|  |  |
| --- | --- |
| Auditoría Interna Nº | 1 |
| Fecha de inicio | 19 – Agosto – 2024 |
| Fecha de término | 18 – Octubre – 2024 |
| Lugar de ejecución | Av. Pedro de Valdivia 641, Providencia, Santiago, Chile |
| Hora de inicio | 09:00 |
| Hora de término | 17:00 |

**Objetivos de la Auditoría**

|  |
| --- |
| Evaluar la efectividad de los controles de acceso físico y la gestión de incidentes de seguridad en el datacenter de Quilicura y las oficinas de la empresa, con el fin de garantizar la protección de los activos críticos y cumplir con los requisitos de la norma ISO 27001.  **Evaluar la Eficacia de los Controles de Acceso Físico:**   * **Verificar la implementación y adecuación de los controles de acceso físico** en el datacenter de Quilicura y en las oficinas de la empresa, asegurando que solo el personal autorizado tenga acceso a áreas sensibles. * **Determinar si los controles existentes cumplen con los requisitos de la norma ISO 27001** en relación con la protección de la infraestructura física y los activos críticos de la empresa. * **Evaluar la adecuación de los dispositivos de seguridad física**, como cámaras, cerraduras electrónicas, y sistemas de autenticación, asegurando que funcionen correctamente y sean suficientes para mitigar riesgos.   **Revisar la Gestión de Incidentes de Seguridad:**   * **Analizar los procedimientos actuales de gestión de incidentes de seguridad**, verificando que estén claramente definidos y alineados con las mejores prácticas establecidas por la ISO 27001. * **Evaluar la capacidad de respuesta del personal ante incidentes de seguridad mediante simulaciones o revisión de incidentes pasados, asegurando que las lecciones aprendidas se apliquen efectivamente.** * **Verificar que los roles y responsabilidades en la gestión de incidentes estén claramente definidos** y que el personal involucrado esté debidamente capacitado para manejar situaciones de crisis.   **Identificar Áreas de No Conformidad y Oportunidades de Mejora:**   * **Detectar cualquier no conformidad en la implementación de los controles de acceso físico** y la gestión de incidentes de seguridad, recomendando medidas correctivas para cerrar las brechas identificadas. * **Proporcionar recomendaciones para fortalecer la seguridad física y la gestión de incidentes**, contribuyendo a la mejora continua del sistema de gestión de seguridad de la información de la empresa. |

**Alcance de la Auditoría**

|  |
| --- |
| La auditoría se centrará en la revisión y evaluación de los controles de seguridad establecidos en los módulos 11 (Control de Acceso Físico) y 16 (Gestión de Incidentes de Seguridad) de la norma ISO 27001, con el objetivo de asegurar la protección adecuada de los activos de información y la capacidad de respuesta efectiva ante incidentes de seguridad. El alcance abarca:   1. **Áreas Físicas y Recursos Involucrados:**    * **Data Center de Quilicura:** Revisión de los controles de acceso físico, incluyendo sistemas de vigilancia, autenticación y autorización para el personal autorizado.    * **Oficinas Corporativas:** Inspección de las medidas de seguridad física en las instalaciones generales, garantizando que las áreas sensibles estén adecuadamente protegidas.    * **Equipamiento y Activos Críticos:** Evaluación del manejo y protección de equipos críticos, tales como servidores, dispositivos de red y otros recursos esenciales para la continuidad del negocio. 2. **Procesos y Procedimientos a Evaluar:**    * **Control de Acceso Físico:** Evaluación de políticas, procedimientos, y tecnologías implementadas para gestionar y restringir el acceso físico a instalaciones sensibles, asegurando la seguridad de los activos de información.    * **Gestión de Incidentes de Seguridad:** Análisis de los procedimientos de identificación, notificación, respuesta y documentación de incidentes de seguridad, incluyendo la capacitación y preparación del personal.    * **Revisión de Documentación y Registros:** Análisis de la documentación relevante, tales como políticas de acceso, registros de acceso, reportes de incidentes de seguridad, y registros de auditorías anteriores. 3. **Periodo de Tiempo:**    * La auditoría cubrirá los controles y procesos implementados durante el año en curso, incluyendo revisiones de incidentes pasados que puedan haber ocurrido en el período anterior para verificar la aplicación de lecciones aprendidas y mejoras continuas. 4. **Entidades y Personal Involucrado:**    * El alcance incluirá entrevistas y revisiones con personal clave, incluyendo responsables de seguridad física, administradores de sistemas, personal de soporte técnico, y equipos de respuesta a incidentes de seguridad.    * Involucrará también la interacción con personal de auditoría interna para verificar la implementación de controles y procesos, y la revisión de cualquier auditoría previa relacionada. |

**Criterios de Auditoria y Documentación de Referencia**

|  |
| --- |
| **ISO 27001:2013 - Estándar principal que regula los sistemas de gestión de la seguridad de la información. Los módulos relevantes son:**   * **Cláusula 11: Seguridad física y del entorno.** * **Cláusula 16: Gestión de incidentes de seguridad de la información.**   **Política de Control de Ingreso al Data Center - Documento interno que define las directrices y procedimientos para la seguridad física y el control de acceso a las instalaciones de la empresa.**  **Procedimientos de Seguridad Física - Documentación interna sobre las medidas de seguridad y control físico en el Data Center, que cubren desde la vigilancia hasta el manejo de dispositivos y equipos.**  **Política de Gestión de Incidentes de Seguridad - Procedimientos y políticas relacionados con la detección, reporte, y manejo de incidentes de seguridad dentro de la organización.**  **Procedimiento de Gestión de Equipos - Normas internas sobre el manejo, almacenamiento y seguridad de los equipos, particularmente en el contexto del Data Center.**  **Procedimiento de Respaldo - Documentación interna que describe los métodos y prácticas para el respaldo y recuperación de datos críticos para la continuidad del negocio.**  **Registros de Control - Documentos que evidencian el control y monitoreo de accesos, incidentes, y otros aspectos de seguridad física y de información.** |

