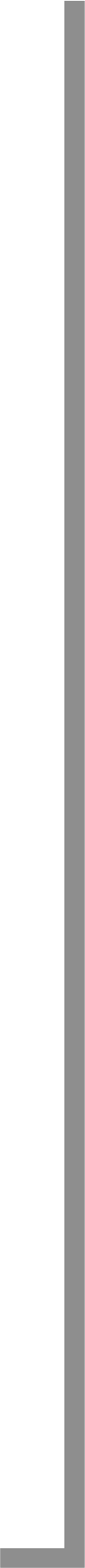
**SECURE SOFT CORPORATION**



**e-Secure Consulting Group**

**REPORTE MENSUAL**

**ESTADO DE SALUD**

**Preparado para:**

**Icono

Descripción generada automáticamente**

**Fecha:**

**${fecha\_actual}**



**El presente documento contiene información estrictamente privada y confidencial para SECURESOFT CORPORATION S.A.C. y BANBIF S.A.**

Indice

[I. OBJETIVO 5](#_Toc97045577)

[II. ALCANCE 5](#_Toc97045578)

[III. CONTENIDO 5](#_Toc97045579)

[**1.** **MONITOREO Y GESTIÓN DE LA INFRAESTRUCTURA** 5](#_Toc97045580)

[**2.** **CAPACIDAD TOTAL DE LOS EQUIPOS** 6](#_Toc97045581)

[**3.** **ESTADO DE PLATAFORMAS** 7](#_Toc97045582)

[**3.1.** **Resumen General y Detalle de las Plataformas** 7](#_Toc97045583)

[**3.2.** **PLATAFORMA CISCO** 8](#_Toc97045584)

[**3.2.1.** **Antispam Activo -San Isidro (10.1.100.24)** 8](#_Toc97045585)

[3.2.1.1. Recurso 8](#_Toc97045586)

[3.2.1.2. Estructura Sistema 8](#_Toc97045587)

[3.2.1.3. Correo Entrante 9](#_Toc97045588)

[3.2.1.4. Correo Saliente 9](#_Toc97045589)

[3.2.1.5. Licencia 9](#_Toc97045590)

[**3.2.2.** **Antispam Standby-IBM (10.3.200.24)** 10](#_Toc97045591)

[3.2.2.1. Recurso 10](#_Toc97045592)

[3.2.2.2. Estatus del Sistema 10](#_Toc97045593)

[3.2.2.3. Licencia 10](#_Toc97045594)

[**3.2.3.** **Tickets Asociados a la Plataforma** 11](#_Toc97045595)

[**3.2.4.** **Planeamiento** 20](#_Toc97045596)

[**3.2.5.** **Actualizaciones** 21](#_Toc97045597)

[**3.2.6.** **Conclusiones** 21](#_Toc97045598)

[**3.2.7.** **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)** 21](#_Toc97045599)

[**3.2.8.** **Recomendaciones:** 21](#_Toc97045600)

[**3.3.** **PLATAFORMA F5** 22](#_Toc97045601)

[**3.3.1.** **Balanceador Interno Principal-Virtual** 22](#_Toc97045602)

[3.3.1.1. Estado del equipo 22](#_Toc97045603)

[3.3.1.2. Recurso 22](#_Toc97045604)

[3.3.1.3. Conexiones concurrentes 22](#_Toc97045605)

[3.3.1.4. Throughput (bit) 23](#_Toc97045606)

[3.3.1.5. Licencia 23](#_Toc97045607)

[**3.3.2.** **Balanceador Interno Secundario-Virtual** 23](#_Toc97045608)

[3.3.2.1. Estado del equipo 23](#_Toc97045609)

[3.3.2.2. Recurso 24](#_Toc97045610)

[3.3.2.3. Conexiones concurrentes 24](#_Toc97045611)

[3.3.2.4. Throughput (bits) 24](#_Toc97045612)

[3.3.2.5. Licencia 24](#_Toc97045613)

[**3.3.3.** **Balanceador Perimetro Principal – San Isidro** 24](#_Toc97045614)

[3.3.3.1. Estado del Equipo 24](#_Toc97045615)

[3.3.3.2. Recurso 25](#_Toc97045616)

[3.3.3.3. Conexiones concurrentes 25](#_Toc97045617)

[3.3.3.4. Throughput (bit) 25](#_Toc97045618)

[3.3.3.5. Licencia 26](#_Toc97045619)

[**3.3.4.** **Balanceador Perimetro Secundario-IBM** 26](#_Toc97045620)

[3.3.4.1. Estado Equipo 26](#_Toc97045621)

[3.3.4.2. Recurso 26](#_Toc97045622)

[3.3.4.3. Conexiones Concurrentes 27](#_Toc97045623)

[3.3.4.4. Throughput (bit) 27](#_Toc97045624)

[3.3.4.5. Licencia 27](#_Toc97045625)

[**3.3.5.** **Balanceador Standalone QA-Virtual** 27](#_Toc97045626)

[3.3.5.1. Estado del Equipo 27](#_Toc97045627)

[3.3.5.2. Recurso 28](#_Toc97045628)

[3.3.5.3. Licencia 28](#_Toc97045629)

[**3.3.6.** **Tickets Asociados a la Plataforma** 28](#_Toc97045630)

[**3.3.7.** **Planeamiento** 30](#_Toc97045631)

[**3.3.8.** **Actualización** 31](#_Toc97045632)

[**3.3.9.** **Conclusiones** 31](#_Toc97045633)

[**3.3.10.** **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)** 31](#_Toc97045634)

[**3.3.11.** **Recomendaciones** 32](#_Toc97045635)

[**3.4.** **FIREWALL PERIMETRAL** 32](#_Toc97045636)

[**3.4.1.** **Firewall Perimetral Primario (IP)** 32](#_Toc97045637)

[3.4.1.1. Recursos 32](#_Toc97045638)

[3.4.1.2. Conexiones 32](#_Toc97045639)

[3.4.1.3. Licencias 32](#_Toc97045640)

[**3.4.2.** **Firewall Perimetral Secundario** 33](#_Toc97045641)

[3.4.2.1. Recursos 33](#_Toc97045642)

[3.4.2.2. Conexiones 33](#_Toc97045643)

[3.4.2.3. Licencias 33](#_Toc97045644)

[**3.4.3.** **Planeamiento** 34](#_Toc97045645)

[**3.4.4.** **Actualización** 34](#_Toc97045646)

[**3.4.5.** **Conclusiones** 35](#_Toc97045647)

[**3.4.6.** **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)** 35](#_Toc97045648)

[**3.4.7.** **Recomendaciones** 35](#_Toc97045649)

[**3.5.** **FORTIANALYZER** 35](#_Toc97045650)

[3.5.1. Recursos 35](#_Toc97045651)

[3.5.2. Licencia 35](#_Toc97045652)

[**3.5.3.** **Planeamiento** 36](#_Toc97045653)

[**3.5.4.** **Actualización:** 36](#_Toc97045654)

[**3.5.5.** **Conclusiones** 36](#_Toc97045655)

[**3.5.6.** **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)** 37](#_Toc97045656)

[**3.5.7.** **Recomendaciones** 37](#_Toc97045657)

[**3.6.** **PLATAFORMA DE AUTENTICACIÓN** 38](#_Toc97045658)

[**3.6.1.** **PLATAFORMA DE AUTENTICACION PRIMARIO** 38](#_Toc97045659)

[3.6.1.1. Recursos 38](#_Toc97045660)

[3.6.1.2. Licencia 38](#_Toc97045661)

[**3.6.2.** **PLATAFORMA DE AUTENTICACION SECUNDARIO** 38](#_Toc97045662)

[3.6.2.1. Recursos 38](#_Toc97045663)

[3.6.2.2. Licencia 39](#_Toc97045664)

[**3.6.3.** **Tickets Asociados a la Plataforma** 39](#_Toc97045665)

[**3.6.4.** **Planeamiento** 45](#_Toc97045666)

[**3.6.5.** **Actualización** 45](#_Toc97045667)

[**3.6.6.** **Conclusiones** 45](#_Toc97045668)

[**3.6.7.** **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)** 46](#_Toc97045669)

[**3.6.8.** **Recomendaciones** 46](#_Toc97045670)

[**3.7.** **PLATAFORMA IMPERVA** 46](#_Toc97045671)

[**3.7.1.** **SBF (Consola de Administración) (IP)** 46](#_Toc97045672)

[3.7.1.1. CPU 46](#_Toc97045673)

[3.7.1.2. Conexiones concurrentes 47](#_Toc97045674)

[3.7.1.3. Estado de Firewalls administrable de la consola 47](#_Toc97045675)

[3.7.1.4. Resumen de estado de los agentes en los Firewall 48](#_Toc97045676)

[**3.7.2.** **Tickets Asociado a la Plataforma** 48](#_Toc97045677)

[**3.7.3.** **Planeamiento** 50](#_Toc97045678)

[**3.7.4.** **Conclusiones** 50](#_Toc97045679)

[**3.7.5.** **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)** 50](#_Toc97045680)

[**3.7.6.** **Recomendaciones** 50](#_Toc97045681)

[**3.8.** **PLATAFORMA QUALYS** 51](#_Toc97045682)

[3.8.1. Vulnerabilidades por Severidad 51](#_Toc97045683)

[3.8.2. Licencias 51](#_Toc97045684)

[3.8.3. Tickets Asociados a la Plataforma 51](#_Toc97045685)

[**3.8.4.** **Conclusiones** 52](#_Toc97045686)

[**3.8.5.** **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)** 52](#_Toc97045687)

[**3.8.6.** **Recomendaciones** 52](#_Toc97045688)

[**3.9.** **VPN** 53](#_Toc97045689)

[**3.9.1.** **VPN Securesoft-Banbif** 53](#_Toc97045690)

[**3.9.2.** **VPN Americatel-Banbif** 53](#_Toc97045691)

[**4.** **MONITOREO DE SEGURIDAD** 53](#_Toc97045692)

[IV. CONCLUSIONES 59](#_Toc97045693)

1. **OBJETIVO**

Este documento dará a conocer el estado de salud de plataformas de seguridad durante el último mes.

1. **ALCANCE**

Este documento servirá como herramienta para verificar el estado de las plataformas de seguridad y su correcto funcionamiento.

