|  |  |  |
| --- | --- | --- |
| LOGO | **REPORTE DE HALLAZGOS** | **REGISTRO**  **R-AUD-REP-03**  14-10-2024 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **AUDITOR** | **FECHA** | | **NOMBRE DE EMPRESA AUDITADA Y SITIOS:** | | | | | **Auditoría N°** | | | | **Reporte N°** |
| 14/10/2024 | |  | | | | |  | | | |  |
| **NO CONFORMIDAD / OBSERVACIÓN** | | | | | | | | | | | |
| Acceso no controlado a áreas sensibles de la organización.  Se ha observado que las áreas sensibles, como Recursos Humanos y los servidores dentro de la empresa, carecen de controles de acceso adecuados, permitiendo que cualquier persona que ingrese a la sede pueda acceder a estas zonas sin restricciones. Esto representa un riesgo significativo para la confidencialidad de la información y la seguridad física de la organización. | | | | | | | | | | | |
| **DESCRIPCION EVIDENCIA OBJETIVA** | | | | | | | | | | | |
| Se revisaron los registros de acceso y se encontró que las puertas de entrada a las áreas sensibles, como Recursos Humanos y los servidores en la empresa, no cuentan con sistemas de control de acceso adecuados, tales como tarjetas magnéticas o sistemas biométricos. Esta falta de controles representa un riesgo significativo para la seguridad de los activos e información crítica de la organización. Durante la visita a las instalaciones, se constató que varias personas ajenas a la organización se encontraban en las cercanías de Recursos Humanos sin supervisión ni control, lo que evidencia un fallo en la implementación de medidas de seguridad física. Además, en entrevistas realizadas al personal, se reportó que no existe una política clara sobre el control de acceso a estas áreas sensibles, lo que ha agravado la situación debido a la falta de actualización de los descriptores de cargo y roles. | | | | | | | | | | | |
| **DESCRIPCION DEL REQUISITO NORMATIVO** | | | | | | | | | | | |
| Según la norma ISO 27001:2013, las organizaciones deben implementar controles de acceso físico que protejan las áreas sensibles y los activos críticos, garantizando que solo el personal autorizado pueda acceder a estas zonas. Específicamente, el control A.11.1 de la norma establece la necesidad de restringir el acceso a las instalaciones mediante mecanismos como tarjetas magnéticas, sistemas biométricos, o registros formales, así como la obligación de mantener un registro detallado de todos los accesos. Además, se requiere que las organizaciones implementen barreras físicas y procedimientos de seguridad perimetral para evitar el acceso no autorizado a las instalaciones. | | | | | | | | | | | |
| **CLASIFICACION** | | | **AUDITOR LIDER** | | **AUDITOR** | | | | **REPRESENTANTE AUDITADO** | | |
| **MAYOR** | **MENOR** | | Jesus Castillo | | Osvaldo Herrera | | | | Jefe de Guardias | | |
| X |  | |
| **DEBE SER COMPLETADO ANTES DE** | | | | | **7/11/2024** | | | | | | |
| **AUDITADO** | **ANÁLISIS DE CAUSA RAÍZ [ Describir cuál fue la causa que originó este hallazgo ]** | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **ACCION INMEDIATA y CORRECCIÓN CAUSA RAÍZ**  **[ Describir qué hacer para corregir el problema informado y evitar su recurrencia ]** | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **VERIFICACION**  **DE**  **ACCIONES CORRECTIVAS** | | | | **FECHA DE TÉRMINO** | | | |  | | | |
| **REPRESENTANTE AUDITADO** | | | |  | | | |
|  | **FECHA** | | **ESTADO** | | | | **AUDITOR** | |
|  | |  | | | |  | |
| **COMENTARIOS AUDITOR** | | | |  | | | | | | | |