo con lo recomendado 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 riesgo de inicio de sesión para el usuario Mario Solorza Valenzuela, varios intentos de inicio de sesión desde el España el día 08/08/2024, como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Se detectan problemas con la VPN VPN_AProd_QA. Error de negociación en la fase 2. Se solicita diagnóstico a Novared.


Summary Logs

VPN Tunnel == VPN_AProd_QA | Level = error, emergency, alert, critical, warning | Search | VPN Events | Minvu01 | FortiAnalyzer | 24 hour

Date/Time	Level	Action	Status	Message	VPN Tunnel	Tu
2024/08/08 09:17:21	Error	dpd	dpd_failure	IPsec DPD failure	VPN_AProd_QA	
2024/08/08 02:14:51	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA	
2024/08/08 02:14:51	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA	
2024/08/08 02:13:31	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA	
2024/08/07 18:44:49	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA	
2024/08/07 18:21:43	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA	

-
- Se detectan problemas con la VPN VPN_ADsarrollo. Error de negociación en la fase 2. Se solicita diagnóstico a Novared.



Date/Time	Level	Action	Status	Message	VPN Tunnel
2024/08/08 09:11:13	Error	dpd	dpd_failure	IPsec DPD failure	VPN_ADesarrollo
2024/08/08 09:01:56	Error	dpd	dpd_failure	IPsec DPD failure	VPN_ADesarrollo
2024/08/08 08:45:16	Error	negotiate	failure	progress IPsec phase 2	VPN_ADesarrollo
2024/08/08 08:45:16	Error	negotiate	failure	progress IPsec phase 2	VPN_ADesarrollo
2024/08/08 08:32:04	Error	negotiate	failure	progress IPsec phase 2	VPN_ADesarrollo
2024/08/08 08:32:03	Error	negotiate	failure	progress IPsec phase 2	VPN_ADesarrollo
2024/08/08 08:31:42	Error	negotiate	failure	progress IPsec phase 2	VPN_ADesarrollo

-
- Incidente FW Fortinet. Perdida de conectividad a nivel internet, intermitencia del servicio. Se hace roll-back de solicitud de cambio realizado el día de ayer. Se reinicia dispositivo. Se recupera la conectividad.

09/08/2024:

- 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 riesgo de inicio de sesión para el usuario Mario Solorza Valenzuela, varios intentos de inicio de sesión desde el España el día 08/08/2024, como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Reunión Minvu – DINFO: Revisión plataforma Exchange On premises y estrategia de parchado.
    - Estado del parchado de los servidores a nivel de SO: Todos los servidores parchados e incorporados a Defender. Se tiene que analizar cómo aplicar el parchado a futuro: en forma manual o a través de SCCM.
        - Se plantea aplicar el escenario asociado al parchado de los servidores SQL, en el que se presenta el parche disponible y la necesidad de instalarlo. Con ello se programa la actividad de parchado en forma manual.
        - Para la próxima liberación de parches se aplicará en forma manual, tal como se aplicaron los parches anteriores @Carlos Valdés España aplicará en forma separada en horario no hábil.
        - Para las siguientes liberaciones de parches, aplicará el escenario SQL, @Waldo Gonzalez Armani configurará en SCCM la tarea.
    - Parchado a nivel de Exchange: Falta instalar último CU, sin embargo, se hace conveniente habilitar la replicación del DAG entre los servidores existentes (EXCH01, EXCH02, EXCH05 y EXCH06).
        - Seguimos a la espera de lo que se resuelva con el aumento de capacidad de recursos para los servidores que están en Liray.
    - Abrir caso DAG en Microsoft, responsable apertura: @Jorge Ramos Collio