1. **CONTENIDO**
   1. **MONITOREO Y GESTIÓN DE LA INFRAESTRUCTURA**

* En el mes de enero, se atendieron 211 requerimientos reactivos, entre cambios, solicitudes e incidentes.
* Se notificaron 24 eventos de seguridad – threat hunting, 34 eventos de salud.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Etiquetas de fila** | **Cambio** | **Evento** | **Solicitud** | **Incidente** |
| F5-BALANCEADOR-BIF2BIGIP10.DOMBIF.PERU | 23 |  | 6 | 1 |
| F5-BALANCEADOR-BIGIP01-SI-BANBIF |  | 17 |  |  |
| FORTINET-FIREWALL-FORTIAUTENTICADOR PRIMARIO-BANBIF | 56 | 1 | 2 |  |
| FORTINET-FIREWALL-PERIMETRAL PRIMARIO-BANBIF | 6 | 6 | 4 |  |
| FORTINET-FORTIANALYZER-BANBIF |  |  | 1 |  |
| IMPERVA-DATABASE FIREWALL-01-BANBIF | 2 | 1 |  |  |
| IMPERVA-MANAGEMENT WAF-BANBIF | 10 |  | 3 |  |
| QUALYS-VULNERABILITY MANAGER-BANBIF | 6 |  | 3 |  |
| F5-BALANCEADOR-BIGIP01-SI-BANBIF |  | 3 |  |  |
| CISCO-ANTISPAM-MOLINA-BANBIF |  |  | 4 |  |
| CISCO-ANTISPAM-IBM-BANBIF | 6 | 6 | 20 |  |
| CISCO-ANTISPAM-SMA-BANBIF |  | 24 |  |  |
| **Total General** | **109** | **58** | **43** | **1** |

* 1. **CAPACIDAD TOTAL DE LOS EQUIPOS**

|  |  |  |
| --- | --- | --- |
| **EQUIPO** | **CAPACIDAD** | |
| **DISCO** | **MEMORIA** |
| **AntiSpam Activo – San Isidro** | 320 GB | 8 GB |
| **AntiSpam Standby - IBM** | 320 GB | 8 GB |
| **Balanceador Interno Principal - Virtual** | 85 GB | 15.6 GB |
| **Balanceador Interno Secundario - Virtual** | 85 GB | 15.6 GB |
| **Balanceador Perimetro Principal – San Isidro** | 326 GB | 15.6 GB |
| **Balanceador Perimetro Secundario – IBM** | 326 GB | 15.6 GB |
| **Balanceador Standalone QA – Virtual** | 59 GB | 7.7 GB |
| **Firewall Perimetral Primario** | - | 94.6 GB |
| **Firewall Perimetral Secundario** | - | 94.6 GB |
| **Fortianalyzer** | 32 TB | 62.1 GB |
| **Plataforma de Autenticación Primario** | 4 TB | 15.7 GB |
| **Plataforma de Autenticación Secundaria** | 4 TB | 15.7 GB |
| **Lataforma Imperva DBF** | 500 GB | 8 GB |

* 1. **ESTADO DE PLATAFORMAS**
  2. **Resumen General y Detalle de las Plataformas**

|  |  |  |
| --- | --- | --- |
| Equipos | Estado | Servicio |
| AntiSpam Activo-San Isidro | UP | OK |
| AntiSpam Standby-IBM | UP | OK |
| Balanceador Interno Principal-Virtual | UP | OK |
| Balanceador Interno Secundario-Virtual | UP | OK |
| Balanceador Perimetro Principal-San Isidro | UP | OK |
| Balanceador Perimetro Secundario-IBM | UP | OK |
| Balanceador Standalone QA-Virtual | UP | OK |
| Firewall Perimetral Primario | UP | OK |
| Firewall Perimetral Secundario | UP | OK |
| Fortianalyzer | UP | OK |
| Plataforma de Autenticación Primaria | UP | OK |
| Plataforma Imperva DBF | UP | OK |
| Plataforma Qualys | UP | OK |
| VPN Securesoft-Banbif | UP | OK |
| VPN Americatel-Banbif | UP | OK |

* 1. **PLATAFORMA CISCO**
     1. **Antispam Activo -San Isidro (10.1.100.24)**
        1. Recurso

${graph2618}

* Se observó que el uso promedio de **CPU** durante el mes es de 26.65%.
* Se observó que el uso promedio de **Disco** durante el mes es de 25.05%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 5.35%.
  + - 1. Estructura Sistema

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* + - 1. Correo Entrante

Gráfico

Descripción generada automáticamente con confianza media

(\*) Se presenta data de la última semana del mes de Enero.

* + - 1. Interfaz de usuario gráfica, Aplicación

         Descripción generada automáticamenteCorreo Saliente

(\*) Se presenta data de la última semana del mes de Enero.

* + - 1. Licencia

Fecha de Expiración: 16/Sep/2022

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

* + 1. **Antispam Standby-IBM (10.3.200.24)**
       1. Recurso

${graph2622}

* Se observó que el uso promedio de **CPU** durante el mes es de 16.09%.
* Se observó que el uso promedio de **Disco** durante el mes es de 4%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 1%.
  + - 1. Estatus del Sistema

