**L-3**

Entidad XXXXXXX

Auditoría de Procesos

Del 01 de Enero al 31 de Diciembre de 2024

**Mapa prioritario de procesos, riesgos y controles**

**Area Tecnología de Información**

### ****1. Procesos Clave y Riesgos Asociados****

| **Proceso** | **Riesgo Clave** | **Impacto** | **Probabilidad** | **Descripción del Impacto** |
| --- | --- | --- | --- | --- |
| Gestión de Tickets de Soporte | Información incompleta o incorrecta en tickets. | Alto | Media | Retrasos en la solución de incidentes y aumento de reclamos de los usuarios. |
| Validación de Actualizaciones | Aplicación de actualizaciones sin pruebas suficientes. | Muy Alto | Media | Fallos en sistemas críticos que afectan la operación de la organización. |
| Gestión de Accesos y Permisos | Permisos no actualizados o excesivos. | Muy Alto | Media | Brechas de seguridad que pueden permitir accesos no autorizados. |
| Mantenimiento de Infraestructura | Falta de monitoreo de equipos clave. | Alto | Media | Fallas en servidores o redes que afectan la continuidad operativa. |
| Gestión de Incidentes de Seguridad | Respuesta tardía a incidentes de ciberseguridad. | Muy Alto | Alta | Pérdida de datos sensibles o interrupciones operativas prolongadas. |

### ****2. Controles Implementados y Eficiencia****

| **Proceso** | **Control Actual** | **Eficiencia del Control** | **Observaciones** |
| --- | --- | --- | --- |
| Gestión de Tickets de Soporte | Revisión manual de tickets al ser ingresados en el sistema. | Media | Dependencia de procesos manuales aumenta el riesgo de errores humanos. |
| Validación de Actualizaciones | Pruebas previas en un entorno de pruebas antes de implementación. | Alta | Efectivo, pero falta documentación de resultados en algunos casos. |
| Gestión de Accesos y Permisos | Revisión trimestral de accesos y roles asignados. | Alta | Proceso estructurado, pero dependiente de actualizaciones manuales. |
| Mantenimiento de Infraestructura | Monitoreo continuo a través de herramientas como Zabbix. | Alta | Sistema eficiente, pero falta de alertas personalizadas en algunos equipos clave. |
| Gestión de Incidentes de Seguridad | Plan de respuesta definido y monitoreo con un SIEM (Security Information and Event Management). | Media | Faltan simulacros periódicos para evaluar la efectividad del plan de respuesta. |

### ****3. Priorización de Riesgos****

| **Riesgo Clave** | **Prioridad** | **Razonamiento** |
| --- | --- | --- |
| Respuesta tardía a incidentes de ciberseguridad | Muy Alta | Puede generar impactos críticos en la operación y reputación de la organización. |
| Permisos no actualizados o excesivos | Muy Alta | Riesgo significativo de brechas de seguridad y accesos indebidos a sistemas críticos. |
| Aplicación de actualizaciones sin pruebas | Alta | Riesgo de interrupción operativa debido a fallos en sistemas críticos tras actualizaciones mal ejecutadas. |
| Información incompleta o incorrecta en tickets | Alta | Genera ineficiencia y demoras en la resolución de problemas reportados por los usuarios. |
| Falta de monitoreo de equipos clave | Media | Puede ocasionar fallas en la infraestructura que afecten la continuidad operativa de forma parcial. |

### ****4. Acciones de Mejora****

| **Proceso** | **Acción Propuesta** | **Impacto Esperado** |
| --- | --- | --- |
| Gestión de Tickets de Soporte | Implementar validaciones obligatorias al registrar tickets. | Reducción de errores y mayor rapidez en la resolución de incidentes. |
| Validación de Actualizaciones | Documentar todas las pruebas y automatizar parte del proceso de validación. | Reducción de riesgos operativos y mayor trazabilidad. |
| Gestión de Accesos y Permisos | Automatizar la revisión trimestral de permisos mediante un sistema IAM (Identity and Access Management). | Menor riesgo de accesos indebidos y mejora en el cumplimiento de normativas. |
| Mantenimiento de Infraestructura | Configurar alertas avanzadas para detectar fallas en equipos críticos. | Mayor continuidad operativa y detección temprana de problemas. |
| Gestión de Incidentes de Seguridad | Realizar simulacros periódicos de respuesta a incidentes. | Mejor preparación del equipo ante incidentes reales y reducción del impacto de los mismos. |

### ****Conclusión:****

Este mapa prioritario destaca los riesgos más críticos en el área de Tecnología de Información, proponiendo mejoras específicas para reforzar los controles internos y aumentar la eficiencia operativa. La implementación de estas acciones reducirá significativamente los riesgos asociados y mejorará la gestión del área.

Firma

Auditor

Fecha