        - Caso abierto, y atendido, es factible generar la replicación en el DAG, pero se requieren recursos en los servidores para poder mantener una copia de la base de datos de casilla a la cuál esté replicando.
        - Mientras no se tenga claridad con respecto a los recursos, se cierre el caso con Microsoft.
    - Mover tareas administrativas desde servidor EXCH03 a EXCH02 @Daniel Varela González, una vez migradas las tereas se puede sacar de la comunidad Exchange los servidores virtuales EXCH03 y EXCH04 y proceder a su apagado (junto con las máquinas físicas que los soportan).
        - Serán realizadas por @Carlos Valdés España, deberían estar migradas el martes próximo martes 13.
        - Posterior a la validación del correcto funcionamiento de las tareas, se puede proceder a dar de baja los servidores EXCH03 y EXCH04.
    - Conector Internet. Habilitar el ingreso de correos desde el conector Exchange On line, dejando fuera de flujo el Barracuda, los correos ingresan directamente desde internet.
        - Sigue como tema planteado. Ya se cuenta con la configuración necesaria, solo faltaría aplicarla.
    - @Jorge Ramos Collio debe revisar los recursos disponibles en Liray en caso de que sea necesario generar un nuevo servidor o si deba ser necesario agregar capacidad a los servidores EXCH01, EXCH02, EXCH05 y EXCH06.
        - Tema recursos. Pendiente.
    - Casillas compartidas: Hacer pruebas, identificar escenarios a aplicar.
        - Se generará documento de como generar casillas compartidas y cuando correspondería aplicarlas. Con @Daniel Varela González revisaremos la aplicabilidad.

12/08/2024:

- 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 inicio de sesión desde Brasil (Sao Paulo) el día 12/08/2024 para el usuario Ricardo Andrés Orellana Dubo, último inicio de sesión fue el 09/08/2024 en Chile (Santiago), se considera falso positivo (viaje posible). Riesgo de inicio de sesión para el usuario Diego Palma Zapata, varios intentos de inicio de sesión fallidos desde USA los días 11 y 12/08/2024, como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Reunión Minvu – Dinfo. Revisión del cambio de protocolo a aplicar en el firewall para lograr un mayor detalle de monitoreo.

- Definición de plantilla RFC para registrar y controlar cambios aplicados a nivel transversal en la infraestructura TI. Se elabora propuesta.

13/08/2024:

- 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 el usuario Camila Schmidlin Roccatagliata, a partir del 12/08/2024 solo hace inicio de sesión desde Españavarios intentos de inicio de sesión desde el España el día 08/08/2024, como medida preventiva, se fuerza el cambio de contraseña. Licencia EMS E5 vencida (trial) se deshabilitan varias funcionalidades relacionadas con Identity Manager.
- Revisión de Procedimiento de gestión de incidentes de Seguridad de la Información, en lo que concierne a eventos/incidentes de ciberseguridad. Correcciones revisadas en última reunión de coordinación. Homologación de categoría de riesgos.

14/08/2024:

- 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 DINFO. Tema: Incidente aplicación DS27. Para autenticación y definición de roles se utiliza PSSIM, para ello utiliza un token de autenticación y mediante consulta a PSSIM se obtienen los roles aplicables. En el incidente se hizo un bypass sin hacer consulta de roles a PSSIM, para ello se copió la URL de un acceso permitido y se accedió con una cuenta que no tenía el rol para acceder. Por cada clic en el sitio es necesario ir a consultar a la PSSIM por la autenticación y el rol, lo anterior provoca una lentitud en el tiempo de respuesta. Se modificará la aplicación para incorporar filtros de autenticación y rol en todas las páginas en que sea necesario.
- Revisión de boletín de seguridad emitido por el CSIRT de Gobierno N°266 – del 03/08/2024 al 09/08/2024. 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°266 (03/08/2024 al 09/08/2024) se incluyen el bloqueo EndPoint de Defender los siguientes Hash SHA256:

  Nombre asociado: CGE - Suplantación con malware - CSIRT
  06e049e5ab0d0d9cde2f65dcea95c652455497739bf65cb9b436ca38219d466f -->
  eletricidadRegularizarSituacionimediata.zip
  95c16c2f74bfe9878117d341d4b259c5327f87fc10e8407b27e9a905aff0ac11
  a4cf36830c669834e94109899ecd6e51787141f08045702b63d279b683ec1de0 -->
  eletricidadRegularizarSituacionimediata.cmd

  Nombre asociado: TGR - Suplantación con malware - CSIRT
  0f2bd749ec8827b857f82ab12e306840cffbe4000629b33f4cb60f336cf10c67 -->
  DevolucionImpuestoJulioTGR.cmd_N6sBSUmaTkleTr.cmd
  408b48b85c218925056c6951a8b29db3c81cee0696f35dcc1dfe3dfcf9e0ce5a -->
  DevolucionImpuestoJulioTGR.cmd_51648.zip