Tabla

Descripción generada automáticamente con confianza media

* + - 1. Licencia

Fecha de Expiración: 16/Septiembre/2022

Tabla

Descripción generada automáticamente

* + 1. **Tickets Asociados a la Plataforma**

|  |  |  |
| --- | --- | --- |
| **Ticket** | **Referencia** | **Comentario** |
| CAM68999 | Ticket Aranda 98772 - Crear usuario VPN BANBIF | Se brindó los permisos RDP se solicitó. |
| SOL271532 | Ticket Aranda 98784 - Revision de politicas de acceso BANBIF | Se realizaron las revisiones solicitadas. |
| SOL272083 | Reporte Mensual Qualys - ticket 98805 | para informar que se importó todos los reportes generados, mensuales de la consola Qualys a la ruta compartida. Correspondientes a mis tareas cada fin de mes. Nuevos reportes SICN solicitados: |
| CAM69146 | Errores de waf modulos adicionales F5 - ticket 98806 | se observo que el bloqueo fue por un parametro no permitido en el request, se acepto la sugerencia del waf y luego de ello se valida que no hay bloqueos de waf |
| SOL272091 | Liberar correo Antispam - TICKET 98807 | se libero el correo retenido |
| SOL272092 | Consulta de salida de correo fuera de la organización - 98008 | se cierra el ticket debido a que estamos a al espera de confirmación de jeniffer y hernan lopez, de obtener el VB se puede realizar la configuración , se abrirá nuevo ticket cuando tengamos la aprobación |
| SOL272096 | Reporte Mensual Qualys - ticket 98833 | se envio el informe mensual técnico Global de Vulnerabilidad. a jeniffer rojas |
| SOL272108 | Bitácora de cambios - 1Q Y 2Q DICIEMBRE | informe enviado al cliente |
| SOL272109 | Bitácora de cambios - 1Q Y 2Q DICIEMBRE FORTINET | informe enviado al cliente |
| CAM69161 | Ticket Aranda 98813 - Crear usuario VPN BANBIF | Se brindó los permisos RDP solicitados. |
| SOL272176 | Restauracion de archivo a identificar quien lo borro - Imperva DBF | se envio el reporte de los usuarios que realizaron la acción delete para la ruta tecnología |
| CAM69214 | Ticket Aranda 98855 - Extencion de permisos usuario VPN | Se brindaron los permisos solicitados. |
| CAM69215 | Ticket Aranda 98804 - Crear usuario VPN BANBIF | Se brindaron los permisos solicitados. |
| CAM69407 | Ticket Aranda 98911 - Crear usuario VPN BANBIF | Se brindó los permisos VPN solicitados. |
| CAM69447 | Ticket Aranda 98920 - Renovacion de acceso usuario VPN BANBIF | Se brindó los permisos VPN solicitados. |
| SOL273365 | Informe Mensual - BACKUP DICIEMBRE | informe enviado |
| CAM69628 | Ticket Aranda 98931 - Crear usuario VPN Proveedores. | Se brindó los permisos VPN solicitados. |
| CAM69760 | Ticket Aranda 98973 - Crear usuario VPN BANBIF | Se brindó los permisos VPN solicitados. |
| CAM69802 | SOL 274107 - BOLETÍN-NUEVA CAMPAÑA DE ZLOADER EXPLOTA VERIFICACIÓN DE FIRMAS DE MICROSOFT-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM69949 | SOL 274608-BOLETÍN-NUEVA ACTUALIZACION DE LOS INDICADORES DEL MALWARE REDLINE STEALER-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70040 | SOL 274865-BOLETÍN-NUEVA ACTUALIZACION DE LOS INDICADORES DEL MALWARE REDLINE STEALER-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70041 | SOL 274865-BOLETÍN-NUEVA ACTUALIZACION DE LOS INDICADORES DEL MALWARE REDLINE STEALER-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70042 | SOL 274882-BOLETÍN-NUEVA ACTIVIDAD DEL BACKDOOR PURPLE FOX UTILIZA APLICACIÓN FALSA DE TELEGRAM MESSENGER-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70104 | Ticket Aranda 99021 - Crear usuario VPN BANBIF. | Se brindó los permisos VPN solicitados. |
| CAM70107 | SOL 275053-BOLETÍN-NUEVA CAMPAÑA DE SKIMMER A CADENA DE SUMINISTROS DE VIDEO EN LA NUBE-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70114 | SOL 275096-BOLETÍN-MALWARE REDLINE ROBA CREDENCIALES GUARDADAS EN NAVEGADORES WEB-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70140 | Ticket Aranda 99038 - Renovacion de Acceso usuario VPN BANBIF | Se brindó los permisos VPN solicitados. |
| SOL275288 | QUALYS - ORDENAMIENTO DE REPORTES - ticket 99047 | se realizo el re-ordenamiento de todos los reportes mensuales de la carpeta compartida y se informo a jeniffer rojas, quien no solicito realizar la tarea de reordenar los reportes. |
| CAM70145 | SOPORTE F5 WAF - ticket 99048 | se valido que waf reconocia los caracteres /var/ como desconocidos por lo cual lo bloqueaba, pero f5 nos recomendaba aceptar la recomendación para que se aplique a la política y ya no sé tengan bloqueos en bpiuat2 |
| SOL275293 | EH Integral - F5 ticket 99049 | se envio el excel de todas las publicaciones " Virtual Servers" para que sea sustentado por brian paredes. |
| SOL275296 | antispam - ticket 98876 | solo hubo 1 correo retenido de LATAM el cual fue liberado |
| SOL275297 | Antispam - ticket 98810 | no sé tienen correos retenidos, el unico que se encontro fue liberado. |
| SOL275309 | EVIDENCIAS DE CONFIGURACIÓN F5 INTERNO - TICKET 99050 | se envio las evidencias de princing a marcial pardo, sobre las reglas waf que ya fueron configuradas. |
| SOL275310 | Print configuraciones Princing en el F5 - WAF - ticket 99051 | se valida que no existe servicios con el nombre VS-WebPricePresentacion-https-prd y se informo a marcial pardo lo mencionado |
| SOL275313 | CERTIFICADO F5 VENCIDOS Y BEST PRACTICE - ticket 99053 | se envio la documentación del RFC para que sea sustentado en comite por parte de Brian Paredes |
| CAM70156 | errores de waf modulos adicionales - ticket 99054 | se valido que el bloqueo fue por problemas de caracteres no permitidos, se procedio a aceptarlos y el problema fue superado. |
| CAM70157 | Liberar correo - ticket 99055 | se libero el correo retenido para infratisapia01@banbif.com.pe |
| CAM70167 | BIFRECUPERA30 AGENTE RUNNING WITH ERRORS - ticket 99056 | se realizo el upgrade del agente a la version 14.4 con lo cual el problema de cipher no soportados fue superado |
| SOL275351 | DIAGRAMA FÍSICO F5 - ticket 99057 | se realizo el diagramá de los f5 externos |
| CAM70170 | TRABAJOS PROGRAMADOS F5 EXTERNO WORK-AROUND F5 - ticket 99059 | se realizo el reinicio del f5 externo para evitar que el consumo de memoría swap afecte servicios, con lo cual el consumo disminuyo, |
| CAM70171 | RECUPERAR PASSWORD GATEWAY 10.200.100.214 - ticket 99060 | se reseteo el password del gw para poder acceder al equipo que estaba bloqueado,   luego del reseteo de credenciales se valida el acceso al gateway imperva |
| CAM70172 | DEPURAR ESPACIO DEL DISCO - ticket 99067 | se depuro políticas de auditoría para liberar el espacio del gateway, luego de lo cual el problema del poco espacio del gateway superado. |
| CAM70194 | SOL 275399-BOLETÍN-NUEVA CAMPAÑA DE SPEAR-PHISHING DE SIDECOPY APT-BAN-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70274 | INC 273958-ALERTA-ESPACIO EN DISCO-BAN-MEDIA | se depuro políticas de auditoría para liberar el espacio del gateway, luego de lo cual el problema del poco espacio del gateway superado. |
| CAM70275 | INC 273958-ALERTA-ESPACIO EN DISCO-BAN-MEDIA | se depuro políticas de auditoría para liberar el espacio del gateway, luego de lo cual el problema del poco espacio del gateway superado. |
| CAM70277 | Regla de Balanceo - Proyecto TI-EA2021-12164 TIN Inmediatas IPS- ticket 99097 | se valido que luego de configrar el automap en el virtual server el problema fue superado. |
| CAM70368 | Ticket Aranda 99103 - Crear usuario VPN BANBIF. | Se brindó los permisos VPN solicitados. |
| CAM70396 | Ticket Aranda 99141 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70405 | SOL 276020-BOLETÍN-NUEVA ACTIVIDAD DEL RANSOMWARE ECH0RAIX-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70409 | Ticket Aranda 99144 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM70410 | Ticket Aranda 99145 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM70418 | Ticket Aranda 99154 - Modificar politica de usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM70584 | Ticket Aranda 99178 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM70585 | Ticket Aranda 99211 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM70597 | Ticket Aranda 99208 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70599 | Ticket Aranda 99212 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70600 | Ticket Aranda 99213 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70601 | Ticket Aranda 99214 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70604 | Ticket Aranda 99217 - Crear Politica de acceso para de lexmark. | Se brindo los permisos solicitados en la MATRIZ. |
| CAM70606 | Ticket Aranda 99199 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70618 | SOL 276575-BOLETÍN-NUEVO MALWARE FLAGPRO UTILIZADO POR BLACKTECH-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70619 | SOL 276575-BOLETÍN-NUEVO MALWARE FLAGPRO UTILIZADO POR BLACKTECH-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| SOL276642 | SCANEO DE VULNERABILIDADES | se envio el reporte de los servidores 10.200.150.150 y 10.200.150.151, luego de realizar el scan en qualys, se compartio el detalle onsite de optical jesus peña herrera. |
| SOL276661 | REPORTE F5 EXTERNOS - ESTADO DE SALUD | se envio el reporte mensual de los equipos de seguridad, del estado de salud |
| SOL276670 | Liberar correo usuario jwong@banbif.com.pe | se libero el correo retenido a josewong el motivo era que en el cuerpo del mensaje utilizaban la palabra " haga click aqui " la cual está en el diccionario considerado como palabra de indole maliciosa. |
| CAM70639 | Ticket Aranda 99232 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM70642 | SOL 276682-BOLETÍN-NUEVA INFORMACIÓN DEL GRUPO DE CIBERDELINCUENTES NOBELIUM-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM70648 | Ticket Aranda 99237 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70649 | Ticket Aranda 99240 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM70787 | Asunto: Ticket Aranda 99265 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70891 | INC 276175-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Se procedio con el bloqueo del correo @pabrikapd.com |
| CAM70949 | Ticket Aranda 99318 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70950 | Ticket Aranda 99323 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70957 | Ticket Aranda 99325 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70962 | Ticket Aranda 99326 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70969 | importacion de certificado f5 | En proceso |
| CAM70974 | Ticket Aranda 99324 - Extender vigencia de usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70989 | Ticket Aranda 99327 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM71031 | SOL 277907-BOLETÍN-ABCBOT BOTNET VINCULADO A MALWARE XANTHE CRYPTOMINING-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71045 | creacion de balance | En proceso |
| CAM71112 | SOL 278104-BOLETÍN-APT35 EXPLOTA LA VULNERABILIDAD DE LOG4J PARA OFRECER ESTA NUEVA BACKDOOR 'MODULAR'-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71113 | SOL 278104-BOLETÍN-APT35 EXPLOTA LA VULNERABILIDAD DE LOG4J PARA OFRECER ESTA NUEVA BACKDOOR 'MODULAR'-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71244 | SOL 278507-BOLETÍN-RANSOMWARE UTILIZA LA FALLA LOG4J COMO PARTE DE SUS ATAQUES-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71245 | SOL 278507-BOLETÍN-RANSOMWARE UTILIZA LA FALLA LOG4J COMO PARTE DE SUS ATAQUES-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| SOL279015 | RE: INC 278638-ALERTA-ESPACIO EN DISCO-BAN-MEDIA | se observa que el espacio de disco del equipo BANBIF - Imperva - DBF - Firewall BD Servidores Produccion destinado a Disco/var se encuentra dentro del umbral permitido, superando la alerta. Adicional a ello no se visualizan alarmas en el equipo |
| SOL279032 | Ticket Aranda 99353 - Reporte de usuario VPN Proveedores. | Se brindó los datos solicitados. |
| CAM71461 | INC 277378-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Se realizó el bloqueo de la IOC malicioso  @srebanetools.com |
| CAM71480 | Ticket Aranda 99393 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM71484 | SOL 278372-BOLETÍN-MALWARE FLUBOT SE DISTRIBUYE COMO FLASH PLAYER -BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71486 | SOL 278812-BOLETÍN-NUEVO BACKDOOR MALWARE LLAMADO SYSJOCKER-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71529 | SOL 279259-BOLETÍN-CAMPAÑA SNATCHCRYPTO DEL MALWARE BLUENOROFF-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71530 | SOL 279259-BOLETÍN-CAMPAÑA SNATCHCRYPTO DEL MALWARE BLUENOROFF-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71553 | Ticket Aranda 99434 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM71559 | Pase A PRD WAF F5 de Pricing | Buenas noches, se procedió a modificar la política a modo bloqueo según lo solicitado |
| CAM71625 | SOL 279433-BOLETÍN-NUEVA INFORMACIÓN DEL RANSOMWARE TELLYOUTHEPASS-BIF-ALTA | Se procedio con el bloqueo de las siguientes IOCs: IP 158[.]247[.]216[.]148 45[.]76[.]99[.]222 |
| CAM71695 | Ticket Aranda 99459 - Generar token usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM71794 | SOL 279929-BOLETÍN-NUEVA VERSIÓN DEL MALWARE REDLINE DIFUNDIDO COMO UN CONTADOR DE ESTADÍSTICAS FALSO DE OMICRON-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71795 | SOL 279929-BOLETÍN-NUEVA VERSIÓN DEL MALWARE REDLINE DIFUNDIDO COMO UN CONTADOR DE ESTADÍSTICAS FALSO DE OMICRON-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71849 | INC 278822-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Se procedió con el bloqueo de dominio. |
| CAM71914 | SOL 280130-BOLETÍN-NUEVA ACTIVIDAD ASOCIADA A LOG4SHELL-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM71955 | Ticket Aranda 97720 - Crear politica de acceso FIREWALL. | Se brindó los permisos solicitados. |
| CAM71956 | Ticket Aranda 99488 - Crear politica de bloqueo FIREWALL. | Se realizaron los bloqueos solicitados. |
| CAM71960 | Ticket Aranda 99489 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM71961 | Ticket Aranda 99490 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM71979 | Ticket Aranda 99508 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM72009 | SOL 280556-BOLETÍN-APLICACIÓN FALSA UTILIZA INFORMACIÓN COVID-19 OMICRON PARA DISTRIBUIR MALWARE REDLINE STEALER-BAN-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM72010 | SOL 280556-BOLETÍN-APLICACIÓN FALSA UTILIZA INFORMACIÓN COVID-19 OMICRON PARA DISTRIBUIR MALWARE REDLINE STEALER-BAN-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM72015 | SOL 280566-BOLETÍN-RANSOMWARE MAGNIBER SE DISTRIBUYE A TRAVEZ DE MICROSOFT EDGE Y GOOGLE CHROME-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM72021 | Ticket Aranda 99517 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM72038 | Ticket Aranda 99527 - Crear usuario VPN Proveedores. | Se brindaron los accesos solicitados. |
| CAM72049 | Ticket Aranda 99531 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM72050 | Ticket Aranda 99532 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM72169 | SOL 280876-BOLETÍN-NUEVA CAMPAÑA POR CIBERDELINCUENTES INTENTA PROPAGAR DIFERENTES MALWARE RAT-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM72171 | SOL 280876-BOLETÍN-NUEVA CAMPAÑA POR CIBERDELINCUENTES INTENTA PROPAGAR DIFERENTES MALWARE RAT-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM72230 | Ticket Aranda 99533 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| SOL281258 | revision de alertas antispam cisco | En proceso |
| CAM72348 | SOL 281387-BOLETÍN-NUEVO RANSOMWARE WHITE RABBIT ES UTILIZADO POR EL GRUPO DE CIBERDELINCUENTES FIN8-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM72414 | Ticket Aranda 99589 - Crear usuario VPN BANBIF. | Se brindó los permisos VPN solicitado. |
| CAM72438 | revision bloqueo waf | En proceso |
| CAM72447 | Ticket Aranda 99603 - Crear usuario VPN Proveedores. | Se brindó los permisos VPN solicitados. |
| CAM72574 | SOL 282273-BOLETÍN-NUEVA CAMPAÑA DE PHISHING ESTA PROPAGANDO ARCHIVOS .MHTML-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM72741 | SOL 282741-BOLETÍN-NUEVO MALWARE BHUNT-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM72747 | Ticket Aranda 99569 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM72758 | INC 281406-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Se realizó el bloqueo de la IOC malicioso  @hanazza.com |
| CAM73065 | SOL 283530-BOLETÍN-NUEVA INFORMACIÓN DEL RANSOMWARE HIVE-BAN-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM73076 | Ticket Aranda 99675 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM73089 | Ticket Aranda 99677 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM73186 | Ticket Aranda 99707 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM73210 | Ticket Aranda 99715 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM73447 | SOL 284479-BOLETÍN-NUEVA ACTIVIDAD DEL RANSOMWARE CONTI-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM73450 | SOL 284479-BOLETÍN-NUEVA ACTIVIDAD DEL RANSOMWARE CONTI-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM73460 | SOL 284471-BOLETÍN-NUEVA CAMPAÑA DE EMOTET-BIF-ALTA | se realizó el bloqueo de la IOC malicioso |
| CAM73485 | SOL 284517 - BOLETÍN-NUEVA CAMPAÑA DE PHISHING APARENTA SER EL DEPARTAMENTO DE TRABAJO DE EE.UU -BIF -MEDIA | se realizó el bloqueo de la IOC malicioso |
| CAM73531 | Configuración de Balanceo Balanceador 10.200.104.244 - TICKET 99610 | se modifico el puerto en los pool members del balanceador 10.200.104.244 que direcciona hacía los nodos 10.30.31.87 y 10.30.31.86 |
| CAM73532 | Actualizar regla en WAF Pricing - TICKET 99612 | Se agregó la excepción en la política waf princing de acuerdo a lo solicitado por marcial pardo |
| CAM73533 | F5 Balanceo NUEVO Aplicativo Tablero de Control APP- TICKET 99673 | se creo los virtual server para los servicios, Virtual server con IP: 10.200.104.233, Virtual server con IP: 10.200.104.235 |
| CAM73534 | Correos - TICKET 99674 | se libero el correo retenido para el sender preyesd@intercorp.com.pe |
| CAM73535 | Antispam - TICKET 99701 | se libero los correos que envía La Caja Militar de Pensiones, |
| CAM73545 | RECEPCION DE CORREO EXTERNO - TICKET 130907 | se libero los correos retenidos del sender noreply@vendemas.com.pe |
| INC284630 | :INCIDENCIA BXI - TICKET 130937 | el incidente se debido a el cambio de política de modo transparente a modo bloqueo, el presente cambio fue solicitado debido a una vulnerabilidad de etical hacking brindada por el equipo de banbif y para mitigarlo el cliente banbif solicito realizar el cambio de política a modo bloqueo lo que ocacionó el INC |
| SOL284631 | problemas con recepción de correos - TICKET 99757 | se valido que no hay bloqueos del dominio @ortizlossio.com y los correos fluyen sin problemas |
| CAM73631 | [BANBIF] F5 WAF - POLITICA MODO BLOCK | se acepto las sugerencias de f5, para la exepción de los falsos positivos |
| CAM73655 | Ticket Aranda 99775 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM73715 | [CAM73631][BANBIF]F5 WAF - POLITICA MODO BLOCK | En proceso |
| CAM73716 | BLOQUEOS DE F5 | se acepto las sugerencias de f5, para la exepción de los falsos positivos |
| CAM73718 | INC 284592-ALERTA-ESPACIO EN DISCO-BIF-MEDIA | se depuro los archivos de backup antiguos |
| CAM73719 | NUEVOS Servidores Controladores de dominio 2019 PRD - AÑADIR ASSEST | se añadio los servidores al grupo Directorio Activo – LDAP\_PRD |
| CAM73721 | NUEVOS Servidores Controladores de dominio 2019 PRD - Plantilla reporte | se creo el template para la generación de reportes para el grupo Directorio Activo – LDAP\_PRD |
| CAM73730 | NUEVOS Servidores Controladores de dominio 2019 PRD - CREACIÓN DE GRUPO | se añadio los nuevos servidores al se creo al grupo Directorio Activo – LDAP\_PRD |
| CAM73731 | Urgente - Transferencias al Exterior vía Web | se realizo el cambio de la política a modo bloqueo, pero se encuentra en proceso de monitoreo en caso de encontrarse QID de bloqueo |
| CAM73732 | BANCA POR INTERNETEMPRESAS | se realizo el cambio de la política a modo bloqueo, pero se encuentra en proceso de monitoreo en caso de encontrarse QID de bloqueo |
| SOL285084 | Revisión Health Check Imperva BANBIF | Se envio el reporte de healcheck de los equipos imperva |
| SOL285089 | Reporte alertas Check Imperva BANBIF | se genero el reporte de alertas del imperva MX al equipo de BANBIF |
| CAM73736 | Ticket Aranda 99525 - Habilitar politica BANBIF. | Se habilito la política con ID 1152. |
| CAM73738 | Ticket Aranda 99801 - Extender vigencia de usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM73739 | Ticket Aranda 99802 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| SOL285136 | TEMAS IMPERVA | se realizo la transferencia de conocimiento a lizbeth Quispe |
| SOL285140 | INFORME MANTENIMIENTO Antispam | se envio el informe de mantenimiento del equipo antispam a victor pineda |
| SOL285143 | INFORME MANTENIMIENTO F5 | se envio el informe de mantenimiento del equipo F5 a victor pineda |
| SOL285148 | EXCEL IPS PUBLICAS - F5 EXTERNOS | se envio el reporte de ips publicas a brian paredes y jorge piñan |
| CAM73757 | Depuración IPs - Qualys | se realizo la depuración de las 30 IPs del qualys brindadas por jeniffer rojas |
| SOL285162 | Reportes IMPERVA | En proceso |
| SOL285177 | Ajuste en Politica de VS observados | se realizo el cambio de politica de modo transparente a modo bloqueo |
| CAM73764 | BLOQUEO ANTISPAM | se colocó el dominio en lista negra @SAASONIA , a solicitud de jose wong por motivos de spam |
| CAM73765 | Asunto:ISSUE WITH AGENT BIF1REC22 - RUNNING WITH ERRORS | se actualizo el agente a la versión 14.4 y luego del upgrade el issue fue mitigado |
| CAM73766 | ISSUE WITH AGENT GENERICO-RUNNING WITH ERRORS | se actualizo el agente a la versión 14.4 y luego del upgrade el issue fue mitigado |
| CAM73853 | SOL 285296-BOLETÍN-NUEVA ACTIVIDAD HACKTIVISTAS EN BIELORRUSIA-BIF-ALTA | Se realizo el bloqueo del dominio 3proxy.ru |
| CAM73918 | Ticket Aranda 99825 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM73956 | F5 Balanceo NUEVO Aplicativo Tablero de Control APP | se creo el balanceo con IP: 10.200.104.235 |
| CAM73957 | Balanceo NUEVO Aplicativo Tablero de Control APP - Certificado | se importo el certificado para el balanceo con IP: 10.200.104.235 |
| CAM73958 | F5 Balanceo NUEVO Aplicativo Tablero de Control APP - Certificado | se renovarlo certificados SSL para los virtual Server   Certificado TableroControlsrv-uat.pfx  Aplicar al Virtual server con IP: 10.200.104.235 |
| CAM73960 | ALERT-SERVIDOR DESCONECTADO-BIF-MEDIA | se realizo la depuración del agente BIF1LYNC30 |
| CAM73961 | ALERT-SERVIDOR DESCONECTADO-BIF-MEDIA | se realizo la depuración del agenteBIF1MEYCOR30 |
| CAM73965 | ALERT-SERVIDOR DESCONECTADO-BIF-MEDIA | se realizo la depuración del agente , políticas y template |
| CAM73966 | BLOQUEO WAF | se acepto la sugerencia de WAF para evitar falsos posítivos |
| CAM73967 | Seminario: TRABAJO REMOTO y retorno a la Presencialidad | se bloqueó el dominio por motivos de spam  @sfk-security.com |
| CAM73968 | BLOQUEO WAF2 | se acepto las sugerencias de waf para evitar falsos positivos |
| CAM73981 | TRABAJO REMOTO y retorno a la Presencialidad | se realizo el bloqueo del sender spam |
| CAM73983 | Liberar correo | se libero los correos retenidos para el usuario infratiMS |
| SOL285857 | Solicitud de Salida de Correos - ticket 99817 | Se envio la lista de correos que se enviaron los correos al siguiente cliente: Correo Destino: PAULOPOZZUOLI@GMAIL.COM, la información fue entragada a Jayshon chavez de banbif |
| SOL285858 | Antispam | se valido que no hay correos retenidos del dominio @notarialaos.com.pe, el flujo de correos es normal |
| SOL285859 | Antispam - ticket 99836 | se valido que no hay bloqueos del domini @notarialaos.com.pe y que el flujo de correos se mantiene sin problemas |
| SOL285861 | Correos - ticket 99864 | se liberaron los correos retenidos de los sender :ozcocodovaisabel@gmail.com nramos@maquinarias.pe |

