Cargo: Consultor en Monitoreo de Ciberseguridad

Objetivo de la consultoría

Implementar medidas para garantizar la detección temprana, clasificación y escalamiento de eventos de seguridad informática mediante el monitoreo continuo de los sistemas corporativos, así como apoyar en la gestión de vulnerabilidades para reducir riesgos cibernéticos y proteger la información institucional.

Funciones principales

- **Monitoreo constante** de alertas en plataformas de seguridad (SIEM, EDR, IDS/IPS, firewalls, DLP).
- **Clasificación inicial de eventos** de seguridad, diferenciando falsos positivos de incidentes reales.
- **Escalamiento oportuno** de incidentes a niveles superiores
- **Gestión de vulnerabilidades**:
    - Participar en la identificación de vulnerabilidades en sistemas, aplicaciones y dispositivos.
    - Apoyar en la priorización de riesgos según criticidad.
    - Coordinar con áreas técnicas para la remediación y seguimiento de vulnerabilidades detectadas.
- **Documentación de hallazgos** y elaboración de reportes básicos de incidentes y vulnerabilidades.
- **Soporte en la operación diaria del SOC**, incluyendo la atención de tickets y coordinación con otras áreas de TI.
- **Cumplimiento normativo**: aplicar políticas internas de seguridad y alinearse con estándares regulatorios (ASFI, ISO/IEC 27001).
- **Colaboración interáreas**: trabajar con equipos de infraestructura, redes y seguridad para asegurar la continuidad operativa.

Perfil requerido

- Formación en **Ingeniería de Sistemas, Informática o carreras afines**.
- Conocimientos básicos en ciberseguridad, redes y sistemas operativos.
- Experiencia en uso de herramientas de monitoreo de seguridad (SIEM, antivirus corporativo, firewalls).
- Familiaridad con procesos de **gestión de vulnerabilidades** (escaneo, clasificación, remediación).
- Capacidad de análisis, atención al detalle y trabajo bajo presión.
- Deseable certificación inicial en seguridad

Responsabilidades del Consultor en Monitoreo de Ciberseguridad

- **Supervisión avanzada de alertas** en plataformas de seguridad (**SIEM, EDR, IDS/IPS, firewalls, DLP, MDM**), garantizando la detección temprana de amenazas y anomalías que puedan comprometer la infraestructura tecnológica del BDP.

- **Clasificación y análisis de eventos de seguridad**, diferenciando falsos positivos de incidentes reales, aplicando criterios de riesgo y criticidad para optimizar la capacidad de respuesta del SOC.
- **Escalamiento oportuno y documentado de incidentes** hacia niveles superiores del SOC, asegurando una gestión eficiente y coordinada de incidentes críticos.
- **Gestión integral de vulnerabilidades**:
    - Identificación proactiva en sistemas, aplicaciones y dispositivos.
    - Análisis y priorización de riesgos según impacto operativo y estratégico.
    - Coordinación con áreas técnicas para la remediación, seguimiento y verificación de cierre de vulnerabilidades.
- **Supervisión del control de navegación y uso de recursos tecnológicos**, aplicando políticas internas para prevenir accesos indebidos y garantizar el cumplimiento normativo.
- **Monitoreo de infraestructura tecnológica crítica** (servidores, redes, aplicaciones y dispositivos móviles), asegurando disponibilidad, continuidad y resiliencia frente a incidentes.
- **Documentación exhaustiva de hallazgos** y elaboración de reportes técnicos de incidentes, vulnerabilidades y métricas de seguridad, aportando insumos estratégicos para la toma de decisiones.
- **Apoyo en la operación diaria del SOC**, atendiendo tickets, gestionando incidentes y coordinando con otras áreas de TI para asegurar la continuidad operativa.
- **Cumplimiento normativo y regulatorio**, aplicando políticas internas y alineando las operaciones con estándares nacionales e internacionales (**ASFI, ISO/IEC 27001, mejores prácticas de ciberseguridad**).
- **Colaboración interáreas**, trabajando de manera conjunta con equipos de infraestructura, redes, seguridad y gestión de riesgos para fortalecer la postura de seguridad institucional.
- **Acompañar la implementación y operación de nuevas soluciones de seguridad previstas para la gestión 2026**, como **MDM Kaspersky**, **DLP** y otras herramientas complementarias, asegurando su integración efectiva en la estrategia global de ciberseguridad.

Requisitos del Consultor en Monitoreo de Ciberseguridad

Formación Académica

- Título universitario en **Ingeniería de Sistemas, Informática, Telecomunicaciones o carreras afines**.
- Deseable contar con **especializaciones** en **Ciberseguridad, Seguridad de la Información o Gestión de Riesgos Tecnológicos**.

Experiencia Laboral

- Experiencia mínima de **3 años en áreas de seguridad informática o administración de infraestructura tecnológica**.
- Experiencia comprobada en la operación de **SOC (Security Operations Center)**.
- Conocimiento demostrable y manejo de plataformas de seguridad como **SIEM, EDR, IDS/IPS, firewalls, DLP y MDM**.

- Experiencia en **gestión de vulnerabilidades**, análisis de riesgos y coordinación de remediaciones técnicas.