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

15/08/2024: Feriado

16/08/2024:

- 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). 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 de los reportes generados por Novared para la gestión de los equipos firewall perimetral más proxy de navegación.
- 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

19/08/2024:

- 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). 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 de cuentas con Azure MFA habilitado. Se cheque que las cuentas asociadas al rol Global Administrator tengan "forzada" o "habilitada" la opción de MFA. Dos alternativas para resolver el problema: 1.- No hacer nada y dejar que la cuenta de AD Connect siga perteneciendo al ROL de Global Administrator. Esto implicará que esta cuenta no se podrá utilizar, en el corto plazo (a partir del 15/10/2024), para acceder a los portales de administración de: Azure, Entra ID e Intune, y en el largo plazo (a partir de mediados del 2025) no se podrá utilizar para Azure Command Line, Azure Power Shell, Azure Mobile App e Infrastruture as Code (IaC). El resultado no tiene impacto ya que esa cuenta solo se utiliza para el servicio de sincronización de AD On Premises con Entra ID en Azure. No obstante lo anterior, seguiremos recibiendo advertencias por esta cuenta. 2.- Sacar la cuenta AD Connector del ROL Global Administrator, en la práctica no lo requiere. Para esta cuenta se recomienda solo asignar los siguientes permisos:
    - Administrador de usuarios: Permite crear, actualizar y eliminar usuarios en Azure AD.
    - Administrador de autenticación: Permite configurar y administrar la autenticación, incluyendo MFA.

  Este cambio podría tener algún impacto negativo en la sincronización de AD. Asignar el rol de Administrador Global a la cuenta de AD Connector puede otorgar más permisos de los necesarios, lo cual no es una práctica recomendada desde el punto de vista de la seguridad.

20/08/2024:

- 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 detectan usuarios en riesgo y/o con problemas de inicio de sesión (error). Usuario externo Sharepoint alejandrocuevas.arq@gmail.com, viaje imposible entre Concepción y Aisén, no se puede forzar el cambio de contraseña, se confirma compromiso de riesgo de la cuenta. 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°267 – del 10/08/2024 al 16/08/2024. 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°267 (10/08/2024 al 16/08/2024) se incluyen el bloqueo EndPoint de Defender los siguientes Hash SHA256:

Nombre asociado: TGR - Suplantación con malware - CSIRT - 14082024
4b4e7e2d39f3162e26766d8028ea9543f7932eaeed570d993e359ba13f403fad -->
DevolucionTGRnuevoImpuesto_27616.zip
bbab46ed7e7e2909c8d444aad7fa82d8e5e059a45d1b17e4a09f2f122390cd8c -->
DevolucionTGRnuevoImpuesto_jxoGJPU29vg.cmd

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

21/08/2024:

- 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_ADesarrollo. Para la VPN VPN_Aprod_QA se detectaron los siguientes errores:
- Entre las 15:04 y las 15:05 del 20/08/2024 se registraron errores de negociación en la VPN_APROD_QA.
-

Summary Logs

VPN Tunnel == VPN_AProd_QA ✕ Level = emergency, alert, critical, error, warning ✕ Search | VPN Events | Minvu01 | FortiAnalyzer

Date/Time	Level	Action	Status	Message	VPN Tunnel
2024/08/20 15:16:24	Error	dpd	dpd_failure	IPsec DPD failure	VPN_AProd_QA
2024/08/20 15:05:54	Error	dpd	dpd_failure	IPsec DPD failure	VPN_AProd_QA
2024/08/20 15:04:29	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:29	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:29	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:29	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:29	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:29	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:29	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:28	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:28	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:28	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:28	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:28	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:27	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA
2024/08/20 15:04:27	Error	negotiate	failure	progress IPsec phase 2	VPN_AProd_QA

-
-
- A las 15:05 y 15:16 del mismo día se registraron errores "dpd_failure".

Summary Logs

VPN Tunnel == VPN_AProd_QA ✕ Level = emergency, alert, critical, error, warning ✕ Search | VPN Events

Date/Time	Level	Action	Status	Message	
2024/08/20 15:16:24	Error	dpd	dpd_failure	IPsec DPD failure	VPN_AProd_
2024/08/20 15:05:54	Error	dpd	dpd_failure	IPsec DPD failure	VPN_AProd_

-
-

- 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.

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	22/08/2024