* + 1. **Planeamiento**
    2. **Actualizaciones**
    3. Actualizaciones Realizadas en el mes:

No se realizó actualizaciones durante este periodo.

* + 1. Actualización a Realizarse en el próximo mes:

No sé realizará, debido a que la nueva versión 14.0.2 no es estable.

* + 1. **Conclusiones**
* Se observa los recursos estables del Antispam Activo y Standby .
* Las licencias vencen el 16/09/2022
* Los indicadores de consumo de CPU y memoria RAM muestran un performance Correcto del clúster.
* Se observa que los equipos se encuentran en la versión 14.0.0-698
* Se valida que los filtros de seguridad para correos con spam, virus operan correctamente siendo estos retenidos por el antispam
  + 1. **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)**

**“Se recomienda depurar los usuarios locales, debido a que la plataforma actualmente**

**se tiene enganchada al AD, por lo cual solo se recomienda dejar 3 usuarios**

**1 para seguridad de información Banbif, 1 para soporte Securesoft, finalmente 1**

**para el monitoreo de salud – SecureSoc. ”**

Se compartió la lista y el sustento de los usuarios a eliminar al equipo de banco,

el presente cambio se encuentra en coordinación con el cliente y se llevará acabo

durante el periodo 2022.

**“Se mantendrá en monitoreo verificar la estabilidad (validando con fabricante)**

**de la versión 14.0.2 y realizar la actualización de la plataforma cisco ESA y SMA”.**

Se valido con fabricante y aún la versión 14.0.2 no es recomendable por temas de

estabilidad.

* + 1. **Recomendaciones:**

Se recomienda mantener en monitoreo la estabilidad de la versión 14.0.2 para realizar

la actualización de la plataforma cisco ESA y SMA.

* 1. **PLATAFORMA F5**
     1. **Balanceador Interno Principal-Virtual**
        1. Estado del equipo

${graph2638}

\*2: Estado Pasivo

**\*4: Estado Activo**

* + - 1. Recurso

${graph2629}

* Se observó que el uso promedio de CPU durante el mes es de 21.28%.
* Se observó que el uso promedio de **Disco** durante el mes es de 24%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 38.04%.
  + - 1. Conexiones concurrentes

${graph2631}

* + - 1. Throughput (bit)

${graph2626}

* + - 1. Licencia

La licencia es bajo el tiempo de soporte adquirido.

* + 1. **Balanceador Interno Secundario-Virtual**
       1. Estado del equipo

${graph2657}

**\*2: Estado Pasivo** \*4: Estado Activo

* + - 1. Recurso

${graph2648}

* Se observó que el uso promedio de **CPU** durante el mes es de 19.47%.
* Se observó que el uso promedio de **Disco** durante el mes es de 24%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 30%.
  + - 1. Conexiones concurrentes

${graph2650}

* + - 1. Throughput (bits)

${graph2645}

* + - 1. Licencia

La licencia es bajo el tiempo de soporte adquirido

* + 1. **Balanceador Perimetro Principal – San Isidro**
       1. Estado del Equipo

${graph2676}

\*3: Estado Pasivo  
 **\*4: Estado Activo**

* + - 1. Recurso

${graph2667}

* Se observó que el uso promedio de **CPU** durante el mes es de 35.09%.
* Se observó que el uso promedio de **Disco** durante el mes es de 23%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 17.21%.
  + - 1. Conexiones concurrentes

${graph2669}

* + - 1. Throughput (bit)

${graph2664}

* + - 1. Licencia

La licencia es bajo el tiempo de soporte adquirido.

* + 1. **Balanceador Perimetro Secundario-IBM**
       1. Estado Equipo

${graph2695}

**\*2: Estado Pasivo**

\*4: Estado Activo

* + - 1. Recurso

${graph2686}

* Se observó que el uso promedio de **CPU** durante el mes es de 21.79%.
* Se observó que el uso promedio de **Disco** durante el mes es de 23%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 11.99%.
  + - 1. Conexiones Concurrentes

${graph2688}

* + - 1. Throughput (bit)

${graph2683}

* + - 1. Licencia

La licencia es bajo el tiempo de soporte adquirido.