Conocimientos Técnicos

- Conocimiento de herramientas de monitoreo y correlación de eventos (**SIEM**).
- Conocimiento en soluciones de protección de endpoints (**EDR**) y prevención de fuga de información (**DLP**).
- Conocimiento en administración de dispositivos móviles mediante **MDM** u otras soluciones similares.
- Conocimientos en **protocolos de red, infraestructura tecnológica, sistemas operativos (Windows/Linux)** y aplicaciones críticas.
- Familiaridad con estándares y normativas de seguridad (**ISO/IEC 27001, ASFI, NIST**).

Competencias

- **Capacidad analítica y de resolución de problemas**, con enfoque en la detección temprana de amenazas.
- **Trabajo en equipo y colaboración interáreas**, especialmente con infraestructura, redes y gestión de riesgos.
- **Comunicación efectiva**, tanto para la elaboración de reportes técnicos como para la coordinación con áreas estratégicas.
- **Orientación a resultados**, asegurando la continuidad operativa y el cumplimiento normativo.
- **Adaptabilidad y aprendizaje continuo**, frente a nuevas amenazas y tecnologías emergentes.

Plazo

La consultoría tendrá una duración de doce (12) meses a partir de la firma del contrato en el horario de 09:00 a 17:30.

Monto y forma de Pago

El monto total de la **consultoría a nivel técnico** será de 66.000 Bs, (Sesenta y seis mil bolivianos), pagaderos en 12 cuotas mensuales de 5,500 Bs. Los pagos se realizarán previa aprobación del informe mensual del consultor

Planificación Anual – Consultor de Monitoreo de Ciberseguridad

Durante la consultoría se desarrollarán actividades de manera continua, con énfasis en el **monitoreo de alertas, gestión de vulnerabilidades, control de navegación y elaboración de informes periódicos** de las soluciones de seguridad implementadas (MDM, EDR, Control de Navegación y SIEM).

Primer mes

- Escaneo inicial de vulnerabilidades, se elaborará el informe base de estado de seguridad y se coordinará con el área de TI el plan anual de parches.
- Se iniciará el monitoreo diario de alertas y el seguimiento a las vulnerabilidades detectadas, complementado con el primer informe mensual de seguridad.

Segundo mes

- Actividad de monitoreo constante, verificación y validación de remediaciones a vulnerabilidades críticas.
- Capacitación interna sobre políticas y procedimientos de la JNIP.
- Emisión de informe mensual consolidando los hallazgos de MDM, EDR y Control de Navegación.

Tercer mes,

- Primer escaneo **trimestral de vulnerabilidades a sistemas críticos**, acompañado de la revisión del inventario de dispositivos y la elaboración de un informe de cumplimiento normativo.
- Se dará seguimiento a las vulnerabilidades detectadas en dichos escaneos y se emitirá el informe mensual correspondiente.

Cuarto mes

- Estarán orientados al monitoreo diario y continuo, la validación de parches aplicados y la ejecución de escaneos específicos en aplicaciones críticas.

Quinto mes

- Se elaborarán informes de hallazgos y planes de remediación, además de los reportes mensuales de seguridad.

Sexto mes,

- Segundo **escaneo trimestral de vulnerabilidades a sistemas críticos**, junto con la coordinación con áreas de infraestructura.
- Se emitirá un informe semestral consolidado que integrará los resultados de los primeros seis meses, además del informe mensual.

Séptimo mes

- Monitoreo constante, escaneos en endpoints y validación de remediaciones.
- Se emitirán los informes mensuales.

Octavo mes

- Seguimiento de vulnerabilidades.
- Se emitirán los informes mensuales.

Noveno mes

- Tercer **escaneo trimestral de vulnerabilidades a sistemas críticos**, acompañado de la revisión de políticas, procedimientos y la elaboración de un informe de cumplimiento normativo.
- Se dará seguimiento a las vulnerabilidades detectadas y se emitirá el informe mensual.

Décimo mes

- Se emitirá el informe mensual consolidando los hallazgos de todas las soluciones implementadas para la subsanación de vulnerabilidades.

Decimo primer mes

- Escaneo de vulnerabilidades en servidores críticos, junto con la revisión y el seguimiento de vulnerabilidades en proceso.
- Se emitirá el informe mensual.

Decimo primer mes

- Cuarto escaneo **trimestral de vulnerabilidades a sistemas críticos**, el cierre y consolidación de vulnerabilidades detectadas durante el año y la elaboración del **informe anual consolidado**, que integrará los resultados de los informes mensuales y trimestrales, proporcionando una visión completa del estado de la seguridad institucional.

Entregables

- Reportes mensuales de eventos tecnológicos
- Reportes Mensuales de vulnerabilidades.
- Informes trimestrales de escaneo de vulnerabilidades y seguimiento a remediación de hallazgos.
- Informes mensuales de progreso y resultados obtenidos.
- Informe anual consolidado, que integrará los resultados de los informes mensuales y trimestrales.

Nota: Para poder postularse al cargo deben enviar sus Curriculum al siguiente correo:

bdpsam.proveedor@gmail.com