BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0346-2017-GTI230-N

ASUNTO : Informe técnico previo de evaluación de software - Adquisición de solución para gestión de identidades privilegiadas

---

1. NOMBRE DEL ÁREA:

Dpto. de Redes, Telecomunicaciones y Bases de Datos

2. RESPONSABLE DE LA EVALUACIÓN:

Jackes Matos Manguinuri

3. CARGO:

Especialista en Redes, Telecomunicaciones y Bases de datos

4. JUSTIFICACIÓN:

Entender los riesgos a los que nos enfrentamos permite conocer los controles necesarios que deben ser implementados para una efectiva gestión de identidades privilegiadas con lo cual lograríamos mantener una operación segura sin afectar las funcionalidades, accesos rápidos y flexibles que requieren los administradores de plataformas y evitar posibles sucesos como los acontecidos en el Banco de Bangladesh – 2016, según un informe emitido por la firma de seguridad Kaspersky Lab se indica que el grupo hacker *Lazarus* realizó uno de los robos cibernéticos más grandes registrados con una pérdida alrededor de 81 millones de dólares, brevemente se explica el ataque donde indica que los atacantes utilizaron privilegios de administrador en los sistemas para ejecutar remotamente un malware avanzado específico que se desarrolló a medida para ocultar pistas y atacar sistemas como la red SWIFT.

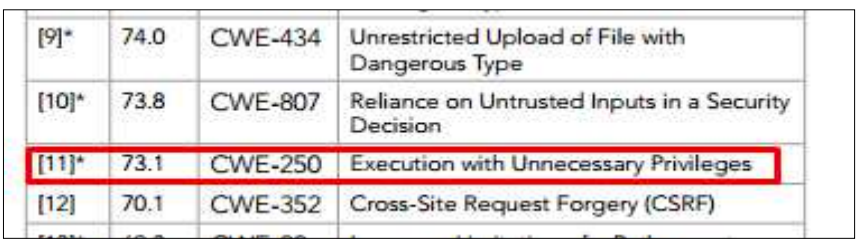
Bancos privados y Bancos centrales manejan cientos de identidades, cuentas y contraseñas privilegiadas; gestionarlas y actualizarlas manualmente es un proceso costoso, repetitivo y lento. Las cuentas administrativas y de aplicación se encuentran prácticamente en cualquier componente de hardware, software y aplicación incluyendo los entornos virtuales asimismo estas se comparten, lo que significa existe una vulnerabilidad en el que no se rastrea QUIÉN ha iniciado sesión como administrador, únicamente que se ha producido un inicio de sesión, lo que supone una importante dificultad para su auditoría, vulnerabilidad y riesgo porque afecta la continuidad operativa.

Los resultados de un estudio realizado han revelado algunos datos importantes sobre las contraseñas privilegiadas y los riesgos que representan.

¿Dónde existe la contraseña?	Ejemplos	¿Cuántas hay?*	¿Cuál es el riesgo para la seguridad?*	Soluciones
Estación de trabajo personal (Usuario Final)	Inicios de sesión: Administrador	El 40% de las empresas tienen más de 5000 trabajadores. En el caso del BCRP la cantidad es de 1200.	La trazabilidad del usuario administrador, dado que no se tiene un control granular de las actividades en los sistemas críticos.	Soluciones de contraseñas privilegiadas.
Servidores	UNIX (Root), LINUX (Root)	El 44% de las empresas tienen mas de 500 servidores, cada uno de ellos con 1-5 contraseñas administrativas.	La trazabilidad del usuario administrador, dado que no se tiene un control granular de las actividades en los sistemas críticos.	Soluciones de contraseñas privilegiadas.
Enrutadores	Cisco (Enable)	El 41% de las empresas tienen más de 500 servidores, cada uno de ellos con 1-5 contraseñas administrativas	La trazabilidad del usuario administrador, dado que no se tiene un control granular de las actividades en los sistemas críticos.	Soluciones de contraseñas privilegiadas.
Bases de Datos	Oracle (System, Sys), Microsoft SQL Server (SA)	El 66% de las empresas tienen más de 100 aplicaciones únicas, incluyendo bases de datos.	La trazabilidad del usuario administrador, dado que no se tiene un control granular de las actividades en los sistemas críticos.	Soluciones de contraseñas privilegiadas.
Scripts que conectan aplicaciones de software	Aplicación de seguimiento de ventas a base de datos principal.	Las empresas informan de que cuentan con más de 100 aplicaciones, con un 92% de ellas vinculadas al menos a otra aplicación. Cada vínculo único crea un incidente de contraseña único.	La trazabilidad del usuario administrador, dado que no se tiene un control granular de las actividades en los sistemas críticos.	Soluciones de contraseñas privilegiadas.