* + 1. **Balanceador Standalone QA-Virtual**
       1. Estado del Equipo

${graph2714}

\*3: Estado Pasivo  
**\*4: Estado Activo**

* + - 1. Recurso

${graph2705}

* Se observó que el uso promedio de **CPU** durante el mes es de 11.75%.
* Se observó que el uso promedio de **Disco** durante el mes es de 24%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 17.99%.
  + - 1. Licencia

NA

* + 1. **Tickets Asociados a la Plataforma**

|  |  |  |
| --- | --- | --- |
| **Ticket** | **Referencia** | **Comentario** |
| CAM69146 | Errores de waf modulos adicionales F5 - ticket 98806 | se observo que el bloqueo fue por un parametro no permitido en el request, se acepto la sugerencia del waf y luego de ello se valida que no hay bloqueos de waf |
| CAM70145 | SOPORTE F5 WAF - ticket 99048 | se valido que waf reconocia los caracteres /var/ como desconocidos por lo cual lo bloqueaba, pero f5 nos recomendaba aceptar la recomendación para que se aplique a la política y ya no sé tengan bloqueos en bpiuat2 |
| SOL275293 | EH Integral - F5 ticket 99049 | se envio el excel de todas las publicaciones " Virtual Servers" para que sea sustentado por brian paredes. |
| SOL275309 | EVIDENCIAS DE CONFIGURACIÓN F5 INTERNO - TICKET 99050 | se envio las evidencias de princing a marcial pardo, sobre las reglas waf que ya fueron configuradas. |
| SOL275310 | Print configuraciones Princing en el F5 - WAF - ticket 99051 | se valida que no existe servicios con el nombre VS-WebPricePresentacion-https-prd y se informo a marcial pardo lo mencionado |
| SOL275313 | CERTIFICADO F5 VENCIDOS Y BEST PRACTICE - ticket 99053 | se envio la documentación del RFC para que sea sustentado en comite por parte de Brian Paredes |
| CAM70156 | errores de waf modulos adicionales - ticket 99054 | se valido que el bloqueo fue por problemas de caracteres no permitidos, se procedio a aceptarlos y el problema fue superado. |
| CAM70157 | Liberar correo - ticket 99055 | se libero el correo retenido para infratisapia01@banbif.com.pe |
| SOL275351 | DIAGRAMA FÍSICO F5 - ticket 99057 | se realizo el diagramá de los f5 externos |
| CAM70170 | TRABAJOS PROGRAMADOS F5 EXTERNO WORK-AROUND F5 - ticket 99059 | se realizo el reinicio del f5 externo para evitar que el consumo de memoría swap afecte servicios, con lo cual el consumo disminuyo, |
| CAM70969 | importacion de certificado f5 | En proceso |
| CAM71045 | creacion de balance | En proceso |
| CAM71559 | Pase A PRD WAF F5 de Pricing | Buenas noches, se procedió a modificar la política a modo bloqueo según lo solicitado |
| CAM73531 | Configuración de Balanceo Balanceador 10.200.104.244 - TICKET 99610 | se modifico el puerto en los pool members del balanceador 10.200.104.244 que direcciona hacía los nodos 10.30.31.87 y 10.30.31.86 |
| CAM73532 | Actualizar regla en WAF Pricing - TICKET 99612 | Se agregó la excepción en la política waf princing de acuerdo a lo solicitado por marcial pardo |
| CAM73533 | F5 Balanceo NUEVO Aplicativo Tablero de Control APP- TICKET 99673 | se creo los virtual server para los servicios, Virtual server con IP: 10.200.104.233, Virtual server con IP: 10.200.104.235 |
| CAM73545 | RECEPCION DE CORREO EXTERNO - TICKET 130907 | se libero los correos retenidos del sender noreply@vendemas.com.pe |
| INC284630 | :INCIDENCIA BXI - TICKET 130937 | el incidente se debido a el cambio de política de modo transparente a modo bloqueo, el presente cambio fue solicitado debido a una vulnerabilidad de etical hacking brindada por el equipo de banbif y para mitigarlo el cliente banbif solicito realizar el cambio de política a modo bloqueo lo que ocacionó el INC |
| CAM73715 | [CAM73631][BANBIF]F5 WAF - POLITICA MODO BLOCK | En proceso |
| CAM73716 | BLOQUEOS DE F5 | se acepto las sugerencias de f5, para la exepción de los falsos positivos |
| CAM73718 | INC 284592-ALERTA-ESPACIO EN DISCO-BIF-MEDIA | se depuro los archivos de backup antiguos |
| CAM73731 | Urgente - Transferencias al Exterior vía Web | se realizo el cambio de la política a modo bloqueo, pero se encuentra en proceso de monitoreo en caso de encontrarse QID de bloqueo |
| CAM73732 | BANCA POR INTERNETEMPRESAS | se realizo el cambio de la política a modo bloqueo, pero se encuentra en proceso de monitoreo en caso de encontrarse QID de bloqueo |
| SOL285143 | INFORME MANTENIMIENTO F5 | se envio el informe de mantenimiento del equipo F5 a victor pineda |
| SOL285148 | EXCEL IPS PUBLICAS - F5 EXTERNOS | se envio el reporte de ips publicas a brian paredes y jorge piñan |
| SOL285177 | Ajuste en Politica de VS observados | se realizo el cambio de politica de modo transparente a modo bloqueo |
| CAM73956 | F5 Balanceo NUEVO Aplicativo Tablero de Control APP | se creo el balanceo con IP: 10.200.104.235 |
| CAM73957 | Balanceo NUEVO Aplicativo Tablero de Control APP - Certificado | se importo el certificado para el balanceo con IP: 10.200.104.235 |
| CAM73958 | F5 Balanceo NUEVO Aplicativo Tablero de Control APP - Certificado | se renovarlo certificados SSL para los virtual Server   Certificado TableroControlsrv-uat.pfx  Aplicar al Virtual server con IP: 10.200.104.235 |
| CAM73966 | BLOQUEO WAF | se acepto la sugerencia de WAF para evitar falsos posítivos |
| CAM73968 | BLOQUEO WAF2 | se acepto las sugerencias de waf para evitar falsos positivos |
| CAM73981 | TRABAJO REMOTO y retorno a la Presencialidad | se realizo el bloqueo del sender spam |
| CAM74054 | ENMASCARAMIENTO DE TARJETAS DE CREDITO - F5 | En proceso |

* + 1. **Planeamiento**
    2. **Actualización**

1. Actualizaciones Realizadas en el mes:

-No sé tiene contemplado actualización en el presente mes.

1. Actualizaciones a Realizarse en el siguiente mes:

-No sé tiene contemplado actualización en el presente mes.

* + 1. **Conclusiones**
* Se observa los recursos se encuentran dentro de los parámetros normales, se tiene certificados vencidos y virtuales servers deshabilitados.
  + 1. **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)**

**“Se recomienda realizar el seguimiento del proyecto renovación tecnológica F5, para realizar**

**el cambio de equipos físicos, y proseguir con la depuración de certificados no utilizados y**

**virtual servers deshabilitados, finalmente actualizar el equipo a la versión 15.1.3.1”**

Se recomienda realizar el seguimiento del proyecto renovación tecnológica F5, para realizar

el cambio de equipos físicos durante el periodo 2022 (actualmente se encuentra en proceso de

implementación).

* + 1. **Recomendaciones**

Se recomienda realizar el seguimiento del proyecto renovación tecnológica F5, para realizar

el cambio de equipos físicos durante el periodo 2022(se encuentra en implementación).

* 1. **FIREWALL PERIMETRAL**
     1. **Firewall Perimetral Primario (IP)**
        1. Recursos

${graph29419}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.40%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 20.07%.
  + - 1. Conexiones

${graph29427}

* + - 1. Licencias

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* + 1. **Firewall Perimetral Secundario**
       1. Recursos

${graph29407}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.001%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 20.56%.
  + - 1. Conexiones

${graph29415}

* + - 1. Licencias

Tabla

Descripción generada automáticamente

* + 1. **Planeamiento**
    2. **Actualización** 
       - 1. Actualizaciones Realizadas en el mes:

No se realizó upgrade de la versión en ambos firewalls.

* + - * 1. Actualizaciones a Realizarse en el siguiente mes:

No se tiene programado ningún upgrade para el mes de febrero del 2022.

* + 1. **Conclusiones**
* Los recursos de sistema tienen mayor consumo en el equipo principal pues todas las sesiones fluyen por el miembro activo del clúster.
* Los valores de consumo de CPU y memoria están dentro del umbral permitido para un buen rendimiento del appliance.
* El número de conexiones refleja un correcto trabajo del appliance firewall y se encuentra dentro de los valores estimados y permitidos por el equipo.
* Las licencias generales del equipo se encuentran activas y válidas hasta el 27/08/2025.
  + 1. **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)**

**“Se recomienda seguir con el hardening de políticas y objetos que dejen de usarse”**

* Se ejecuto el mantenimiento continuo de hardening de política, donde se busca ordenar de la mejor manera las políticas del firewall por zonas y funciones.
  + 1. **Recomendaciones**
* Continuar con el hardening de políticas mensual y objetos que dejen de usarse.

- Se tiene la versión de firmware más estable “v6.4.5” recomendada por Fortinet; se estará evaluando migrar a la versión 7.0.4 en el próximo mantenimiento preventivo en los primeros meses del presente año 2022.

* 1. **FORTIANALYZER**
     1. Recursos

${graph16236}

* Se observó que el uso promedio de **Disco** durante el mes es de 45.92%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 65.43%.
  + 1. Licencia

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

* + 1. **Planeamiento**
    2. **Actualización:**

Actualizaciones Realizadas en el mes:

* No se realizó upgrade de la versión de la plataforma.

Actualizaciones a Realizarse en el siguiente mes:

* No se tiene programado ningún upgrade para el mes de febrero del 2022.
  + 1. **Conclusiones**

Los valores de consumo de CPU y memoria se encuentran dentro de los umbrales permitidos para un correcto funcionamiento del appliance.

Las licencias se encuentran activas hasta el 27/08/2025.

* + 1. **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)**

**“Revisar periódicamente el consumo de disco para logs archive y analytics con el fin de mantener todos los logs por 365 días”.**

* Se realizo la revisión de consumo de disco para logs archive y analytics, donde se observo que los valores son estables asegurando los logs por 365 días.
* **“Realizar programación de reportes diarios para consultas frecuentes como consumo de VPN o login de usuarios VPN”.**
* Tabla, Sitio web

  Descripción generada automáticamenteSe realizo modificación de las plantillas para los reportes de consumo y login de usuarios VPN; estos reportes se ejecutan a solicitud del banco.
* **“Se tiene la versión más estable recomendada por Fortinet; se estará evaluando el upgrade del firmware el próximo mantenimiento preventivo”.**
* Se continúa trabajando con la versión más estable recomendada por Fortinet; la cual no ha presentado problemas durante el mes.



* + 1. **Recomendaciones**

- Revisar periódicamente el consumo de disco para logs archive y analytics con el fin de mantener todos los logs por 365 días.

- Realizar programación de reportes diarios para consultas frecuentes como consumo de VPN o login de usuarios VPN.

- Se tiene la versión de firmware 6.4.5 estable recomendada por Fortinet; se estará evaluando una actualización en el próximo mantenimiento preventivo en los primeros meses del presente año 2022.