**Equipo Auditor**

|  |  |
| --- | --- |
| **Identificación Auditores** | **Cargo** |
| Jesús Castillo | Especialista en Seguridad Informática Auditor Líder |
| Vicente Farías | Técnico en Redes o Ciberseguridad  Auditor en Formación |
| Osvaldo Herrera | Técnico en Seguridad Informática  Auditor Asistente |
| Nicolás Páez | Profesional en formación  Observador |

**Representante de áreas Auditadas**

|  |  |
| --- | --- |
| **Identificación Representante** | **Área** |
| Administrador de sistemas | Data Center Principal |
| Jefe de Operaciones | Equipo Respaldo Energía |
| Jefe de Guardias | Control de Acceso y Vigilancia |
| Responsable de TI | Gestión de Incidentes de Seguridad |

**Programación**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hora** | **Fecha** | **Área** | **Documentos Aplicables** | **Representante** | **Auditor** |
| 09:00 | 18-08-2024 | **REUNION DE INICIO** | | Todos | Equipo |
| 10:00 | 23-08-2024 | Sistema Completo | ISO 27001:2013, Política de Control de Ingreso al Data Center, Procedimientos de Seguridad Física, Política de Gestión de Incidentes de Seguridad, Procedimiento de Gestión de Equipos, Procedimiento de Respaldo, Registros de Control | Administrador de sistemas | Jesus Castillo |
| 11:00 | 23-08-2024 | Auditoría de Personal | ISO 27001:2013, Política de Gestión de Incidentes de Seguridad, Procedimiento de Gestión de Equipos | Jefe de Operaciones | Vicente Farías (Auditor en Formación) |
| 12:00 | 23-08-2024 | Auditoría de Infraestructura | ISO 27001:2013, Procedimientos de Seguridad Física, Política de Control de Ingreso al Data Center, Procedimiento de Respaldo | Jefe de Guardias | Osvaldo Herrera (Auditor Asistente) |
| 13:00 |  | ALMUERZO | | | |
| 14:00 | 23-08-2024 | Auditoría de Cableado | ISO 27001:2013, Procedimiento de Gestión de Equipos, Registros de Control | Administrador de sistemas | Nicolas Paez (observador) |
| 15:00 | 30-08-2024 | Sistema Completo | ISO 27001:2013, Política de Control de Ingreso al Data Center, Procedimientos de Seguridad Física, Política de Gestión de Incidentes de Seguridad, Procedimiento de Gestión de Equipos, Procedimiento de Respaldo, Registros de Control | Administrador de sistemas | Vicente Farías (Auditor en Formación |
| 16:00 | 30-08-2024 | Auditoría de Personal | ISO 27001:2013, Política de Gestión de Incidentes de Seguridad, Procedimiento de Gestión de Equipos | Jefe de Operaciones | Osvaldo Herrera (Auditor Asistente) |
| 17:00 | 30-08-2024 | Auditoría de Infraestructura | ISO 27001:2013, Procedimientos de Seguridad Física, Política de Control de Ingreso al Data Center, Procedimiento de Respaldo | Jefe de Guardias | Osvaldo Herrera (Auditor Asistente) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hora** | **Fecha** | **Área** | **Documentos Aplicables** | **Representante** | **Auditor** |
| 09:00 | 30-08-2024 | Auditoría de Cableado | **ISO 27001:2013, Procedimiento de Gestión de Equipos, Registros de Control** | **Administrador de sistemas** | Nicolas Paez (observador) |
| 10:00 |  |  |  |  |  |
| 11:00 |  |  |  |  |  |
| 12:00 |  |  |  |  |  |
| 13:00 |  | ALMUERZO | | | |
| 14:00 |  |  |  |  |  |
| 15:00 |  |  |  |  |  |
| 16:00 |  |  |  |  |  |
| 17:00 | 18-09-2024 | **REUNION DE CIERRE** | | Todos | Equipo |

**Observaciones**

|  |
| --- |
| En el ámbito del **Control de Acceso Físico** (Dominio 11), se han identificado varias áreas de mejora. Primero, los roles y descriptores de cargos no están actualizados, lo que dificulta una definición clara de las responsabilidades para el control de acceso. En la oficina principal, se observa una falta de controles adecuados en las puertas de entrada y medidas contra amenazas externas, exponiendo a riesgos significativos. Aunque se han implementado controles avanzados en el área de TI, otras áreas no cuentan con medidas físicas suficientes para protegerse adecuadamente. Además, la ausencia de un área específica para el manejo de equipos dificulta el control efectivo y aumenta el riesgo de pérdida de activos.  En cuanto a la **Gestión de Incidentes de Seguridad** (Dominio 16), se detectan deficiencias en los procedimientos establecidos. Los procedimientos de gestión de incidentes no están actualizados ni adecuadamente probados, lo que afecta la eficacia en la resolución de incidentes. La falta de asignación clara de responsabilidades y pruebas de continuidad compromete la capacidad de respuesta ante eventos de seguridad. Además, se observa una carencia de evidencia documentada y lecciones aprendidas, lo que limita la capacidad para gestionar eventos de seguridad y mejorar las respuestas futuras. |