Actualmente el BCRP se enfrenta a enormes desafíos de seguridad que hacen mandatorio controlar y supervisar a sus usuarios privilegiados. Las cuentas de superusuario, como las de los administradores de bases de datos (DBAs), administradores de sistemas operativos (root, administrator), aplicaciones e infraestructura ha generado una ardua tarea de manejo de estas cuentas dado el número creciente de dispositivos y complejidad tecnológica que acarrean los mismos, lo que implica un alto riesgo a la manipulación de la información confidencial, daños malintencionados o compromisos en la red.

De acuerdo con CWE/SANS la ejecución de procesos con privilegios en el sistema está dentro de los errores más peligrosos y que no tienen control ni trazabilidad de lo que realizan.



[9]*	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]*	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]*	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)

Brief Listing of the Top 25 (muestra parcial de los errores más comunes)
Fuente: *2011 CWE/SANS Top 25 Most Dangerous Software Errors*

Para mitigar estas vulnerabilidades, existen soluciones que proporcionan un conjunto completo de controles para la protección y administración de todo tipo de credenciales a los recursos tecnológicos, se les conocen como gestión de identidades privilegiadas o privileged identity management en inglés**,** estas soluciones se adaptan a los diversos entornos operativos tecnológicos que posee el BCRP permitiéndole conseguir una mayor reducción en el riesgo y carga de trabajo operativa. Podemos mencionar los siguientes controles:

- Evitar el acceso no autorizado. Evitando que un usuario no autorizado (interno o externo) obtenga acceso al sistema (crítico) o puede detener un ataque incluso antes de que empiece. Una autenticación sólida es la mejor manera de proteger sus credenciales en esta etapa.

- Limitar el aumento de privilegios. Proporcionar controles de acceso granular en las sesiones de acceso de usuarios privilegiados, evitando la asignación de accesos elevados innecesarios y protegiéndolos contra exposición hacia atacantes o error humano, en este punto se puede mencionar el acceso remoto que se le brinda a proveedores o terceros con privilegios dentro de las plataformas tecnológicas para realizar configuraciones o tunning de los sistemas.

- Monitoreo, registro y auditoria de actividad. Ya sea se trate de un usuario interno de confianza que ingresó inadvertidamente a los recursos del área equivocada o de un atacante con intenciones maliciosas, cualquier eventos de este tipo debe ser grabado. El desafío entonces, es mejorar la visibilidad y el análisis en torno a la actividad de los usuarios en los sistemas confidenciales.

En la actualidad los bancos privados están adoptando el ciclo de vida de estas soluciones la cual es un marco de arquitectura de tecnología que consta de cuatro etapas continuas que se ejecutan bajo una plataforma automatizada central:

- Acceso a recursos privilegiados
- Control de los recursos privilegiados
- Seguimiento de las acciones emprendidas sobre recursos privilegiados
- Remediación para revertir los cambios realizados en los recursos de TI privilegiados a un buen estado conocido.