* 1. **PLATAFORMA DE AUTENTICACIÓN** 
     1. **PLATAFORMA DE AUTENTICACION PRIMARIO**
        1. Recursos

${graph15609}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.03%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 29.44%.
* Se observó que el uso promedio de **Disco** durante el mes es de 1%.
  + - 1. Licencia

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* + 1. **PLATAFORMA DE AUTENTICACION SECUNDARIO**
       1. Recursos

${graph26690}

* Se observó que el uso promedio de **CPU** durante el mes es de 0.00%.
* Se observó que el uso promedio de **Memoria** durante el mes es de 16.60%.
  + - 1. Licencia

Tabla

Descripción generada automáticamente

* + 1. **Tickets Asociados a la Plataforma**

|  |  |  |
| --- | --- | --- |
| **Ticket** | **Referencia** | **Comentario** |
| CAM68999 | Ticket Aranda 98772 - Crear usuario VPN BANBIF | Se brindó los permisos RDP se solicitó. |
| SOL271532 | Ticket Aranda 98784 - Revision de politicas de acceso BANBIF | Se realizaron las revisiones solicitadas. |
| SOL272109 | Bitácora de cambios - 1Q Y 2Q DICIEMBRE FORTINET | informe enviado al cliente |
| CAM69161 | Ticket Aranda 98813 - Crear usuario VPN BANBIF | Se brindó los permisos RDP solicitados. |
| CAM69214 | Ticket Aranda 98855 - Extencion de permisos usuario VPN | Se brindaron los permisos solicitados. |
| CAM69215 | Ticket Aranda 98804 - Crear usuario VPN BANBIF | Se brindaron los permisos solicitados. |
| CAM69407 | Ticket Aranda 98911 - Crear usuario VPN BANBIF | Se brindó los permisos VPN solicitados. |
| CAM69447 | Ticket Aranda 98920 - Renovacion de acceso usuario VPN BANBIF | Se brindó los permisos VPN solicitados. |
| SOL273365 | Informe Mensual - BACKUP DICIEMBRE | informe enviado |
| CAM69628 | Ticket Aranda 98931 - Crear usuario VPN Proveedores. | Se brindó los permisos VPN solicitados. |
| CAM69760 | Ticket Aranda 98973 - Crear usuario VPN BANBIF | Se brindó los permisos VPN solicitados. |
| CAM69802 | SOL 274107 - BOLETÍN-NUEVA CAMPAÑA DE ZLOADER EXPLOTA VERIFICACIÓN DE FIRMAS DE MICROSOFT-ALTA | se realizó el bloqueo d |
| CAM69949 | SOL 274608-BOLETÍN-NUEVA ACTUALIZACION DE LOS INDICADORES DEL MALWARE REDLINE STEALER-BIF-ALTA | se realizó el bloqueo d |
| CAM70040 | SOL 274865-BOLETÍN-NUEVA ACTUALIZACION DE LOS INDICADORES DEL MALWARE REDLINE STEALER-BIF-ALTA | se realizó el bloqueo d |
| CAM70041 | SOL 274865-BOLETÍN-NUEVA ACTUALIZACION DE LOS INDICADORES DEL MALWARE REDLINE STEALER-BIF-ALTA | se realizó el bloqueo d |
| CAM70042 | SOL 274882-BOLETÍN-NUEVA ACTIVIDAD DEL BACKDOOR PURPLE FOX UTILIZA APLICACIÓN FALSA DE TELEGRAM MESSENGER-BIF-ALTA | se realizó el bloqueo d |
| CAM70104 | Ticket Aranda 99021 - Crear usuario VPN BANBIF. | Se brindó los permisos VPN solicitados. |
| CAM70107 | SOL 275053-BOLETÍN-NUEVA CAMPAÑA DE SKIMMER A CADENA DE SUMINISTROS DE VIDEO EN LA NUBE-BIF-ALTA | Se procedio con el bloqueo de la IOCS Maliciosas IP 36[.]75[.]75[.]75 |
| CAM70114 | SOL 275096-BOLETÍN-MALWARE REDLINE ROBA CREDENCIALES GUARDADAS EN NAVEGADORES WEB-BIF-ALTA | se procedio con el bloqueo de la IOCS Maliciosas Dominio topkeygen[.]com |
| CAM70140 | Ticket Aranda 99038 - Renovacion de Acceso usuario VPN BANBIF | Se brindó los permisos VPN solicitados. |
| CAM70194 | SOL 275399-BOLETÍN-NUEVA CAMPAÑA DE SPEAR-PHISHING DE SIDECOPY APT-BAN-ALTA | se realizó el bloqueo d |
| CAM70368 | Ticket Aranda 99103 - Crear usuario VPN BANBIF. | Se brindó los permisos VPN solicitados. |
| CAM70396 | Ticket Aranda 99141 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70405 | SOL 276020-BOLETÍN-NUEVA ACTIVIDAD DEL RANSOMWARE ECH0RAIX-BIF-ALTA | se realizó el bloqueo d |
| CAM70409 | Ticket Aranda 99144 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM70410 | Ticket Aranda 99145 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM70418 | Ticket Aranda 99154 - Modificar politica de usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM70584 | Ticket Aranda 99178 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM70585 | Ticket Aranda 99211 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM70597 | Ticket Aranda 99208 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70599 | Ticket Aranda 99212 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70600 | Ticket Aranda 99213 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70601 | Ticket Aranda 99214 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70604 | Ticket Aranda 99217 - Crear Politica de acceso para de lexmark. | Se brindo los permisos solicitados en la MATRIZ. |
| CAM70606 | Ticket Aranda 99199 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70618 | SOL 276575-BOLETÍN-NUEVO MALWARE FLAGPRO UTILIZADO POR BLACKTECH-BIF-ALTA | se realizó el bloqueo d |
| CAM70619 | SOL 276575-BOLETÍN-NUEVO MALWARE FLAGPRO UTILIZADO POR BLACKTECH-BIF-ALTA | se realizó el bloqueo d |
| CAM70639 | Ticket Aranda 99232 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM70642 | SOL 276682-BOLETÍN-NUEVA INFORMACIÓN DEL GRUPO DE CIBERDELINCUENTES NOBELIUM-BIF-ALTA | se realizó el bloqueo d |
| CAM70648 | Ticket Aranda 99237 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70649 | Ticket Aranda 99240 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM70787 | Asunto: Ticket Aranda 99265 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70949 | Ticket Aranda 99318 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70950 | Ticket Aranda 99323 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70957 | Ticket Aranda 99325 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70962 | Ticket Aranda 99326 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70974 | Ticket Aranda 99324 - Extender vigencia de usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM70989 | Ticket Aranda 99327 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM71031 | SOL 277907-BOLETÍN-ABCBOT BOTNET VINCULADO A MALWARE XANTHE CRYPTOMINING-BIF-ALTA | se realizó el bloqueo d |
| CAM71112 | SOL 278104-BOLETÍN-APT35 EXPLOTA LA VULNERABILIDAD DE LOG4J PARA OFRECER ESTA NUEVA BACKDOOR 'MODULAR'-BIF-ALTA | se realizó el bloqueo d |
| CAM71113 | SOL 278104-BOLETÍN-APT35 EXPLOTA LA VULNERABILIDAD DE LOG4J PARA OFRECER ESTA NUEVA BACKDOOR 'MODULAR'-BIF-ALTA | se realizó el bloqueo d |
| CAM71244 | SOL 278507-BOLETÍN-RANSOMWARE UTILIZA LA FALLA LOG4J COMO PARTE DE SUS ATAQUES-BIF-ALTA | se realizó el bloqueo d |
| CAM71245 | SOL 278507-BOLETÍN-RANSOMWARE UTILIZA LA FALLA LOG4J COMO PARTE DE SUS ATAQUES-BIF-ALTA | se realizó el bloqueo d |
| SOL279032 | Ticket Aranda 99353 - Reporte de usuario VPN Proveedores. | Se brindó los datos solicitados. |
| CAM71480 | Ticket Aranda 99393 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM71484 | SOL 278372-BOLETÍN-MALWARE FLUBOT SE DISTRIBUYE COMO FLASH PLAYER -BIF-ALTA | se realizó el bloqueo d |
| CAM71486 | SOL 278812-BOLETÍN-NUEVO BACKDOOR MALWARE LLAMADO SYSJOCKER-BIF-ALTA | se realizó el bloqueo d |
| CAM71529 | SOL 279259-BOLETÍN-CAMPAÑA SNATCHCRYPTO DEL MALWARE BLUENOROFF-BIF-ALTA | se realizó el bloqueo d |
| CAM71530 | SOL 279259-BOLETÍN-CAMPAÑA SNATCHCRYPTO DEL MALWARE BLUENOROFF-BIF-ALTA | se realizó el bloqueo d |
| CAM71553 | Ticket Aranda 99434 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM71625 | SOL 279433-BOLETÍN-NUEVA INFORMACIÓN DEL RANSOMWARE TELLYOUTHEPASS-BIF-ALTA | se realizó el bloqueo d |
| CAM71695 | Ticket Aranda 99459 - Generar token usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM71794 | SOL 279929-BOLETÍN-NUEVA VERSIÓN DEL MALWARE REDLINE DIFUNDIDO COMO UN CONTADOR DE ESTADÍSTICAS FALSO DE OMICRON-BIF-ALTA | se realizó el bloqueo d |
| CAM71795 | SOL 279929-BOLETÍN-NUEVA VERSIÓN DEL MALWARE REDLINE DIFUNDIDO COMO UN CONTADOR DE ESTADÍSTICAS FALSO DE OMICRON-BIF-ALTA | se realizó el bloqueo d |
| CAM71914 | SOL 280130-BOLETÍN-NUEVA ACTIVIDAD ASOCIADA A LOG4SHELL-BIF-ALTA | se realizó el bloqueo d |
| CAM71955 | Ticket Aranda 97720 - Crear politica de acceso FIREWALL. | Se brindó los permisos solicitados. |
| CAM71956 | Ticket Aranda 99488 - Crear politica de bloqueo FIREWALL. | Se realizaron los bloqueos solicitados. |
| CAM71960 | Ticket Aranda 99489 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM71961 | Ticket Aranda 99490 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM71979 | Ticket Aranda 99508 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM72009 | SOL 280556-BOLETÍN-APLICACIÓN FALSA UTILIZA INFORMACIÓN COVID-19 OMICRON PARA DISTRIBUIR MALWARE REDLINE STEALER-BAN-ALTA | se realizó el bloqueo d |
| CAM72010 | SOL 280556-BOLETÍN-APLICACIÓN FALSA UTILIZA INFORMACIÓN COVID-19 OMICRON PARA DISTRIBUIR MALWARE REDLINE STEALER-BAN-ALTA | se realizó el bloqueo d |
| CAM72015 | SOL 280566-BOLETÍN-RANSOMWARE MAGNIBER SE DISTRIBUYE A TRAVEZ DE MICROSOFT EDGE Y GOOGLE CHROME-BIF-ALTA | se realizó el bloqueo d |
| CAM72021 | Ticket Aranda 99517 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM72038 | Ticket Aranda 99527 - Crear usuario VPN Proveedores. | Se brindaron los accesos solicitados. |
| CAM72049 | Ticket Aranda 99531 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM72050 | Ticket Aranda 99532 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM72169 | SOL 280876-BOLETÍN-NUEVA CAMPAÑA POR CIBERDELINCUENTES INTENTA PROPAGAR DIFERENTES MALWARE RAT-BIF-ALTA | se realizó el bloqueo d |
| CAM72171 | SOL 280876-BOLETÍN-NUEVA CAMPAÑA POR CIBERDELINCUENTES INTENTA PROPAGAR DIFERENTES MALWARE RAT-BIF-ALTA | se realizó el bloqueo d |
| CAM72230 | Ticket Aranda 99533 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM72348 | SOL 281387-BOLETÍN-NUEVO RANSOMWARE WHITE RABBIT ES UTILIZADO POR EL GRUPO DE CIBERDELINCUENTES FIN8-BIF-ALTA | Se procedio con el bloqueo de las siguientes IOCs: Dominio 104-168-132-128[.]nip[.]io/ URL hxxps://104-168-132-128[.]nip[.]io/ |
| CAM72414 | Ticket Aranda 99589 - Crear usuario VPN BANBIF. | Se brindó los permisos VPN solicitado. |
| CAM72447 | Ticket Aranda 99603 - Crear usuario VPN Proveedores. | Se brindó los permisos VPN solicitados. |
| CAM72574 | SOL 282273-BOLETÍN-NUEVA CAMPAÑA DE PHISHING ESTA PROPAGANDO ARCHIVOS .MHTML-BIF-ALTA | se realizó el bloqueo d |
| CAM72741 | SOL 282741-BOLETÍN-NUEVO MALWARE BHUNT-BIF-ALTA | se realizó el bloqueo d |
| CAM72747 | Ticket Aranda 99569 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM73065 | SOL 283530-BOLETÍN-NUEVA INFORMACIÓN DEL RANSOMWARE HIVE-BAN-ALTA | Se realizó el bloqueo de la IOC malicioso 46.166.161.123 46.166.161.93 192.53.123.202 |
| CAM73076 | Ticket Aranda 99675 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM73089 | Ticket Aranda 99677 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM73186 | Ticket Aranda 99707 - Crear usuario VPN Proveedores | Se brindo los permisos VPN solicitados. |
| CAM73210 | Ticket Aranda 99715 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM73447 | SOL 284479-BOLETÍN-NUEVA ACTIVIDAD DEL RANSOMWARE CONTI-BIF-ALTA | se realizó el bloqueo d |
| CAM73450 | SOL 284479-BOLETÍN-NUEVA ACTIVIDAD DEL RANSOMWARE CONTI-BIF-ALTA | se realizó el bloqueo d |
| CAM73460 | SOL 284471-BOLETÍN-NUEVA CAMPAÑA DE EMOTET-BIF-ALTA | se realizó el bloqueo d |
| CAM73485 | SOL 284517 - BOLETÍN-NUEVA CAMPAÑA DE PHISHING APARENTA SER EL DEPARTAMENTO DE TRABAJO DE EE.UU -BIF -MEDIA | se realizó el bloqueo d |
| CAM73631 | [BANBIF] F5 WAF - POLITICA MODO BLOCK | se acepto las sugerencias de f5, para la exepción de los falsos positivos |
| CAM73655 | Ticket Aranda 99775 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM73736 | Ticket Aranda 99525 - Habilitar politica BANBIF. | Se habilito la política con ID 1152. |
| CAM73738 | Ticket Aranda 99801 - Extender vigencia de usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM73739 | Ticket Aranda 99802 - Crear usuario VPN BANBIF | Se brindo los permisos VPN solicitados. |
| CAM73853 | SOL 285296-BOLETÍN-NUEVA ACTIVIDAD HACKTIVISTAS EN BIELORRUSIA-BIF-ALTA | Se realizo el bloqueo del dominio 3proxy.ru |
| CAM73918 | Ticket Aranda 99825 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM74150 | SOL 286162-BOLETÍN-NUEVA INFORMACIÓN DEL APT DONOT TEAM-BIF-ALTA | Se realizo el bloqueo de los siguientes Indicadores de Compromiso Dominio soundedge.live printerjobs.xyz |
| CAM74278 | SOL 286536-BOLETÍN-NUEVA INFORMACIÓN DEL MALWARE BRATA-BIF-MEDIA | Se procedió con el bloqueo de las siguientes IOCs: IP 5.39.217.241 |
| CAM74354 | Ticket Aranda 99915 - Crear usuario VPN BANBIF. | Se brindo los permisos VPN solicitados. |
| CAM74361 | Ticket Aranda 99845 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |
| CAM74363 | Ticket Aranda 99922 - Crear usuario VPN Proveedores. | Se brindo los permisos VPN solicitados. |

* + 1. **Planeamiento**
    2. **Actualización**

Actualizaciones Realizadas en el mes:

No se ha realizado ningún upgrade durante el presente mes.

Actualizaciones a Realizarse en el siguiente mes:

No se realizará ningún upgrade durante el mes de Febrero del 2022.

* + 1. **Conclusiones**

Los valores de consumo de CPU y memoria se encuentran dentro de los umbrales permitidos para un correcto funcionamiento del appliance.

Las licencias se encuentran activas hasta el 27/08/2025.

* + 1. **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)**

**“Mantener un control de grupos con usuarios que ya no existen en el AD”.**

* Se mantiene una revisión continua de los usuarios depurados en el AD.

**“Mantener un control de los FortiToken asignados a cada usuario que usen VPN”.**

* Se mantiene una revisión continua de los fortiToken disponibles, los cuales son liberados cuando se hace una depuración de usuarios en el AD.

**“Se tiene la versión más estable recomendada por Fortinet; se estará evaluando migrar a la versión 6.4.5 en el próximo mantenimiento preventivo”.**

* Se continúa trabajando con la versión más estable recomendada por Fortinet; la cual no ha presentado problemas durante el mes.



* + 1. **Recomendaciones**
* Mantener un control de grupos con usuarios que ya no existen en el AD.
* Mantener un control de los FortiToken asignados a cada usuario que usen VPN.
* Se tiene la versión más estable recomendada por Fortinet; se estará evaluando migrar a la versión 6.4.5 en el próximo mantenimiento preventivo a principios del 2022.
  1. **PLATAFORMA IMPERVA**
     1. **SBF (Consola de Administración) (IP)**
        1. CPU

${graph2726}

* Se observó que el uso promedio de **CPU** durante el mes es de 17.70%.
  + - 1. Conexiones concurrentes

${graph2727}

Se observa que la cantidad de conexiones es estable.

* + - 1. Estado de Firewalls administrable de la consola

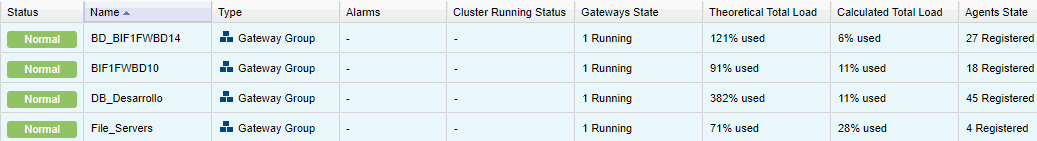
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Se puede observar lo siguiente.

* Los equipos se encuentran activos.
* El consumo de CPU en los Firewall es estable.
* Se visualiza que el estado de los Gateways en running sin errores.

* + - 1. Resumen de estado de los agentes en los Firewall



Se puede observar lo siguiente:

En el Firewall “BD\_BIF1FWBD14” se observan 25 agentes registrados sin problemas.

En el Firewall “BIF1FWBD10” se observan 18 agentes registrados sin problemas.

En el Firewall “DB\_Desarrollo” se observan 44 agentes registrados sin problemas.

En el Firewall “File\_ Servers” se observan 5 agentes registrados sin problemas.

Licencia



* + 1. **Tickets Asociado a la Plataforma**

|  |  |  |
| --- | --- | --- |
| **Ticket** | **Referencia** | **Comentario** |
| SOL272176 | Restauracion de archivo a identificar quien lo borro - Imperva DBF | se envio el reporte de los usuarios que realizaron la acción delete para la ruta tecnología |
| CAM70167 | BIFRECUPERA30 AGENTE RUNNING WITH ERRORS - ticket 99056 | se realizo el upgrade del agente a la version 14.4 con lo cual el problema de cipher no soportados fue superado |
| CAM70171 | RECUPERAR PASSWORD GATEWAY 10.200.100.214 - ticket 99060 | se reseteo el password del gw para poder acceder al equipo que estaba bloqueado,   luego del reseteo de credenciales se valida el acceso al gateway imperva |
| CAM70172 | DEPURAR ESPACIO DEL DISCO - ticket 99067 | se depuro políticas de auditoría para liberar el espacio del gateway, luego de lo cual el problema del poco espacio del gateway superado. |
| CAM70274 | INC 273958-ALERTA-ESPACIO EN DISCO-BAN-MEDIA | se depuro políticas de auditoría para liberar el espacio del gateway, luego de lo cual el problema del poco espacio del gateway superado. |
| CAM70275 | INC 273958-ALERTA-ESPACIO EN DISCO-BAN-MEDIA | se depuro políticas de auditoría para liberar el espacio del gateway, luego de lo cual el problema del poco espacio del gateway superado. |
| CAM70277 | Regla de Balanceo - Proyecto TI-EA2021-12164 TIN Inmediatas IPS- ticket 99097 | se valido que luego de configrar el automap en el virtual server el problema fue superado. |
| SOL279015 | RE: INC 278638-ALERTA-ESPACIO EN DISCO-BAN-MEDIA | se observa que el espacio de disco del equipo BANBIF - Imperva - DBF - Firewall BD Servidores Produccion destinado a Disco/var se encuentra dentro del umbral permitido, superando la alerta. Adicional a ello no se visualizan alarmas en el equipo |
| CAM72438 | revision bloqueo waf | En proceso |
| SOL285084 | Revisión Health Check Imperva BANBIF | Se envio el reporte de healcheck de los equipos imperva |
| SOL285089 | Reporte alertas Check Imperva BANBIF | se genero el reporte de alertas del imperva MX al equipo de BANBIF |
| SOL285136 | TEMAS IMPERVA | se realizo la transferencia de conocimiento a lizbeth Quispe |
| SOL285162 | Reportes IMPERVA | En proceso |
| CAM73765 | Asunto:ISSUE WITH AGENT BIF1REC22 - RUNNING WITH ERRORS | se actualizo el agente a la versión 14.4 y luego del upgrade el issue fue mitigado |
| CAM73766 | ISSUE WITH AGENT GENERICO-RUNNING WITH ERRORS | se actualizo el agente a la versión 14.4 y luego del upgrade el issue fue mitigado |
| CAM73960 | ALERT-SERVIDOR DESCONECTADO-BIF-MEDIA | se realizo la depuración del agente BIF1LYNC30 |
| CAM73961 | ALERT-SERVIDOR DESCONECTADO-BIF-MEDIA | se realizo la depuración del agenteBIF1MEYCOR30 |
| CAM73965 | ALERT-SERVIDOR DESCONECTADO-BIF-MEDIA | se realizo la depuración del agente , políticas y template |
| CAM74052 | INSTALACIÓN DE AGENTE IMPERVA | En proceso |
| CAM74053 | Actualización de agente imperva BIF1MARCA20 | En proceso |

* + 1. **Planeamiento**
    2. **Conclusiones**

Se valida que el espacio de disco en los Gateway es el adecuado por tal motivo no sé observan alertas relacionadas a alguno de los 4 Gateways.

