

**SECURESOFT CORPORATION**

**e-Secure Consulting Group**

**REPORTE DIARIO**

**Preparado para:**



**Fecha de elaboración:**

**${fecha\_dia\_antes}**

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

**INDICE**

1. [OBJETIVO 3](#_Toc89170480)
2. [ALCANCE 3](#_Toc89170481)
3. [ESTADO DE LAS PLATAFORMAS 3](#_Toc89170482)
4. [PLATAFORMA CISCO 3](#_Toc89170483)

[**1.1.Antispam Activo- San Isidro 3**](#_Toc89170484)

[**1.2.Antispam Standby – IBM 5**](#_Toc89170485)

1. [PLATAFORMA F5 6](#_Toc89170486)

[**2.1.Balanceador Interno Principal – Virtual 6**](#_Toc89170487)

[**2.2.Balanceador Interno Secundario – Virtual 8**](#_Toc89170488)

[**2.3.Balanceador Perímetro Principal - San Isidro 10**](#_Toc89170489)

[**2.4.Balanceador Perimetro Secundario – IBM 12**](#_Toc89170490)

[**2.5.Balanceador Standalone QA – Virtual 14**](#_Toc89170491)

1. [PLATAFORMA IMPERVA 16](#_Toc89170492)
2. [PLATAFORMA QUALYS 18](#_Toc89170493)
3. [VPN 18](#_Toc89170494)
4. [CONCLUSIONES 19](#_Toc89170495)
5. OBJETIVO

Este documento dará a conocer el estado de las plataformas de seguridad del cliente.

1. ALCANCE

Este documento presenta información sobre el consumo de recursos de los equipos administrados, así como el estado de su disponibilidad.