Controles & Reducción de Riesgos Asociados

	Reducción de Riesgo	Controles
PAM	• Eliminación de contraseñas estáticas & compartidas • Asociación del acceso a la cuenta privilegiada al usuario individual • Controles basados en politicas de acceso a información sensible • Camuflaje de Contraseñas para que no sean expuestas al usuario • Integración con autenticación fuerte • Auditoría detallada	• Privileged password management • Bóveda de Contraseñas • Acceso de Emergencia • Inicio de Sesiones • Auditoría y Reportes

Fuente: 2014 Securing Privileged Access Across Hybrid Enterprise - ISACA

El BCRP en los últimos años ha adquirido diferentes soluciones tecnológicas como equipos de seguridad informática, equipos de networking, comunicaciones unificadas,

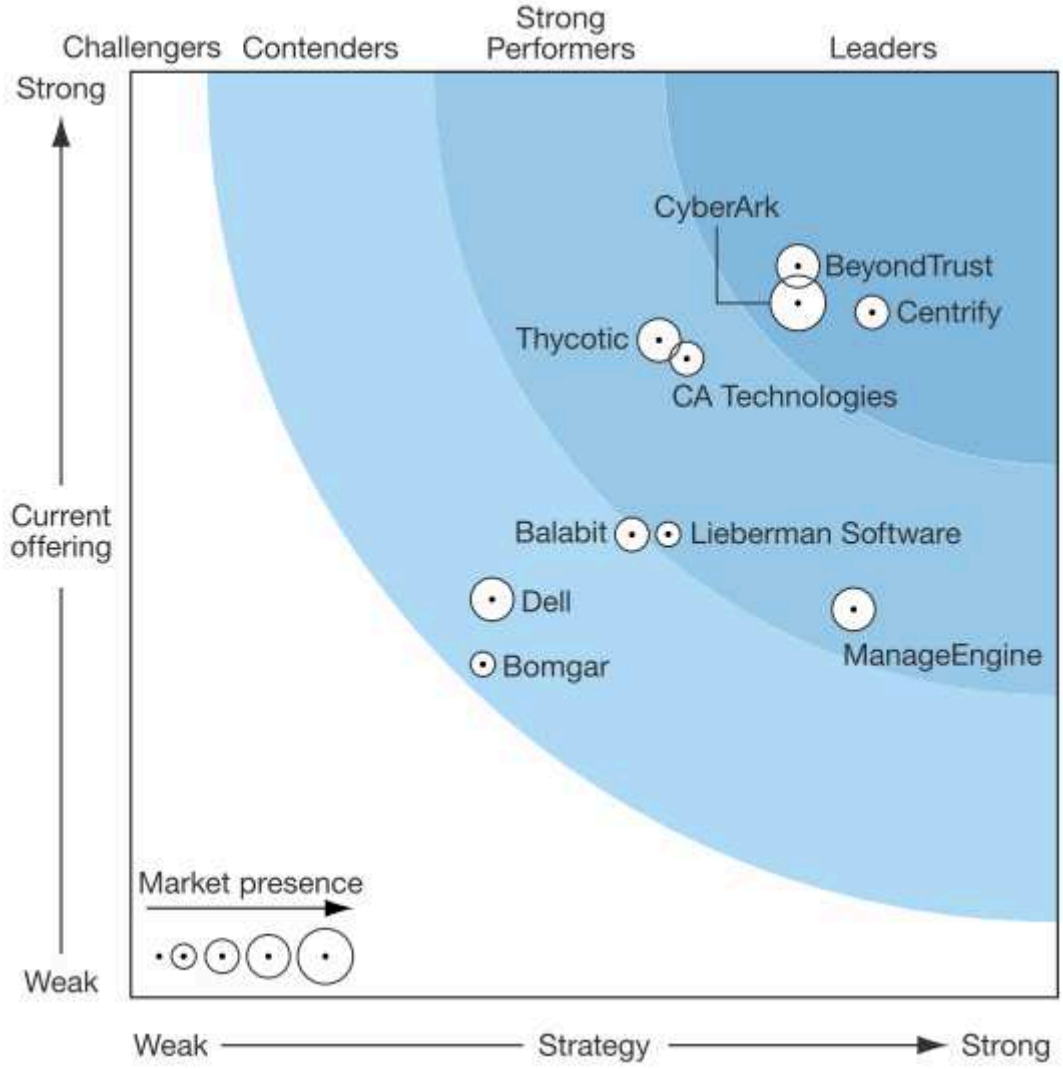
servidores departamentales y corporativos, almacenamiento y equipos que están soportados en la plataforma de virtualización los cuales garantizan la disponibilidad de los procesos y servicios del banco; estos mismos son administrados por los especialistas de los departamentos encargados de estas soluciones, ellos en su tarea diaria ingresan a estos equipos con usuarios que vienen de manera nativa y/o con altos privilegios (root, admin, administrator, etc.), esto representa riesgos informáticos que podrían afectar la continuidad operativa del BCRP, asimismo el soporte de las empresas proveedoras a través de los accesos remotos tienen la misma problemática.

