**CONTROLES APLICADOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N°** | **OBJETIVO DE CONTROL** | **CONTROL** | **ESTADO** | **JUSTIFICACIÓN** |
| A.5 | **POLÍTICAS DE SEGURIDAD.** | | | |
| A.5.1 | Política de seguridad de la información | **5.1.1 Documento de Política de seguridad de la información** | Aplicada | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.2 |
| **5.1.2 Revisión de la Política de seguridad de la información.** | Aplicada | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.2 |
| A.6 | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |
| A.6.1 | Organización Interna | **6.1.1 Compromiso de la Dirección con la Seguridad** | Aplicada | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2. |
| **6.1.2 Coordinación de la Seguridad de la Información.** | Aplicada | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2. |
| **6.1.3 Asignación de responsabilidades en seguridad de la información** | Aplicada | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2. |
| **6.1.4 Proceso de autorización para las instalaciones de procesamiento de la información.** | Aplicada | Aval Técnico para la Adquisición de Equipos y Servicios de Terceros para las Tecnologías de la Información y la Comunicación en la implementación de la Norma ISO 27001 apartado **3.1.3.3.** |
| **6.1.5 Acuerdos de Confidencialidad** | Aplicada | Acuerdo de Confidencialidad de la Información en la implementación de la Norma ISO 27001 apartado **3.1.3.4.** |
| **6.1.6 Contacto con las Autoridades.** | Aplicada | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2, aunque no se considera que ayude a mitigar los riesgos. |
| **6.1.7 Contacto con grupos de interés especial.** | Aplicada | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2. |
| **6.1.8 Revisión Independiente de la seguridad de la información.** | No aplica | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2, aunque no se considera porque el coste de implementación de este control supera al beneficio del Plan de Seguridad. |
| A.6.2 | Terceras Personas | **6.2.1 Identificación de riesgos relacionados con terceras partes.** | No aplica | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2, aunque no se considera porque el coste de implementación de este control supera al beneficio del Plan de Seguridad. |
| **6.2.2 Gestión de la seguridad al tratar con clientes.** | No aplica | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2, aunque no se considera que este control ayude a reducir el riesgo de los activos. |
| **6.2.3 Gestión de la Seguridad en contratos con terceras partes.** | No aplica | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado 3.1.2, aunque no se considera porque el coste de implementación de este control supera al beneficio del Plan de Seguridad. |
| A.7 | **GESTIÓN DE ACTIVOS.** | | | |
| A.7.1 | Responsabilidad de los Activos | **7.1.1 Inventario de activos.** | Aplicado | Procedimiento para la Documentación del Inventario de Activos de la Información en la implementación de la Norma ISO 27001 apartado **3.1.4.1.** |
| **7.1.2 Propiedad de los Activos.** | Aplicado | Procedimiento para la Documentación del Inventario de Activos de la Información en la implementación de la Norma ISO 27001 apartado **3.1.4.1.** |
| **7.1.3 Utilización aceptable de los activos.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| A.7.2 | Clasificación de la Información | **7.2.1 Guías de Clasificación.** | Aplicado | Procedimiento para la Codificación de los Activos de la Información en la implementación de la Norma ISO 27001 apartado **3.1.4.2.** |
| **7.2.2 Etiquetación y Tratamiento de la información.** | Aplicado | Procedimiento para la Codificación de los Activos de la Información en la implementación de la Norma ISO 27001 apartado **3.1.4.2.** |
| A.8 | **SEGURIDAD DE LA GESTIÓN DE LOS RECURSOS HUMANOS** | | | |
| A.8.1 | Antes de la  Contratación | 8.1.1 Roles y Responsabilidades. | No Aplica | Está estipulado en las Políticas SIG, el cual es un documento controlo y confidencial.  En el análisis de riesgos no se lo considera una amenaza. |
| 8.1.2 Análisis y Selección | No Aplica | Está estipulado en las Políticas SIG, el cual es un documento controlo y confidencial.  Se controla la selección de personal por el proceso de Talento Humano. |
| 8.1.3 Términos y condiciones de empleo. | No Aplica | Está estipulado en las Políticas SIG, el cual es un documento controlo y confidencial.  Documentado en los Contratos del Ministerio de Relaciones Laborales. |
| A.8.2 | Durante el empleo | 8.2.1 Responsabilidad de los gestores. | No Aplica | Está estipulado en las Políticas SIG, el cual es un documento controlo y confidencial.  En el análisis de riesgos no se lo considera una amenaza. |
| **8.2.2 Concienciación, formación.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Procedimiento para la Concienciación, Formación y Capacitación en Seguridad Informática en la implementación de la Norma ISO 27001 apartado **3.1.5.1.** |
| 8.2.3 Proceso disciplinario. | No Aplica | Está estipulado en las Políticas SIG, el cual es un documento controlo y confidencial.  Documentado en el Reglamento Interno de Seguridad y Salud de la Compañía CISEPRO CIA. LTDA. |
| A.8.3 | Finalización o cambio de empleo | 8.3.1 Responsabilidades ante la finalización. | No Aplica | Está estipulado en las Políticas SIG, el cual es un documento controlo y confidencial. |
| 8.3.2 Devolución de Activos. | No Aplica | Está estipulado en las Políticas SIG, el cual es un documento controlo y confidencial.  Delegado al Proceso de Operaciones. |
| 8.3.3 Retirada de los Derechos de Acceso. | No Aplica | Está estipulado en las Políticas SIG, el cual es un documento controlo y confidencial.  Delegado al Proceso de Operaciones. |
| A.9 | **SEGURIDAD FÍSICA Y DEL ENTORNO** | | | |
| A.9.1 | Áreas Seguras | **9.1.1 Perímetro de seguridad física.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Existen controles físicos en el perímetro de la empresa. |
| **9.1.2 Controles físicos de entrada.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Existen controles físicos en el perímetro de la empresa. |
| **9.1.3 Asegurar las oficinas, salas e instalaciones.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Existen controles físicos en el perímetro de la empresa. |
| **9.1.4 Protección contra amenazas externas y ambientales.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Las instalaciones de la Empresa se encuentran aseguradas basados en la normativa vigente del SGI y proporcional a la actividad y tamaño. |
| **9.1.5 Trabajo en Áreas Seguras.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
|  |  | 9.1.6 Áreas de acceso público, de carga y de distribución. | No aplica | La empresa CISEPRO CIA. LTDA se dedica a otras labores diferentes al ámbito de la cláusula. |
| A.9.2 | Seguridad de los Equipos | **9.2.1 Emplazamiento y protección de los equipos.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Procedimiento para Emplazamiento y Protección de los Equipo en la implementación de la Norma ISO 27001 apartado **3.1.6.1.** |
| **9.2.2 Servicios de soporte.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Los Servidores cuentan con esquemas alternos para respaldo de la red eléctrica. |
| **9.2.3 Seguridad del cableado.** | Aplicado | Las instalaciones cuentan con cableado seguro.  Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| **9.2.4 Mantenimiento de los Equipos.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| **9.2.5 Seguridad de los equipos fuera de las instalaciones.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| **9.2.6 Descarte o re-utilización seguros de los equipos.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Los Equipos de Cómputo se formatean a bajo nivel para evitar delitos informáticos. |
| **9.2.7 Extracción de elementos de la propiedad.** | Aplicado | No se pueden extraer los equipos fuera de las instalaciones sin disposición de la alta Gerencia.  Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| A.10 | **GESTIÓN DE LAS COMUNICACIONES Y LAS OPERACIONES.** | | | |
| A.10.1 | Procedimientos operativos y responsabilidades | **10.1.1 Procedimientos operativos documentados.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| **10.1.2 Gestión de cambios.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| **10.1.3 Separación de tareas.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| 10.1.4 Separación de las instalaciones de desarrollo, prueba y operación. | No aplica | La empresa CISEPRO no instaura la separación de los recursos de desarrollo. |
| A.10.2 | Gestión de los servicios suministrados por Terceros. | 10.2.1 Suministro de Servicio. | No aplica | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2**, aunque no se considera porque el coste de implementación de este control supera al beneficio del Plan de Seguridad. |
| 10.2.2 Revisión y monitorización de servicios de terceras partes. | No aplica | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2**, aunque no se considera porque el coste de implementación de este control supera al beneficio del Plan de Seguridad. |
| 10.2.3 Gestión de cambios a los servicios de terceras partes. | No aplica | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2**, aunque no se considera porque el coste de implementación de este control supera al beneficio del Plan de Seguridad. |
| A.10.3 | Planificación y aceptación del sistema.  Protección frente o código malicioso y código móvil | **10.3.1 Gestión de capacidad.** | Aplicado | Se hace un estudio periódico de las necesidades de cada uno de los procesos de la Empresa CISEPRO y como se los puede mejorar.    Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| **10.3.2 Aceptación del sistema** | Aplicado | Hasta la fecha de la elaboración de del plan se lo hace por socialización.  Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| **10.4.1 Controles contra código malicioso.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.**  Procedimiento para la instalación de software antivirus en la implementación de la Norma ISO 27001 apartado **3.1.7.1.**  Procedimiento para la instalación de anti malware en la implementación de la Norma ISO 27001 apartado **3.1.7.2.** |
| **10.4.2 Controles contra código móvil.** | Aplicado | Manual de Políticas, Procedimientos del SGSI en la implementación de la Norma ISO 27001 apartado **3.1.2.** |
| A.10.5 | Copias de Seguridad | 10.5.1 Respaldo de la Información. |  |  |
| A.10.6 | Gestión de la seguridad de la red | 10.6.1 Controles de red. |  |  |
| 10.6.2 Servicios de seguridad de redes. |  |  |
| A.10.7 | Gestión de soportes | 10.7.1 Gestión de soportes removibles |  |  |
| 10.7.2 Descarte de medios de almacenamiento de la información. |  |  |
| 10.7.3 Procedimiento de tratamiento de la información. |  |  |
| 10.7.4 Seguridad de la documentación del sistema |  |  |
| A.10.8 | Intercambio de información | 10.8.1 Políticas y procedimientos de intercambio de información. |  |  |
| 10.8.2 Acuerdos de intercambio. |  |  |
| 10.8.3 Soporte físico en tránsito. |  |  |
| 10.8.4 Mensajería electrónica. |  |  |
| 10.8.5 Sistemas de información de negocio. |  |  |
| A.10.9 | Servicios de comercio electrónico. | 10.9.1 Comercio electrónico. |  |  |
| 10.9.2 Transacciones en línea. |  |  |
| 10.9.3 Información pública disponible. |  |  |
| A.10.10 | Seguimiento | 10.10.1 Registro de Auditoria. |  |  |
| 10.10.2 Uso del sistema de monitorización |  |  |
| 10.10.3 Protección de la información de log. |  |  |
| 10.10.4 Log’s del operador y del administrador. |  |  |
| 10.10.5 Registro de fallos |  |  |
| 10.10.6 Sincronización horaria. |  |  |
| A.11 | **CONTROL DE ACCESOS** | | | |
| A.11.1 | Requisitos del negocio para el de acceso | 11.1.1 Política de acceso |  |  |
| A.11.2 | Gestión de accesos de los usuarios | 11.2.1 Registro de usuarios |  |  |
| 11.2.2 Gestión de privilegios. |  |  |
| 11.2.3 Gestión de contraseñas. |  |  |
| 11.2.4 Revisión de derechos de usuario. |  |  |
| A.11.3 | Responsabilidades del usuario | 11.3.1 uso de contraseñas. |  |  |
|  |  | 11.3.2 Equipamiento desatendido por el usuario. |  |  |
|  |  | 11.3.3 Políticas de mesas y pantallas limpias |  |  |
| A.11.4 | Control de acceso a la red | 11.4.1 Política de uso de servicios de red. |  |  |
| 11.4.2 Autenticación de usuarios para conexiones externas. |  |  |
| 11.4.3 Identificación de equipos en las redes. |  |  |
| 11.4.4 Protección del puerto remoto. |  |  |
| 11.4.5 Segmentación de redes. |  |  |
| 11.4.6 Control de conexión. |  |  |
| 11.4.7 Control de encaminamiento de redes. |  |  |
| A.11.5 | Control de acceso a los sistemas en operación. | 11.5.1 Procedimiento seguro de entrada a los sistemas de información. |  |  |
| 11.5.2 Identificación y autenticación de usuarios. |  |  |
| 11.5.3 Sistemas de gestión de contraseñas. |  |  |
| 11.5.4 Uso de utilidades del sistema. |  |  |
| 11.5.5 Finalización del tiempo de sesión. |  |  |
| 11.5.6 Limitación en el tiempo de conexión. |  |  |
| A.11.6 | Control de acceso a las aplicaciones y la información. | 11.6.1 Restricciones de acceso a la información. |  |  |
| 11.6.2 Aislamiento de sistemas sensibles. |  |  |
| A.11.7 | Informática móvil y teletrabajo | 11.7.1 Comunicaciones e informática móvil. |  |  |
|  |  | 11.7.2 Teletrabajo. |  |  |
| A.12 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN. | | | |
| A.12.1 | Requisitos de seguridad de los sistemas de información | 12.1.1 Análisis y especificación de los requisitos de seguridad. |  |  |
| A.12.2 | Tratamiento correcto de las aplicaciones. | 12.2.1 Validación de los datos de entrada. |  |  |
| 12.2.2 Control del procesamiento interno. |  |  |
| 12.2.3 Integridad de los mensajes. |  |  |
| 12.2.4 Validación de los datos de salida. |  |  |
| A.12.3 | Controles criptográficos. | 12.3.1 Política de uso de los controles criptográficos. |  |  |
| 12.3.2 Gestión de claves. |  |  |
| A.12.4 | Seguridad de los archivos de sistema. | 12.4.1 Control del software en explotación. |  |  |
| 12.4.2 Protección de los datos de prueba del sistema. |  |  |
| 12.4.3 Control de acceso al código fuente de los programas. |  |  |
| A.12.5 | Seguridad en los procesos de desarrollo y soporte. | 12.5.1 Procedimientos de control de cambios. |  |  |
| 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. |  |  |
| 12.5.3 Restricciones a los cambios en los paquetes de software. |  |  |
| 12.5.4 Fugas de información. |  |  |
| 12.5.5 Externalización del desarrollo de software. |  |  |
| A.12.6 | Gestión de la vulnerabilidad técnica. | 12.6.1 Control de las vulnerabilidades técnicas. |  |  |
| A.13 | GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. | | | |
| A.13.1 | Notificación de eventos y puntos débiles de seguridad de la información. | 13.1.1 Notificación de los eventos de seguridad de la información. |  |  |
| 13.1.2 Notificación de puntos débiles de seguridad. |  |  |
| A.13.2 | Gestión de incidentes y mejoras de seguridad de la información. | 13.2.1 Responsabilidades y procedimientos. |  |  |
|  |  | 13.2.2 Aprendizaje de los incidentes de seguridad de la información. |  |  |
|  |  | 13.2.3 Recopilación de evidencias. |  |  |
| A.14 | GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | | | |
| 14.1 | Aspectos de seguridad de la información en la gestión de la continuidad del negocio. | 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio. |  |  |
|  |  | 14.1.2 Continuidad del negocio y evaluación de riesgos. |  |  |
|  |  | 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información. |  |  |
|  |  | 14.1.4 Marco de referencia para la planificación de la continuidad del negocio. |  |  |
|  |  | 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad. |  |  |
| A15 | CUMPLIMIENTO | | | |
| A.15.1 | Cumplimiento de los requisitos legales. | 15.1.1 Identificación de la legislación aplicable. |  |  |
| 15.1.2 Derechos de propiedad intelectual (DPI).  15.1.3 Protección de los documentos de la organización. |  |  |
| 15.1.4 Protección de datos y privacidad de la información de carácter personal. |  |  |
| 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información. |  |  |
| 15.1.6 Regulación de los controles criptográficos. |  |  |
| A.15.2 | Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico. | 15.2.1 Cumplimiento de las políticas y normas de seguridad. |  |  |
|  |  | 15.2.2 Comprobación del cumplimiento técnico. |  |  |
| A.15.3 | Consideraciones sobre las auditorías de los sistemas de información. | 15.3.1 Controles de auditoría de los sistemas de información. |  |  |
|  |  | 15.3.2 Protección de las herramientas de auditoría de los sistemas de información. |  |  |