1. ESTADO DE LAS PLATAFORMAS

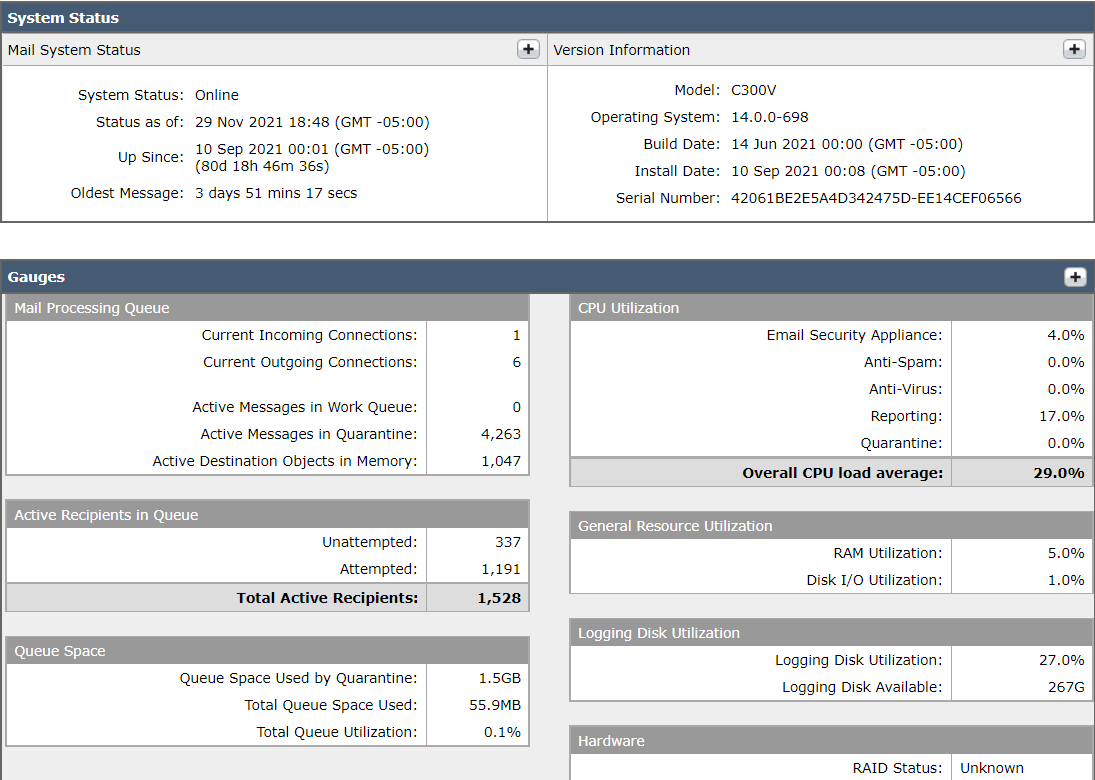
## PLATAFORMA CISCO

### Antispam Activo- San Isidro

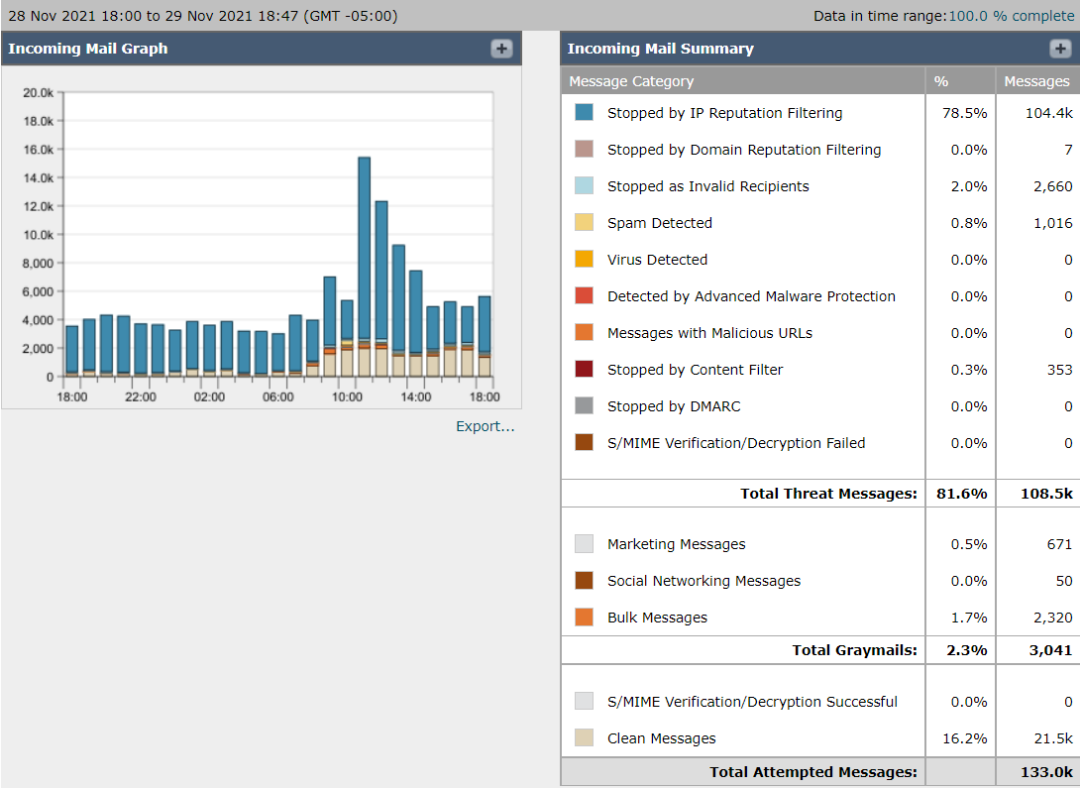
* **Recursos**

${graph2618}

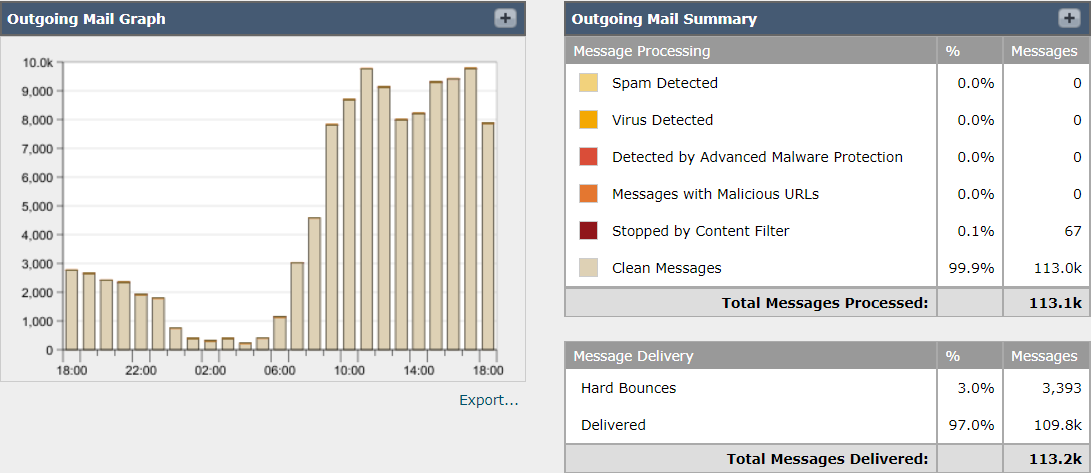
* *Se observó que el uso promedio de* ***CPU*** *es de 24.38%.*
* *Se observó que el uso promedio de* ***Disco*** *es de 23%.*
* *Se observó que el uso promedio de* ***Memoria*** *es de 24.78%.*
* **Estatus del sistema**



* **Correos entrantes**



* **Correos salientes**

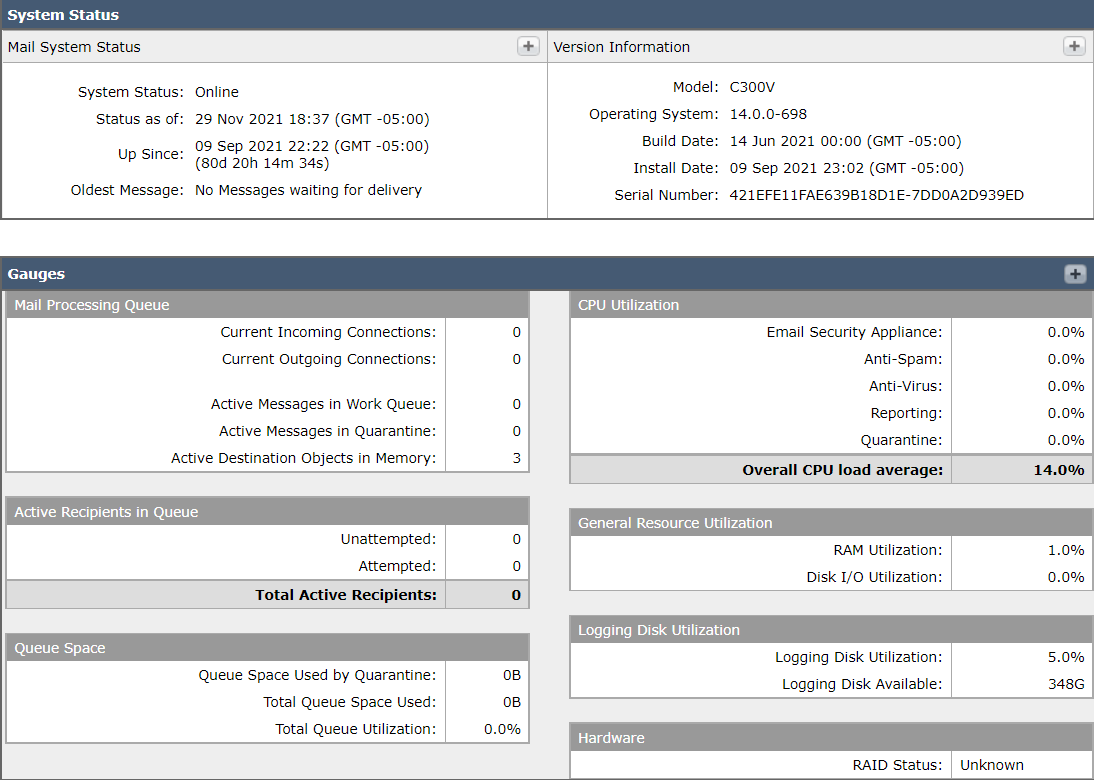


### Antispam Standby – IBM

* **Recursos**

${graph2622}

* *Se observó que el uso promedio de* ***CPU*** *es de 14.20%.*
* *Se observó que el uso promedio de* ***Disco*** *es de 4%.*
* *Se observó que el uso promedio de* ***Memoria*** *es de 1%.*
* **Estatus del sistema**



## PLATAFORMA F5

### Balanceador Interno Principal – Virtual

* **Estado del equipo**

${graph2638}

* *El estado de HA del Balanceador Interno Principal es* ***Activo (4)****.*
* **Recursos**

${graph2629}

* *Se observó que el uso promedio de* ***CPU*** *es de 18.32%.*
* *Se observó que el uso promedio de* ***Disco*** *es de 24%.*
* *Se observó que el uso promedio de* ***Memoria*** *es de 32.51%.*
* **Conexiones concurrentes**

${graph2631}

* **Throughput(bits)**

${graph2626}

### Balanceador Interno Secundario – Virtual

* **Estado del equipo**

${graph2657}

* *El estado de HA del Balanceador Interno Secundario es* ***ForceOffline (2)****.*
* **Recursos**

${graph2648}

* *Se observó que el uso promedio de* ***CPU*** *es de 11.85%.*
* *Se observó que el uso promedio de* ***Disco*** *es de 24%.*
* *Se observó que el uso promedio de* ***Memoria*** *es de 30%.*
* **Conexiones concurrentes**

${graph2650}

* **Throughput(bits)**

${graph2645}

### Balanceador Perímetro Principal - San Isidro

* **Estado del equipo**

${graph2676}

* *El estado de HA del Balanceador perímetro Principal es* ***Activo (4)****.*
* **Recursos**

${graph2667}

* *Se observó que el uso promedio de* ***CPU*** *es de 55.14%.*
* *Se observó que el uso promedio de* ***Disco*** *es de 23%.*
* *Se observó que el uso promedio de* ***Memoria*** *es de 15.02%.*
* **Conexiones concurrentes**

${graph2669}

* **Throughput(bits)**

${graph2664}

### Balanceador Perimetro Secundario – IBM

* **Estado del equipo**

${graph2695}

* *El estado de HA del Balanceador Perímetro Secundario es* ***ForceOffline (2).***
* **Recursos**

${graph2686}

* *Se observó que el uso promedio de* ***CPU*** *es de 19.56%.*
* *Se observó que el uso promedio de* ***Disco*** *es de 23%.*
* *Se observó que el uso promedio de* ***Memoria*** *es de 12%.*
* **Conexiones concurrentes**

${graph2688}

* **Throughput(bits)**

${graph2683}

### Balanceador Standalone QA – Virtual

* **Estado del equipo**

${graph2714}

* *El estado de HA del Balanceador Standalone QA es* ***Activo (4).***
* **Recursos**

${graph2705}

* *Se observó que el uso promedio de* ***CPU*** *es de 11.20%.*
* *Se observó que el uso promedio de* ***Disco*** *es de 24%.*
* *Se observó que el uso promedio de* ***Memoria*** *es de 18%.*
* **Conexiones concurrentes**

${graph2707}

* **Throughput(bits)**

${graph2702}

## PLATAFORMA IMPERVA

* **DBF (Consola de administración)**
* **CPU**

${graph2726}

* *Se observó que el uso promedio de* ***CPU*** *es de 16.17%.*
* **Conexiones**

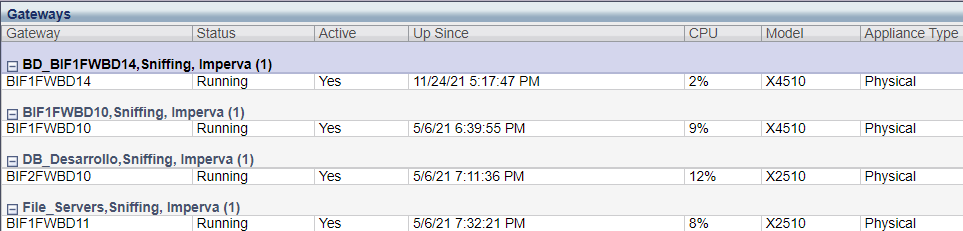
${graph2727}

* **Alertas por Severidad**

Gráfico, Gráfico de burbujas

Descripción generada automáticamente

* Se observan alertas por severidad: 1409 de tipo High, 516 de tipo Medium y 328 de tipo Informativo.
* **Estado de Firewalls y agentes**



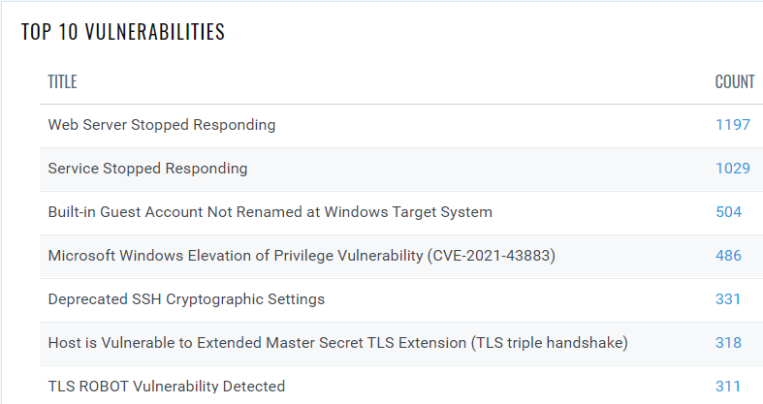
* *A continuación, se muestra el estado de los Firewall administrados por la consola:*
* *Los equipos se encuentran activos.*
* *El estatus de los equipos se encuentra “Funcionando”.*
* *El consumo de CPU en los Firewall es estable.*
* **Resumen del estado de los agentes en los Firewalls**



* *Se puede observar lo siguiente:*
* En el Firewall **“BIF1FWBD14”** se puede observan 25 agentes registrados sin problemas.
* En el Firewall **“BIF1FWBD10”** se observan 16 agentes registrados sin problemas.
* En el Firewall **“Desarrollo”** se puede observan 44 agentes registrados sin problemas.
* En el Firewall **“File Servers”** se observan 4 agentes registrados sin problemas.

## PLATAFORMA QUALYS

* **Top vulnerabilidades durante el día.**





* **Vulnerabilidades por severidad**

Gráfico, Gráfico de barras

Descripción generada automáticamente

* + - * Se identificó vulnerabilidades de nivel de severidad 4 y 5.

## VPN

* **VPN SECURESOFT – BANBIF**



* + - * Se valida el estado UP de la VPN
* **VPN AMERICATEL – BANBIF**



* + - * Se valida en estado UP de la VPN.

1. CONCLUSIONES

* Se observan los recursos de la consola de administración estables.
* En el Firewall **“BIF1FWBD14”** se puede observan 25 agentes registrados sin problemas.
* En el Firewall **“BIF1FWBD10”** se observan 16 agentes registrados sin problemas.
* En el Firewall **“Desarrollo”** se puede observan 44 agentes registrados sin problemas.
* En el Firewall **“File Servers”** se observan 5 agentes registrados sin problemas.
* 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.
* Se valida que las VPNs con Americatel y Securesoft se encuentran en estado UP.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CONTROL DE CAMBIOS** | | | | |
| **Revisión** | **Hecha por** | **Aprobada por** | **Fecha** | **Motivo** |
| 01 | ${autor} | Supervisor | ${fecha\_hoy} | Versión Inicial |