De lo mencionado anteriormente podemos agregar que dentro del procedimiento 005-2014-GTI200-N (GESTIÓN DE INCIDENTES DE SERVICIOS TI CRÍTICOS) se encuentra la relación de servicios que tienen nivel de alta criticidad para el BCRP y en los cuales debemos implementar las medidas y controles necesarios que garanticen la continuidad operativa dichos servicios y minimizar sus vulnerabilidades tanto en su acceso como en su control.

Relación de Servicios TI Críticos

N°	Servicio	Descripción	Nivel de Criticidad
1	Servicio de Información del Entorno (*)	Internet	Alto
2	Servicio de Comunicaciones Digitales (*)	Servicios Telefónicos (Central & Celulares)	Alto
		Correo electrónico	Alto
		Fax	Alto
3	Servicios de consulta y transmisión de Información Financiera (*)	Bloomberg	Alto
		Reuters	Alto
		Datatec	Alto
		Swift	Alto
4	Servicio de Información Institucional	Portal BCRP	Alto
5	Servicio de Información de Operaciones Internacionales	Wilshire	Alto
		Nicelog	Alto
		BIS	Alto
		Trade Thru	Alto
6	Servicio de Base Estadística Financiera	SBEF	Alto
7	Servicio de Información LBTR		Alto
8	Aladi		Alto
9	Servicio de Información Contable		Medio
10	Servicio de Información de la Cámara de Compensación Electrónica		Medio
11	Servicio de Información de los Instrumentos Monetarios Cambiarios	SIMC	Medio
12	Servicio de Información de Administración de Circulante	SAC	Medio
13	Servicio de Información de Estudios Económicos	FAME	Bajo
14	Servicio de Información Administrativa - INSAD		Bajo
15	Servicio de Gestión de Archivos	Respaldo de Información de Servidores Departamentales de Estudios Económicos, Operaciones Internacionales y Estabilidad Financiera (Disco H)	Bajo

Como medida para minimizar estas latentes vulnerabilidades en la administración de estas cuentas en la infraestructura TI critica estamos evaluando soluciones de gestión de identidades privilegiadas en donde encontramos varios fabricantes que cumplen con proveer esta tecnología pero hay factores que los diferencian y que los vuelven más idóneo para las necesidades del BCRP.



Fuente: Forrester Wave™: Privileged Identity Management, Q3 '16

Cabe mencionar que estas soluciones se alinean a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 y la Política General de Seguridad de la Información del BCRP donde expresamente se indica en el *dominio 4: Control de accesos* en los puntos 12, 13,14 sobre la definición de acceso a los servicios TI críticos que contengan información sensible y crítica para el BCRP.