* Se valida que el espacio de disco en los Gateway es el adecuado por tal motivo no sé observan alertas relacionadas a alguno de los 4 Gateways.
* Se valida el estado de los 4 gateways en estado running.
* Las licencias vencen el 09/03/2023
* Se tiene la versión 13.6.0.60 para los Gateways y MX.
* Se observa que se tienen alertas de ciphers no soportados.
* Se valida políticas sin uso para realizar la depuración, se solicitó aprobación.
* Se observa que se tienen 92 agentes enganchados a la consola MX.
  + 1. **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)**

**“Realizar el seguimiento respecto a la desactivación de los ciphers no soportados en el**

**Servidor, adicional a ello realizar el purgado de las políticas sin utilizar.”**

Se realizo el seguimiento para la realización de la desactivación del cipher no

soportado, el cual nos informaron que se encuentra en gestión y se realizará en el

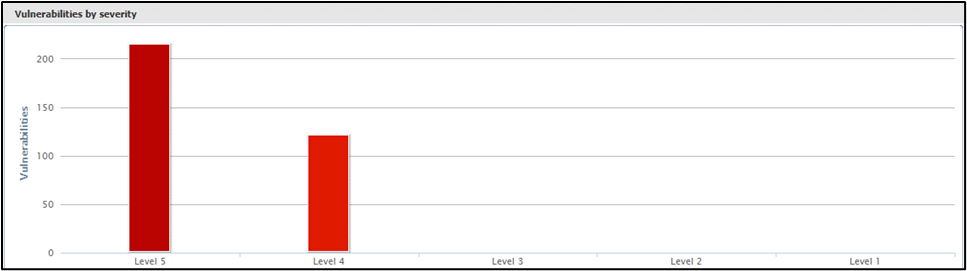
periodo en Febrero 2022 y se compartió la lista de políticas a depurar.

* + 1. **Recomendaciones**

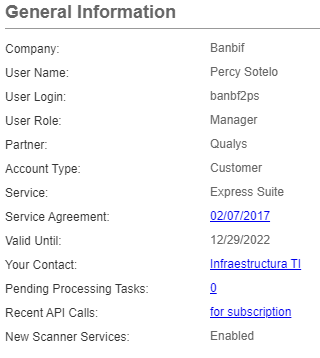
Realizar un afinamiento en la depuración de las políticas de auditoria periódicamente para evitar problemas conocidos por la cantidad de data el MX no puede procesar la data a recolectar y se generan de reportes en blanco.

Como también continuar con el monitoreo de la realización de la desactivación de cipher no soportados en el servidor.

* 1. **PLATAFORMA QUALYS**
     1. Vulnerabilidades por Severidad
* Se identificó vulnerabilidades de nivel de severidad 4 y 5.



* + 1. Licencias



* + 1. Tickets Asociados a la Plataforma

|  |  |  |
| --- | --- | --- |
| **Ticket** | **Referencia** | **Comentario** |
| SOL272083 | Reporte Mensual Qualys - ticket 98805 | para informar que se importó todos los reportes generados, mensuales de la consola Qualys a la ruta compartida. Correspondientes a mis tareas cada fin de mes. Nuevos reportes SICN solicitados: |
| SOL272096 | Reporte Mensual Qualys - ticket 98833 | se envio el informe mensual técnico Global de Vulnerabilidad. a jeniffer rojas |
| SOL275288 | QUALYS - ORDENAMIENTO DE REPORTES - ticket 99047 | se realizo el re-ordenamiento de todos los reportes mensuales de la carpeta compartida y se informo a jeniffer rojas, quien no solicito realizar la tarea de reordenar los reportes. |
| SOL276642 | SCANEO DE VULNERABILIDADES | se envio el reporte de los servidores 10.200.150.150 y 10.200.150.151, luego de realizar el scan en qualys, se compartio el detalle onsite de optical jesus peña herrera. |
| CAM73719 | NUEVOS Servidores Controladores de dominio 2019 PRD - AÑADIR ASSEST | se añadio los servidores al grupo Directorio Activo – LDAP\_PRD |
| CAM73721 | NUEVOS Servidores Controladores de dominio 2019 PRD - Plantilla reporte | se creo el template para la generación de reportes para el grupo Directorio Activo – LDAP\_PRD |
| CAM73730 | NUEVOS Servidores Controladores de dominio 2019 PRD - CREACIÓN DE GRUPO | se añadio los nuevos servidores al se creo al grupo Directorio Activo – LDAP\_PRD |
| CAM73757 | Depuración IPs - Qualys | se realizo la depuración de las 30 IPs del qualys brindadas por jeniffer rojas |
| CAM74055 | NUEVOS Servidores en ambiente Desarrollo - Añadir assest | En proceso |
| CAM74056 | NUEVOS Servidores en ambiente Desarrollo - Creación de template reportes | En proceso |

* + 1. **Conclusiones**

-La plataforma actualiza automáticamente las firmas y vulnerabilidades.

-Se tiene organizado todos los servicios del banco por Asset Group para cada ambiente

(Producción, Desarrollo y UAT).

-Las licencias vencen el 29/12/2022.

-Se valida que la consola Qualys presenta 1544 assest agregados.

-Se configuro el template de reportes autenticados respecto a vulnerabilidades de día cero.

* + 1. **Seguimiento de Actividades Referentes Al Anterior Mes (DICIEMBRE)**

**“Realizar el seguimiento del proyecto renovación tecnológica Qualys 2022, para así**

**Continuar con la ampliación de licencias y nuevos módulos.”**

Continuando con el seguimiento al proyecto Qualys, se mantiene en monitoreo debido

a que se encuentra en proceso de implementación y así adquirir más módulos y

licencias para añadir más servidores a la consola de Qualys.

* + 1. **Recomendaciones**

Continuando con el seguimiento al proyecto Qualys el cual se mantiene en

implementación.

* 1. **VPN**
     1. **VPN Securesoft-Banbif**



* + - El estado de la VNP se encuentra en UP.
    1. **VPN Americatel-Banbif**



El estado de la VNP se encuentra en UP.

* 1. **MONITOREO DE SEGURIDAD**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ticket** | **Fecha de Apertura** | **Referencia** | **Estado** | **Comentario** | **Producto** | **Prioridad** |
| INC276175 | 12/01/22 01:26 | INC 276175-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @pabrikapd.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio@pabrikapd.com a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC278822 | 17/01/22 04:33 | INC 278822-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @boomail.lavaweb.in los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @boomail.lavaweb.in a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC281406 | 21/01/22 02:24 | INC 281406-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @hanazza.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @hanazza.com a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC272431 | 04/01/22 21:20 | INC 272431-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @exact.com.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @exact.com.pe a nivel de AntiSpam (Previa autorización). CLIENTE: Por favor no bloquear, tenemos comunicación con el dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC275808 | 11/01/22 11:43 | INC 275808-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @zest.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @zest.pe a nivel de AntiSpam (Previa autorización). Cliente: Buenas noches, Por favor no bloquear, nos comunicamos con el dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC277737 | 14/01/22 13:13 | INC 277737-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @accenture.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @accenture.com a nivel de AntiSpam (Previa autorización). CLIENTE: Por favor no Bloquear, nos comunicamos con cuentas de correo de ese dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC277739 | 14/01/22 13:15 | INC 277739-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @deloitte.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @deloitte.com a nivel de AntiSpam (Previa autorización). CLIENTE: Por favor no bloquear, nos comunicamos con cuentas de correo del dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC279579 | 18/01/22 09:55 | INC 279579-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @sggestionfinanciera.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @sggestionfinanciera.com a nivel de AntiSpam (Previa autorización). Cliente: Buen día, Por favor no bloquear, nos comunicamos con los usuarios del dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC279584 | 18/01/22 10:00 | INC 279584-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @aset.com.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @aset.com.pe a nivel de AntiSpam (Previa autorización). Cliente: Buenas tardes, Por favor no bloquear, nos comunicamos con cuentas de correo de ese dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC280941 | 20/01/22 11:02 | INC 280941-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @contacto.com.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @contacto.com.pea nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC280945 | 20/01/22 11:06 | INC 280945-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @notariagalvez.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @notariagalvez.com a nivel de AntiSpam (Previa autorización). Cliente: Buenas tardes, Por favor no bloquear, nos comunicamos con cuentas de correos del dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC281607 | 21/01/22 11:08 | INC 281607-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @cgmrental.com.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @cgmrental.com.pea nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC281616 | 21/01/22 11:21 | INC 281616-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @cmail19.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @cmail19.com a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC283468 | 25/01/22 09:37 | INC 283468-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @notarianakasone.org los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @notarianakasone.org a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC277378 | 13/01/22 21:49 | INC 277378-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @srebanetools.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @srebanetools.com a nivel de AntiSpam (Previa autorización). CLIENTE: Proceder SOPORTE: la ing @Lilia Vasquez atenderá lo requerido bajo el/los ticket(s) [CAM71461] se realizó el bloqueo de la IOC malicioso AntiSpam | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC279373 | 17/01/22 21:38 | INC 279373-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @brandsmart.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @brandsmart.pe a nivel de AntiSpam (Previa autorización). CLIENTE: Buen día, Por favor no bloquear, nos comunicamos con los usuarios del dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC279381 | 17/01/22 21:57 | INC 279381-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Pendiente Cliente | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @truecpagroup.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @truecpagroup.com a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC280071 | 18/01/22 22:02 | INC 280071-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @enerlab.com.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @enerlab.com.pe a nivel de AntiSpam (Previa autorización). CLIENTE: Por favor no bloquear, nos comunicamos con los correos del dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC280075 | 18/01/22 22:17 | INC 280075-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @antut-advisors.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @antut-advisors.com a nivel de AntiSpam (Previa autorización). CLIENTE: Por favor no bloquear, nos comunicamos con las cuentas de correo del dominio. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC280711 | 19/01/22 22:17 | INC 280711-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @clubterrazasperu.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @clubterrazasperu.com a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC280716 | 19/01/22 22:29 | INC 280716-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @homesafetysac.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @homesafetysac.com a nivel de AntiSpam (Previa autorización). CLIENTE: Por favor no bloquear, nos comunicamos con correos electrónicos perteneciente al dominio indicado. | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC281297 | 20/01/22 20:54 | INC 281297-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @ddreciclaje.com los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @ddreciclaje.com a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC281301 | 20/01/22 21:12 | INC 281301-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @elpino.com.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @elpino.com.pe a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |
| INC281982 | 21/01/22 22:16 | INC 281982-EVENT-INGENIERÍA SOCIAL-BAN-BAJA | Cerrado | Durante nuestro monitoreo detectamos correos de publicidad provenientes del dominio @tierrasanta.org.pe los cuales debido a la cantidad se han catalogado como SPAM. Bloqueo del dominio @tierrasanta.org.pe a nivel de AntiSpam (Previa autorización). | CISCO-ANTISPAM-SMA-BANBIF | Media |

1. **CONCLUSIONES**

* Se observan los recursos de la consola de administración estables.
* Se observa los recursos estables del Antispam Standby – IBM .
* Se observa los recursos estables del Antispam San Isidro.
* Se observa los recursos estables de los balanceadores F5.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL DE CAMBIOS | | | | |
| Revisión | Hecha por | Aprobada por | Fecha | Motivo |
| 01 | ${Autor} | Supervisor CyberSOC | 3/2/2022 | Versión Inicial |

* Se valida que las VPNs con Americatel y Securesoft se encuentran en estado UP.