VIII. DOMINIO 4: CONTROL DE ACCESOS

12. Las gerencias propietarias de los activos de información, deberán realizar las siguientes acciones relacionadas con el control de acceso a sus servicios TI:
    a) Definir los perfiles de los usuarios para controlar el nivel de acceso a la información.
    b) Administrar los niveles de acceso a la información y mantenerse informado sobre el estado de las actualizaciones vigentes.
    c) Designar al personal encargado de la administración de los accesos.
    d) Mantener vigente la relación del personal autorizado así como revisar periódicamente las bitácoras de acceso.
    e) Identificar a los usuarios autorizados para acceder a la información catalogada como clasificada.

13. La Gerencia de Tecnologías de Información definirá, controlará y mantendrá actualizados los perfiles y accesos de los administradores técnicos a los activos de información tecnológicos.

14. El personal y terceros usuarios de servicios TI deberán:
    a) Cambiar las contraseñas en el periodo de vigencia establecido.
    b) Generar contraseñas cuya longitud no sea menor a 8 caracteres y contenga una combinación de caracteres numéricos, alfabéticos y especiales imprimibles.
    c) Evitar la escritura de las contraseñas en papeles, notas o archivos compartidos así como su almacenamiento en formato legible en archivos a los que puedan acceder terceros.
    d) Acceder a los servicios TI en los periodos u horarios establecidos.

5. ALTERNATIVAS:

En el mercado local se han encontrado los siguientes marcas: CyberArk, CA, BeyondTrust.

6. ANÁLISIS COMPARATIVO TÉCNICO:

Características Claves	CA	Cyberark	BeyondTrust
Despliegue flexible basado en Appliance	Si	No - requiere adquirir hardware y software para soportar su despliegue.	Si – virtual o físico
Control granular basado en host	Si - Solución robusta basada en host para Unix, Linux y Windows.	Módulos Separados: Sudo en Unix/Linux vía OPM y Windows	Si - Unix, Linux, Sudo y Windows

		vía Viewfinity.	
Bridge para Active Directory	Si	Si	Si
Alta disponibilidad embebida	Si - activo/activo con balanceo de carga nativo.	Parcial - activo/pasivo	Si – activo/activo
Multitenancy	Si	Si	Si
Analítica Amenazas	Si	Si	No
Gestión de SSH keys	Si	Si	Si

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Control de acceso a los dispositivos gestionados con inicio de Sesión Automático.
- Control de acceso a los dispositivos gestionados con aplicaciones cliente utilizadas por BCRP.
- Control de acceso a los dispositivos gestionados – Inicio de sesión automático con aprobación.
- Gestión de cuentas privilegiadas – Aplicación de políticas.
- Control de acceso a los dispositivos gestionados - Filtro de comandos.
- Grabación de sesiones.

Costos:

Prestación principal

- Plataforma, basada en appliance(s) virtual(es) y/o físicos incluyendo todo el licenciamiento requerido para su operación.
- Suscripciones de los servicios de mantenimiento de software y soporte técnico (escalamiento) del fabricante.

Prestación accesoria

- Servicio de mesa de ayuda y soporte técnico local 24 x 7.
- Servicio de mantenimiento técnico preventivo.
- Capacitación y/o workshop.

En lo que respecta a los costos asociados, se ha recibido una cotización referencial por S/ 450 000,00 incluido IGV.

8. CONCLUSIONES:

Considerando la importancia de contar con las protecciones mencionadas, se recomienda la adquisición solución de gestión de identidades privilegiadas por el periodo de tres (03) años contabilizados a partir de la firma del acta de conformidad de implementación de la solución.

Lima, 28 de diciembre de 2017

cc. Subgerencia de Logística - César Oscar Delizzia Infante

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Jackes Taylor MATOS MANGUINURI
Especialista en Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

Miguel Angel TEJADA MALASPINA
Subgerente de Servicios de Tecnologías de Información
Subgerencia de Servicios de Tecnologías de Información

Felipe Ernesto ROEL MONTELLANOS
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

Javier Ernesto OLIVERA VEGA
Gerente Central de Administración
Gerencia Central de Administración

Renzo Guillermo ROSSINI MIÑAN
Gerente General
Gerencia General

VISADO POR: