***CONTENIDO***

*INTRODUCCIÓN*

*OBJETIVO*

*ALCANCE Y METODOLOGÍA*

*LIMITANTES O RESTRICCIONES DE LA AUDITORIA*

*RESUMEN EJECUTIVO*

*EVALUACIÓN BASADA EN ISO 27002*

*DETALLE DE EVALUACIÓN ISO 27002*

*GRAFICAS SOBRE IMPLEMENTACIÓN DE ISO 27002*

*CONCLUSIONES Y RECOMENDACIONES GENERALES*

*ANEXOS*

***INTRODUCCIÓN***

El presente informe detalla los resultados de la auditoría informática realizada a la infraestructura y gestión tecnológica del **Instituto Internacional de Investigación y Educación (IIIE)**. Esta auditoría se enfocó en evaluar la solidez de las políticas de seguridad de la información de la institución, así como en identificar posibles vulnerabilidades que puedan comprometer la integridad, confidencialidad y disponibilidad de los datos y servicios críticos.

Para lograr este objetivo, se llevaron a cabo pruebas de seguridad exhaustivas, tanto internas como externas, dirigidas a la plataforma tecnológica del IIIE. Estas pruebas incluyeron evaluaciones de control de acceso, protección, gestión, entre otros aspectos clave de la seguridad informática. Las evaluaciones se basaron en el cumplimiento del estándar internacional **ISO/IEC 27002**, reconocido globalmente por establecer directrices para la implementación de controles de seguridad de la información.

El documento se estructura en dos secciones principales. En la primera sección, se presenta una evaluación detallada del cumplimiento del **ISO/IEC 27002** dentro del instituto. Esta sección incluye matrices que muestran qué controles específicos han sido adoptados como parte de las políticas de seguridad de la institución y cuál es el estado actual de su implementación. Estas matrices permiten visualizar de manera clara las áreas donde la organización ha alcanzado la conformidad con el estándar y aquellas que aún requieren mejoras.

La segunda sección se dedica a la identificación de nuevos hallazgos obtenidos a partir de las pruebas realizadas. Estos hallazgos proporcionan una visión actualizada de las vulnerabilidades y brechas de seguridad presentes en la infraestructura tecnológica del IIIE. Cada hallazgo se analiza en términos de su posible impacto en la operación de la institución y se proponen recomendaciones concretas para mitigar los riesgos asociados.

Es fundamental destacar que las recomendaciones y acciones sugeridas en este informe no solo tienen como objetivo reducir los riesgos identificados, sino también asegurar que el Instituto Internacional de Investigación y Educación (IIIE) cumpla con las mejores prácticas de seguridad informática y protección de los sistemas de información. Esto es esencial para garantizar la continuidad de las operaciones, proteger la información sensible y mantener la confianza de todos los involucrados.

***OBJETIVO***

Revisión exhaustiva del organigrama del Departamento de Informática (TI) del Instituto Internacional de Investigación y Educación (IIIE). Esta revisión tiene como propósito evaluar en detalle las funciones, responsabilidades y obligaciones asignadas a las diferentes unidades administrativas y puestos de trabajo dentro del departamento. El análisis se centrará en determinar si la estructura organizativa actual es adecuada para satisfacer las necesidades tecnológicas de la institución y si las responsabilidades están claramente definidas y alineadas con los objetivos estratégicos del IIIE.

Evaluación integral de los recursos tecnológicos de la institución, que abarca tanto los equipos e infraestructura como los sistemas informáticos en uso. La evaluación de los sistemas informáticos se realizará considerando todos sus componentes: desde las entradas de datos, procedimientos operativos, controles internos, hasta las bases de datos y mecanismos de seguridad implementados. Se analizará la capacidad de estos sistemas para manejar la información de manera segura, eficiente y confiable, garantizando que cumplen con los estándares de la industria y las mejores prácticas en seguridad informática.

Proporcionar una visión clara de los controles necesarios para asegurar que los sistemas informáticos del IIIE sean robustos, confiables y estén protegidos contra posibles amenazas. El buen desempeño de estos sistemas es fundamental para el funcionamiento efectivo de la institución, ya que de ellos depende la seguridad y la integridad de la información, así como la capacidad del instituto para cumplir con sus objetivos educativos y de investigación.

Identificar áreas de mejora y optimización en la gestión de la tecnología dentro del IIIE, asegurando que el departamento de TI esté bien equipado y organizado para enfrentar los desafíos actuales y futuros, y para apoyar el crecimiento y desarrollo continuo de la institución.

***ALCANCE Y METODOLOGÍA***

*Alcance:*

*La auditoría realizada se orientó en evaluar los requerimientos contenidos en los términos de requerimientos del desarrollo de la auditoria informática. Las áreas de evaluación fueron las siguientes:*

1. *POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN*
   1. *Directrices Establecidas Por La Dirección Para La Seguridad De La Información*
      1. *Directrices Establecidas Por La Dirección Para La Seguridad De La Información*
      2. *Revisión de las políticas para seguridad de la información*
2. *ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*
   1. *ORGANIZACIÓN INTERNA*
      1. *Roles y responsabilidades para la seguridad de la información*
      2. *Separación de deberes*
      3. *Contacto con las autoridades*
      4. *Contacto con grupos de interés especial*
      5. *Seguridad de la información en la gestión de proyectos*
   2. *DISPOSITIVOS MÓVILES Y TELETRABAJO*
      1. *Política para dispositivos móviles*
      2. *Teletrabajo*
3. *SEGURIDAD DE LOS RECURSOS HUMANOS*
   1. *ANTES DE ASUMIR EL EMPLEO*
      1. *Roles y Responsabilidades*
      2. *Términos y condiciones del empleo*
   2. *DURANTE LA EJECUCIÓN DEL EMPLEO*
      1. *Responsabilidades de la dirección*
      2. *Toma de conciencia, educación y formación en la seguridad de la información*
      3. *Proceso disciplinario*
   3. *TERMINACIÓN O CAMBIO DE EMPLEO*
      1. *Terminación o cambio de responsabilidades de empleo*
4. *GESTIÓN DE ACTIVOS*
   1. *RESPONSABILIDAD POR LOS ACTIVOS*
      1. *Inventario de activos*
      2. *Propiedad de los activos*
      3. *Uso aceptable de los activos*
      4. *Devolución de activos*
   2. *CLASIFICACIÓN DE LA INFORMACIÓN*
      1. *Clasificación de la información*
      2. *Etiquetado de la información*
      3. *Manejo de activos*
   3. *MANEJO DE MEDIOS*
      1. *Gestión de medios removibles*
      2. *Disposición de los medios*
      3. *Transferencia de medios físicos*
5. *CONTROL DE ACCESO*
   1. *REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO*
      1. *Política de control de acceso*
      2. *Acceso a redes y a servicios en red*
   2. *GESTIÓN DE ACCESO DE USUARIOS*
      1. *Registro y cancelación del registro de usuarios*
      2. *Suministro de acceso de usuarios*
      3. *Gestión de derechos de acceso privilegiado*
      4. *Gestión de información de autenticación secreta de usuarios*
      5. *Revisión de los derechos de acceso de usuarios*
      6. *Retiro o ajuste de los derechos de acceso*
   3. *RESPONSABILIDADES DE LOS USUARIOS*
      1. *Uso de información de autenticación secreta*
   4. *CONTROL DE ACCESO A SISTEMAS Y APLICACIONES*
      1. *Restricción de acceso a la información*
      2. *Procedimiento de ingreso seguro*
      3. *Sistema de gestión de contraseñas*
      4. *Uso de programas utilitarios privilegiados*
      5. *Control de acceso a códigos fuente de programas*
6. *SEGURIDAD FÍSICA Y DEL ENTORNO*
   1. *ÁREAS SEGURAS*
      1. *Perímetro de seguridad física*
      2. *Controles físicos de entrada*
      3. *Seguridad de oficinas, recintos e instalaciones*
      4. *Protección contra amenazas externas y ambientales*
      5. *Trabajo en áreas seguras*
      6. *Áreas de despacho y carga*
   2. *EQUIPOS*
      1. *Ubicación y protección de los equipos*
      2. *Servicios de suministro*
      3. *Seguridad del cableado*
      4. *Mantenimiento de equipos*
      5. *Retiro de activos*
      6. *Seguridad de equipos y activos fuera de las instalaciones*
      7. *Disposición segura o reutilización de equipos*
      8. *Equipos de usuario desatendidos*
      9. *Política de escritorio y pantalla limpios*
7. *ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS*
   1. *REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN*
      1. *Análisis y especificación de requisitos de seguridad de la información*
      2. *Seguridad de servicios de las aplicaciones en redes públicas*
      3. *Protección de transacciones de los servicios de las aplicaciones*
   2. *SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE*
      1. *Política de desarrollo seguro*
      2. *Procedimientos de control de cambios en sistemas*
      3. *Revisión técnica de las aplicaciones después de cambios en la plataforma de operación*
      4. *Restricciones en los cambios a los paquetes de software*
      5. *Principios de construcción de sistemas seguros*
      6. *Ambiente de desarrollo seguro*
      7. *Desarrollo contratado externamente*
      8. *Pruebas de seguridad de sistemas*
      9. *Prueba de aceptación de sistemas*
   3. *DATOS DE PRUEBA*
      1. *Protección de datos de prueba*
8. *RELACIONES CON LOS PROVEEDORES*
   1. *SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES*
      1. *Política de seguridad de la información para las relaciones con proveedores*
      2. *Tratamiento de la seguridad dentro de los acuerdos con proveedores*
      3. *Cadena de suministro de tecnología de información y comunicación*
   2. *GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES*
      1. *Seguimiento y revisión de los servicios de los proveedores*
      2. *Gestión de cambios en los servicios de los proveedores*
9. *ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO*
   1. *CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN*
      1. *Planificación de la continuidad de la seguridad de la información*
      2. *Implementación de la continuidad de la seguridad de la información*
      3. *Verificación, revisión y evaluación de la continuidad de la seguridad de la información*
   2. *REDUNDANCIAS*
      1. *Disponibilidad de instalaciones de procesamiento de información.*
10. *CUMPLIMIENTO*
    1. *CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES*
       1. *Identificación de la legislación aplicable y de los requisitos contractuales*
       2. *Derechos de propiedad intelectual*
       3. *Protección de registros*
       4. *Privacidad y protección de información de datos personales.*
       5. *Reglamentación de controles criptográficos*
    2. *REVISIONES DE SEGURIDAD DE LA INFORMACIÓN*
       1. *Revisión independiente de la seguridad de la información*
       2. *Cumplimiento con las políticas y normas de seguridad*
       3. *Revisión del cumplimiento técnico*

***Evaluación del ISO 27001***

*En esta revisión se evaluaron las categorías que comprende el estándar ISO 27002, cada categoría se evalúá en forma individual, haciendo las excepciones de aquellos controles que no aplican por el tipo de institución que se está evaluando.*

*Se realizaron pruebas tanto internas como externas para verificar la existencia de nuevas vulnerabilidades que pudieran poner en riesgo la plataforma tecnológica.*

***Metodología:***

Para evaluar el cumplimiento de las normas **NTC-ISO/IEC 27002** en el **Instituto Internacional de Investigación y Educación (IIIE)**, se adoptará una metodología estructurada en varias fases clave. En primer lugar, se realizará una revisión documental exhaustiva de las políticas, procedimientos y normativas internas de la institución, con el objetivo de identificar los controles de seguridad ya implementados y compararlos con los requisitos especificados en la norma ISO/IEC 27002. Esto incluirá la identificación de controles relacionados con la gestión de activos, control de accesos, criptografía, seguridad física y ambiental, entre otros. Cada control se evaluará en términos de su existencia, adecuación y efectividad en el contexto operativo del IIIE.

Posteriormente, se llevarán a cabo entrevistas y encuestas con el personal clave del Departamento de TI y otras áreas relevantes para obtener una comprensión más profunda de cómo se aplican y monitorean estos controles en la práctica diaria. Esta fase incluirá las revisiones de registros de auditoría, para verificar la efectividad real de las medidas de seguridad implementadas. Finalmente, se desarrollará un informe que detalle los hallazgos, identificando las brechas de cumplimiento con la norma y proporcionando recomendaciones específicas para fortalecer la postura de seguridad de la institución, alineándola con los estándares internacionales de mejores prácticas en seguridad de la información.

***LIMITANTES O RESTRICCIONES DE LA AUDITORIA***

*Durante el desarrollo de la auditoria informática se presentarón las limitantes:*

* *Políticas Informáticas en Proceso de Aprobación: Las políticas informáticas de la institución se encuentran actualmente en proceso de aprobación, lo que significa que aún no han sido formalmente adoptadas ni comunicadas al personal. Esta situación generó un ambiente de incertidumbre entre los participantes de la auditoría, ya que muchos de los controles y procedimientos clave no estaban completamente establecidos ni operativos en el momento de la evaluación. La falta de políticas aprobadas dificultó la evaluación de su efectividad y su alineación con los estándares de seguridad de la información, introduciendo un grado significativo de indefinición en el proceso de auditoría.*
* *Ausencia de Personal Clave del Área de Informática: Durante la auditoría, se enfrentó la ausencia de varios miembros clave del personal de informática, quienes se encontraban de vacaciones. Esta situación impidió la realización de entrevistas esenciales para evaluar la aplicabilidad y el cumplimiento de los instrumentos de auditoría planificados. La falta de interacción con estos individuos críticos limitó la obtención de información cualitativa importante, como el entendimiento profundo de los procedimientos internos y la verificación directa de la implementación de controles de seguridad específicos.*
* *Falta de Información Soporte: No se logró acceder a toda la información de soporte necesaria para llevar a cabo ciertas pruebas críticas durante la auditoría. Esta restricción incluyó la falta de documentación completa, como registros de actividades, reportes de auditorías anteriores, y evidencia documental sobre la implementación de controles de seguridad. La ausencia de esta información dificultó la validación de algunos de los hallazgos y redujo la capacidad de realizar una evaluación exhaustiva del estado actual de la infraestructura tecnológica y de seguridad de la institución.*

***RESUMEN EJECUTIVO***

*El Presente Informe de Auditoría número 1, correspondiente a la auditoria de Tecnologías de la Información del* **Instituto Internacional de Investigación y Educación (IIIE)**.*, por el periodo comprendido entre el 1 de Mayo al 25 de Agosto de 2024.*

*Los sistemas informáticos actualmente cumplen un papel importante en los diferentes procesos del negocio, sin importar su giro. Los estándares existen para crear un equilibrio entre la presión de la oferta tecnológica por parte de los proveedores y la demanda de sistemas acorde a la necesidad de los ciudadanos e instituciones.*

*Como resultado* de la auditoria, se han encontrados hallazgos, que se detallan en los siguientes párrafos; mismas que permitirán tomar acciones que pueden ser preventivas o correctivas con el propósito de mejorar los controles existentes e incorporar controles inexistentes.

1. ***Gestión de Activos:*** *No se ha realizado un inventario completo de los activos de información, lo que impide un control adecuado de su protección.*
2. ***Clasificación de la Información:*** *La institución carece de un esquema formal de clasificación de la información, lo que pone en riesgo la confidencialidad de los datos sensibles.*
3. ***Control de Acceso:*** *Las políticas de control de acceso no se han actualizado para incluir medidas de autenticación multifactor, aumentando el riesgo de accesos no autorizados.*
4. ***Seguridad Física y Ambiental:*** *No se han implementado controles adecuados para proteger los equipos informáticos contra desastres naturales o interrupciones del servicio eléctrico.*
5. ***Gestión de Contraseñas:*** *Las políticas de gestión de contraseñas no están alineadas con las mejores prácticas, permitiendo el uso de contraseñas débiles y sin rotación periódica.*
6. ***Control de Acceso a Redes:*** *No se han implementado políticas estrictas para el control de acceso a la red, lo que permite conexiones no seguras y potencialmente peligrosas.*
7. *Protección contra Malware: No se cuenta con una solución de protección contra malware actualizada y centralizada, dejando vulnerables los sistemas a infecciones de software malicioso.*
8. ***Cifrado de Datos:*** *La institución no ha implementado el cifrado adecuado para la protección de datos en tránsito y en reposo, exponiendo la información a posibles brechas de seguridad.*
9. ***Gestión de Riesgos:*** *No se ha realizado una evaluación formal de riesgos de seguridad de la información, lo que dificulta la identificación y mitigación de posibles amenazas.*
10. ***Seguridad en las Comunicaciones:*** *No se han establecido procedimientos seguros para la transmisión de información confidencial por correo electrónico o redes públicas.*
11. ***Respaldo de Información:*** *La política de respaldo de información no contempla pruebas regulares de recuperación, poniendo en riesgo la disponibilidad de datos en caso de fallos.*
12. ***Gestión de Incidentes de Seguridad:*** *No se dispone de un plan de respuesta a incidentes de seguridad formalizado y probado, lo que puede retrasar la recuperación ante una brecha.*
13. ***Formación y Concienciación en Seguridad:*** *No se han implementado programas regulares de formación y concienciación en seguridad de la información para el personal.*
14. ***Gestión de Parches y Actualizaciones:*** *No existe un proceso formal de gestión de parches, lo que deja vulnerabilidades conocidas sin corregir en los sistemas de la institución.*
15. ***Auditoría de Accesos:*** *No se realizan auditorías regulares de los registros de acceso a sistemas críticos, lo que podría permitir la actividad maliciosa sin detección.*
16. ***Política de Uso Aceptable:*** *La política de uso aceptable de recursos tecnológicos no se ha actualizado para incluir dispositivos móviles y acceso remoto.*
17. ***Seguridad de Proveedores:*** *No se han establecido acuerdos de seguridad específicos con los proveedores de servicios tecnológicos, lo que podría comprometer la seguridad externa.*
18. ***Gestión de Cambios:*** *No existe un proceso formal de gestión de cambios en los sistemas, lo que aumenta el riesgo de interrupciones no planificadas y errores de configuración.*
19. ***Seguridad en el Desarrollo de Software:*** *No se han implementado controles de seguridad en el ciclo de vida del desarrollo de software, lo que podría introducir vulnerabilidades en aplicaciones críticas.*
20. ***Control de Medios de Almacenamiento:*** *No hay políticas para el manejo seguro de medios de almacenamiento extraíbles, lo que incrementa el riesgo de pérdida o fuga de datos.*
21. ***Seguridad en Entornos Virtuales:*** *No se han implementado controles específicos para la seguridad de los entornos virtuales, dejando estos sistemas expuestos a riesgos adicionales.*
22. ***Acceso a Bases de Datos:*** *Los controles de acceso a bases de datos no están suficientemente segregados, lo que podría permitir accesos no autorizados a información sensible.*
23. ***Seguridad en la Nube:*** *No se ha realizado una evaluación completa de los riesgos asociados al uso de servicios en la nube, lo que podría comprometer la información almacenada externamente.*
24. ***Mantenimiento de Equipos:*** *No se cuenta con un plan formal de mantenimiento preventivo y correctivo para los equipos críticos, lo que puede afectar la disponibilidad de los servicios.*
25. ***Registro de Eventos:*** *No se ha implementado un sistema centralizado para el registro y monitoreo de eventos de seguridad, dificultando la detección de actividades anómalas.*
26. ***Seguridad en Dispositivos Móviles:*** *No existen políticas que regulen el uso seguro de dispositivos móviles con acceso a recursos corporativos, exponiendo datos a riesgos de pérdida o robo.*
27. ***Gestión de Identidades:*** *No se han implementado controles adecuados para la gestión de identidades, lo que podría resultar en la creación de cuentas duplicadas o sin autorización.*
28. ***Seguridad en el Acceso Remoto:*** *No se han establecido procedimientos seguros para el acceso remoto a la red de la institución, lo que aumenta el riesgo de accesos no autorizados.*
29. ***Control de Acceso Físico:*** *No se han actualizado los controles de acceso físico a las áreas sensibles del centro de datos, lo que permite el acceso sin la debida autorización.*
30. ***Evaluación de la Infraestructura de Red:*** *No se ha realizado una evaluación completa de la infraestructura de red para identificar y mitigar vulnerabilidades críticas, lo que podría comprometer la seguridad de la red institucional.*

*El siguiente gráfico muestra el estado actual de la incorporación del ISO 27002 en la institución. ----- Mostrar Grafica resumen de controles definidos según cada grupo ---*

*Redactar los resultados*

***EVALUACIÓN BASADA EN LA NORMA ISO 27002***

*La norma ISO/IEC 27002 está diseñada para guiar la gestión de la seguridad de la información mediante la implementación de las mejores prácticas que aseguren los tres pilares fundamentales: Confidencialidad, Integridad y Disponibilidad de la Información. Estos principios son esenciales para proteger la información crítica de la institución contra accesos no autorizados, alteraciones indebidas y la pérdida de disponibilidad. La evaluación realizada en el Instituto Internacional de Investigación y Educación (IIIE) se basó en una revisión exhaustiva de los controles definidos en los catorce (14) dominios que conforman la norma ISO/IEC 27002.*

*Sin embargo, se excluyeron de la evaluación aquellos controles cuya naturaleza no es aplicable a la institución. Esto incluye, por ejemplo, controles relacionados con el comercio electrónico, la tercerización de servicios, y el desarrollo externo de software, entre otros. La revisión se centró en los controles que, al ser incorporados, permitirían fortalecer significativamente las políticas de seguridad de la información de la institución, alineándolas con un estándar de seguridad internacionalmente reconocido.*

*En las siguientes secciones, se presentan matrices que resumen el estado actual del cumplimiento del estándar ISO/IEC 27002 en relación con las acciones emprendidas por la administración del IIIE para gestionar de manera efectiva las tecnologías de información. Estas matrices proporcionan una visión clara de los controles que han sido implementados, aquellos que están en proceso, y los que aún requieren atención. A continuación, se detalla cada uno de los criterios de control más significativos del ISO/IEC 27002 que no han sido implementados plenamente como parte de los controles de seguridad de la institución. Esta información es crucial para identificar las áreas donde es necesario realizar mejoras o adoptar nuevas medidas para elevar el nivel de seguridad de la información al estándar internacional que la norma exige.*

***CATEGORIA 5: POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| *5.1.1* | *¿Existe un documento formal que contenga la política de seguridad de la información aprobado por la dirección?* |  |  |  |  |  |  |
| *5.1.2* | *¿Las políticas de seguridad de la información abordan adecuadamente los requisitos de la estrategia de negocio, reglamentaciones, legislación, y el entorno de amenazas?* |  |  |  |  |  |  |
| *5.2.1* | *¿Están claramente definidas las responsabilidades generales y específicas para la gestión de la seguridad de la información dentro de las políticas?* |  |  |  |  |  | *Asegurar que las políticas detallen quién es responsable de la implementación, monitoreo, y revisión de las medidas de seguridad, incluyendo tareas específicas como la gestión de riesgos, la respuesta a incidentes, y el cumplimiento regulatorio.* |
| *5.2.2* | *¿Existen políticas específicas para el control de acceso, clasificación de información, seguridad física y del entorno, entre otros temas mencionados?* |  |  |  |  |  |  |
| *5.2.3* | *¿Se cuenta con una política de uso aceptable de los activos y una política de escritorio y pantalla limpia?* |  |  |  |  |  | *Desarrollar e implementar una política de escritorio y pantalla limpia que requiera que los empleados mantengan sus espacios de trabajo ordenados y libres de información sensible cuando no estén presentes.* |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN***

***5.2.1*** *¿Están claramente definidas las responsabilidades generales y específicas para la gestión de la seguridad de la información dentro de las políticas?*

***5.2.3*** *¿Se cuenta con una política de uso aceptable de los activos y una política de escritorio y pantalla limpia?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Durante la auditoría se identificó que las políticas de seguridad de la información del Instituto Internacional de Investigación y Educación (IIIE) no especifican de manera clara las responsabilidades generales y específicas relacionadas con la gestión de la seguridad de la información.*

*Se constató que la institución no cuenta con una política de escritorio y pantalla limpia.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *MEDIO* | *MEDIO* | *BAJO* |

*Recomendación:*

*5.2.1 Hay que asegurar que las políticas detallen quién es responsable de la implementación, monitoreo, y revisión de las medidas de seguridad, incluyendo tareas específicas como la gestión de riesgos, la respuesta a incidentes, y el cumplimiento regulatorio.*

*5.2.3 Desarrollar e implementar una política de escritorio y pantalla limpia que requiera que los empleados mantengan sus espacios de trabajo ordenados y libres de información sensible cuando no estén presentes.*

***GRAFICAS SOBRE IMPLEMENTACIÓN DE ISO 27002***

*Las siguientes gráficas que se muestran un porcentaje aproximado de los requerimientos por dominio la institución fiscal y aduanera ha considerado dentro de sus políticas de seguridad, para lograr adoptar las normas establecidas en el estándar de la ISO 27002.*

***“”””””Agregar el resto de graficos por dominio “””””“”***

***CATEGORIA 6: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| *6.1* | *¿Están claramente definidos y documentados los roles y responsabilidades de seguridad de la información dentro de la organización?* |  |  |  |  |  | *Hay que asegurar que todos los empleados comprendan sus responsabilidades de seguridad de la información a través de capacitaciones y comunicaciones claras. Esto puede incluir la distribución de manuales, políticas, y procedimientos relevantes.* |
| *6.1.1* | *¿Existe un proceso para asignar y revisar regularmente las responsabilidades de seguridad de la información?* |  |  |  |  |  |  |
| *6.1.2* | *¿Tiene la organización procedimientos establecidos para contactar con las autoridades en caso de incidentes de seguridad de la información?* |  |  |  |  |  |  |
| *6.1.3* | *¿Está la organización afiliada a grupos de interés especial o asociaciones profesionales especializadas en seguridad de la información?* |  |  |  |  |  | *Se recomienda que la organización considere afiliarse a asociaciones profesionales especializadas en seguridad de la información.* |
| *6.1.4* | *¿Se realiza una evaluación de riesgos de seguridad de la información en todas las fases de un proyecto?* |  |  |  |  |  |  |
| *6.2* | *¿Tiene la organización una política definida para el teletrabajo, incluyendo condiciones y restricciones?* |  |  |  |  |  |  |
| *6.2.1* | *¿Se han implementado medidas para asegurar la seguridad física y de la información en los sitios de teletrabajo?* |  |  |  |  |  | *Ofrecer capacitación específica sobre las mejores prácticas de seguridad para el teletrabajo, incluyendo la gestión segura de documentos, el uso de redes Wi-Fi seguras, y la identificación de riesgos de seguridad en el entorno doméstico.* |
| *6.2.2* | *¿Existen procedimientos para la revocación de derechos de acceso y devolución de equipos cuando finaliza el teletrabajo?* |  |  |  |  |  |  |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN***

***6.1*** *¿Están claramente definidos y documentados los roles y responsabilidades de seguridad de la información dentro de la organización?*

***6.1.3*** *¿Está la organización afiliada a grupos de interés especial o asociaciones profesionales especializadas en seguridad de la información?*

***6.2.1*** *¿Se han implementado medidas para asegurar la seguridad física y de la información en los sitios de teletrabajo?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Se detectó que dentro de la organización no están claramente definidos y documentados los roles y responsabilidades relacionados con la seguridad de la información.*

*La organización no está actualmente afiliada a grupos de interés especial o asociaciones profesionales especializadas en seguridad de la información.*

*No se han implementado medidas específicas para asegurar la seguridad física y de la información en los sitios de teletrabajo.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *MEDIO* | *ALTO* | *ALTO* |

*Recomendación:*

*6.1 Hay que asegurar que todos los empleados comprendan sus responsabilidades de seguridad de la información a través de capacitaciones y comunicaciones claras. Esto puede incluir la distribución de manuales, políticas, y procedimientos relevantes.*

*6.1.3 Se recomienda que la organización considere afiliarse a asociaciones profesionales especializadas en seguridad de la información.*

*6.2.1 Ofrecer capacitación específica sobre las mejores prácticas de seguridad para el teletrabajo, incluyendo la gestión segura de documentos, el uso de redes Wi-Fi seguras, y la identificación de riesgos de seguridad en el entorno doméstico.*

***CATEGORIA 7: SEGURIDAD DE LOS RECURSOS HUMANOS***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| *7.1.1* | *¿Se realiza una investigación de antecedentes para todos los candidatos antes de la contratación?* |  |  |  |  |  | *Asegurarse de que el proceso de investigación de antecedentes cumpla con las leyes y regulaciones locales sobre privacidad y derechos laborales.* |
| *7.1.2* | *¿Se comunican claramente los términos y condiciones de la contratación a los candidatos antes de su incorporación?* |  |  |  |  |  |  |
| *7.2.1* | *¿Se definen claramente las responsabilidades de gestión relacionadas con la seguridad de la información para cada puesto de trabajo?* |  |  |  |  |  |  |
| *7.2.2* | *¿Se realizan programas continuos de concienciación y capacitación en seguridad de la información para mantener a los empleados actualizados sobre las mejores prácticas y políticas de la organización?* |  |  |  |  |  | *Asegurarse de que los contenidos de las capacitaciones se actualicen regularmente para reflejar las últimas amenazas, normativas y mejores prácticas en el campo de la seguridad de la información.* |
| *7.2.3* | *¿Existen procedimientos disciplinarios claros y documentados para abordar las violaciones a la seguridad de la información?* |  |  |  |  |  |  |
| *7.3.1* | *¿Se desactivan de inmediato los accesos a sistemas y recursos de información para los empleados que dejan la organización?* |  |  |  |  |  |  |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: SEGURIDAD DE LOS RECURSOS HUMANOS***

***7.1.1*** *¿Se realiza una investigación de antecedentes para todos los candidatos antes de la contratación?*

***7.2.2*** *¿Se realizan programas continuos de concienciación y capacitación en seguridad de la información para mantener a los empleados actualizados sobre las mejores prácticas y políticas de la organización?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Se detectó que la organización no realiza de manera sistemática investigaciones de antecedentes para todos los candidatos antes de su contratación.*

*No se llevan a cabo programas continuos y efectivos de concienciación y capacitación en seguridad de la información.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *ALTO* | *page52image17599872ALTA* | *MEDIA* |

*Recomendación:*

*7.1.1 Asegurarse de que el proceso de investigación de antecedentes cumpla con las leyes y regulaciones locales sobre privacidad y derechos laborales.*

*7.2.2 Asegurarse de que los contenidos de las capacitaciones se actualicen regularmente para reflejar las últimas amenazas, normativas y mejores prácticas en el campo de la seguridad de la información.*

***CATEGORIA 8: GESTIÓN DE ACTIVOS***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| *8.1.1* | *¿Se han identificado todos los activos y se mantiene un inventario o registro actualizado de todos los activos importantes?* |  |  |  |  |  |  |
| *8.1.2* | *¿Cada activo identificado tiene asignado un dueño o responsable?* |  |  |  |  |  |  |
| *8.1.3* | *¿Se han definido y comunicado las regulaciones para el uso aceptable de la información y los activos asociados a las instalaciones de procesamiento de información?* |  |  |  |  |  | *Es fundamental definir y comunicar claramente las regulaciones sobre el uso aceptable de la información y los activos relacionados.* |
| *8.1.4* | *¿Existen procedimientos establecidos para la devolución de activos cuando ya no son necesarios o cuando un empleado deja la organización?* |  |  |  |  |  |  |
| *8.2.1* | *¿Se clasifica la información en términos de su valor, requerimientos legales, sensibilidad y criticidad dentro de la organización?* |  |  |  |  |  |  |
| *8.2.2* | *¿Existen procedimientos definidos para el etiquetado y custodia de la información de acuerdo con su clasificación?* |  |  |  |  |  |  |
| *8.2.3* | *¿Se han implementado procedimientos para la correcta manipulación y protección de los activos según su clasificación?* |  |  |  |  |  |  |
| *8.3.1* | *¿Se han implementado procedimientos para la gestión de medios removibles, de acuerdo a la clasificación adoptada por la institución?* |  |  |  |  |  | *Es crucial establecer y aplicar procedimientos específicos para la gestión de medios removibles, alineados con la clasificación de la información de la organización.* |
| *8.3.2* | *¿Existen procedimientos establecidos para la eliminación segura de soportes de almacenamiento?* |  |  |  |  |  |  |
| *8.3.3* | *¿Se han definido medidas de seguridad para el transporte seguro de soportes físicos?* |  |  |  |  |  |  |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: GESTIÓN DE ACTIVOS***

***8.1.3*** *¿Se han definido y comunicado las regulaciones para el uso aceptable de la información y los activos asociados a las instalaciones de procesamiento de información?*

***8.3.1*** *¿Se han implementado procedimientos para la gestión de medios removibles, de acuerdo con la clasificación adoptada por la institución?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Se constató que la organización no ha definido ni comunicado de manera efectiva las regulaciones para el uso aceptable de la información y los activos asociados a las instalaciones de procesamiento de información.*

*La auditoría reveló que la organización no ha implementado procedimientos específicos y adecuados para la gestión de medios removibles, de acuerdo con la clasificación de información adoptada.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *MEDIO* | *MEDIO* | *MEDIO* |

*Recomendación:*

*8.1.3 Es fundamental definir y comunicar claramente las regulaciones sobre el uso aceptable de la información y los activos relacionados.*

*8.3.1 Es crucial establecer y aplicar procedimientos específicos para la gestión de medios removibles, alineados con la clasificación de la información de la organización.*

***CATEGORIA 9: CONTROL DE ACCESO***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| *9.1.1* | *¿Existen políticas, lineamientos y/o directrices para el uso y control de acceso al sistema de información?* |  |  |  |  |  |  |
| *9.1.1* | *¿Se ha establecido, documentar y revisar una política de control de acceso basado en los requisitos y exigencias establecidos según la norma vigente del sector público y de seguridad de la información?* |  |  |  |  |  |  |
| *9.1.2* | *¿Se han implementado procedimientos para darle acceso a los sistemas y servicios de red, a usuarios específicamente autorizados?* |  |  |  |  |  |  |
| *9.2.1* | *¿Se ha implementado un procesamiento formal de registro y retirada de usuarios que hagan posible la asignación de los derechos de acceso?* |  |  |  |  |  |  |
| *9.2.2* | *¿Se ha implementado un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios?* |  |  |  |  |  | *Existe un procedimiento formal para la asignación y revocación de derechos de acceso.* |
| *9.2.3* | *¿Está restringido y controlado la asignación y uso de privilegios de accesos?* |  |  |  |  |  | *La asignación y uso de privilegios de acceso están bajo control estricto.* |
| *9.2.4* | *¿Existe un control para la asignación de la información secreta de autenticación para que sea controlada a través de un proceso formal de gestión?* |  |  |  |  |  |  |
| *9.2.5* | *¿Se ha establecido revisiones de manera periódica al derecho de acceso de usuarios?* |  |  |  |  |  |  |
| *9.2.6* | *¿Los derechos de acceso de todos los funcionarios, a la información y a las instalaciones de procesamiento de la información exigen controles para el retiro de los respectivos accesos a la finalización del empleo, del contrato o del acuerdo, o ajustarlo en caso de cambio?* |  |  |  |  |  |  |
| *9.3.1* | *¿Existe un control para el uso de la información secreta de autenticación del sistema de información?* |  |  |  |  |  | *La información secreta de autenticación está controlada adecuadamente.* |
| *9.4.1* | *¿Se han establecido políticas para restringir el acceso a la información y las aplicaciones del sistema de información?* |  |  |  |  |  |  |
| *9.4.2* | *¿Existe un control mediante una política existente, para el procedimiento seguro de inicio de sesión?* |  |  |  |  |  |  |
| *9.4.3* | *¿Los sistemas y controles para la respectiva gestión de contraseñas son interactivos y aseguran la calidad de contraseñas?* |  |  |  |  |  |  |
| *9.4.4* | *¿Está restringido el uso de programas que pueden ser capaces de invalidar los controles de seguridad del sistema y aplicaciones?* |  |  |  |  |  | *Se restringe el uso de programas que puedan comprometer los controles de seguridad.* |
| *9.4.5* | *¿Existen controles que restringa el acceso al código fuente?* |  |  |  |  |  |  |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: CONTROL DE ACCESO***

***9.2.2*** *¿Se ha implementado un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios?*

***9.2.3*** *¿Está restringido y controlado la asignación y uso de privilegios de accesos?*

***9.3.1*** *¿Existe un control para el uso de la información secreta de autenticación del sistema de información?*

***9.4.4*** *¿Está restringido el uso de programas que pueden ser capaces de invalidar los controles de seguridad del sistema y aplicaciones?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Se identificó que la organización no ha implementado un procedimiento formal y documentado para la asignación y revocación de derechos de acceso para todos los tipos de usuarios en todos los sistemas y servicios.*

*La auditoría reveló que no existen controles estrictos para la asignación y el uso de privilegios de acceso.*

*Se constató que no se implementan controles adecuados para la protección de la información secreta utilizada en los sistemas de autenticación.*

*Se detectó que no existen restricciones efectivas sobre el uso de programas que podrían invalidar los controles de seguridad del sistema y aplicaciones.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *ALTO* | *page52image17599872ALTA* | *BAJA* |

*Recomendación:*

*9.2.2 Realizar un procedimiento formal para la asignación y revocación de derechos de acceso.*

*9.2.3 La asignación y uso de privilegios de acceso están bajo control estricto.*

*9.3.1 La información secreta de autenticación está controlada adecuadamente.*

*9.4.4 Se restringe el uso de programas que puedan comprometer los controles de seguridad.*

***CATEGORIA 11: SEGURIDAD FÍSICA Y DEL ENTORNO***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| *11.1.1* | *¿Está definido y en uso correctamente los perímetros de seguridad para el uso y protección de las áreas que contienen información crítica y/o sensible, así como las estaciones de procesamiento de la información?* |  |  |  |  |  |  |
| *11.1.2* | *¿Existen controles de seguridad adecuados, aplicados en las áreas seguras, para asegurar y garantizar únicamente el acceso al personal autorizado?* |  |  |  |  |  | *Controles de acceso efectivos están en lugar y monitoreados constantemente.* |
| *11.1.3* | *¿Existen controles que exijan el diseño y la aplicación de medidas para garantizar la seguridad física de las oficinas e instalaciones?* |  |  |  |  |  |  |
| *11.1.4* | *¿Existe un control que garantice la protección física contra desastres naturales, ataques naturales, ataques maliciosos o accidentes?* |  |  |  |  |  |  |
| *11.1.5* | *¿Existen procedimientos para trabajar en áreas seguras que deban ser diseñados y aplicados?* |  |  |  |  |  |  |
| *11.1.6* | *¿Existe* un *control en los puntos de acceso, tales como las áreas de carga y entrega, y otros puntos donde pueda acceder personal no autorizado a las instalaciones, y, si fuera posible, aislar dichos puntos de las instalaciones de procesamiento de la información para evitar accesos no adecuados?* |  |  |  |  |  |  |
| *11.2.1* | *¿Existen* controles *que protejan y garanticen que los equipos informáticos estén situados y protegidos de tal forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados?* |  |  |  |  |  | *Los equipos están ubicados y protegidos adecuadamente para minimizar riesgos.* |
| *11.2.2* | *¿Se han establecido* controles *de protección a los equipos informáticos contra fallos eléctricos y otras alteraciones?* |  |  |  |  |  | *Se dispone de controles contra fallos eléctricos y alteraciones.* |
| *11.2.3* | *¿Se estableció un control de seguridad para el cableado eléctrico y de telecomunicaciones que transmite datos o da soporte a los servicios de información?* |  |  |  |  |  |  |
| *11.2.4* | *¿Existe* un *plan de mantenimiento preventivo y correctivo de los equipos que asegure la disponibilidad y la integridad continua?* |  |  |  |  |  |  |
| *11.2.5* | *¿Pueden los equipos, la información o el software retirarse de las instalaciones sin autorización previa?* |  |  |  |  |  | *Cualquier retiro requiere autorización previa.* |
| *11.2.6* | *¿Existen medidas de seguridad para los equipos informáticos fuera de las instalaciones?* |  |  |  |  |  |  |
| *11.2.7* | *¿Se han implementado procedimientos adecuados para la reutilización o eliminación segura de equipos, asegurando que se proteja la información y se cumpla con las normativas de seguridad y medioambientales?* |  |  |  |  |  |  |
| *11.2.8* | *¿Existen controles de seguridad adecuados para el equipo de usuarios desatendido, a fin de proteger la información y prevenir accesos no autorizados?* |  |  |  |  |  |  |
| *11.2.9* | *¿Existen políticas de puesto de trabajo despejado y pantalla limpia para asegurar la protección de la información y prevenir accesos no autorizados cuando los equipos están desatendidos?* |  |  |  |  |  |  |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: SEGURIDAD FÍSICA Y DEL ENTORNO***

***11.1.2*** *¿Existen controles de seguridad adecuados, aplicados en las áreas seguras, para asegurar y garantizar únicamente el acceso al personal autorizado?*

***11.2.1*** *¿Existen controles que protejan y garanticen que los equipos informáticos estén situados y protegidos de tal forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados?*

***11.2.2*** *¿Se han establecido controles de protección a los equipos informáticos contra fallos eléctricos y otras alteraciones?*

***11.2.5*** *¿Pueden los equipos, la información o el software retirarse de las instalaciones sin autorización previa?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Se encontró que los controles de seguridad en las áreas designadas como seguras no son suficientes para garantizar que solo el personal autorizado tenga acceso.*

*Se observó que los equipos informáticos no están ubicados ni protegidos de manera adecuada para minimizar los riesgos de amenazas ambientales y accesos no autorizados.*

*La auditoría reveló que no se han establecido controles efectivos para proteger los equipos informáticos contra fallos eléctricos u otras alteraciones que puedan comprometer su funcionamiento.*

*Se detectó que no existe un control riguroso sobre el retiro de equipos, información o software de las instalaciones.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *MEDIA* | *BAJA* | *BAJA* |

*Recomendación:*

*11.1.2 Controles de acceso efectivos están en lugar y monitoreados constantemente.*

*11.2.1 Los equipos están ubicados y protegidos adecuadamente para minimizar riesgos.*

*11.2.2 Se dispone de controles contra fallos eléctricos y alteraciones.*

*11.2.5 Cualquier retiro requiere autorización previa.*

***CATEGORIA 14: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| ***14.1*** | ***REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN*** |  |  |  |  |  |  |
| *14.1.1* | *¿Existe un control de los análisis y las especificaciones de los requisitos de seguridad que sirvan para los nuevos sistemas de información o para mejoras de los mismos?* |  |  |  |  |  |  |
| *14.1.2* | *¿La organización cuenta con seguridad de las comunicaciones en servicios accesibles por redes públicas y así proteger las actividades?* |  |  |  |  |  |  |
| *14.1.3* | *¿Hay protección para la información involucrada en las transacciones realizadas por redes telemáticas?* |  |  |  |  |  |  |
| ***14.2*** | ***SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE*** |  |  |  |  |  |  |
| *14.2.1* | *¿Se establecen reglas y políticas para el desarrollo seguro de software?* |  |  |  |  |  |  |
| *14.2.2* | *¿Se realizan procedimientos formales de control de cambios en los sistemas?* |  |  |  |  |  |  |
| *14.2.3* | *¿Se realiza una revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo?* |  |  |  |  |  |  |
| *14.2.4* | *¿Hay una lista de las restricciones existentes al momento de realizar cambios en los paquetes de software?* |  |  |  |  |  | *No se tiene un registro de restricciones al momento de realizar cambios en el software.* |
| *14.2.5* | *¿Se han establecido y documentado el uso de los principios de ingeniería involucrados en la protección de sistemas seguros?* |  |  |  |  |  |  |
| *14.2.6* | *¿Se protegen de forma adecuada la seguridad en los entornos de desarrollo existentes?* |  |  |  |  |  |  |
| *14.2.7* | *¿Se supervisa y se hace seguimiento de las actividades que involucran el desarrollo de sistemas de manera externa?* |  |  |  |  |  |  |
| *14.2.8* | *¿Se realizan pruebas de funcionalidad de la seguridad durante el desarrollo de los sistemas?* |  |  |  |  |  |  |
| *14.2.9* | *¿Al finalizar tareas de desarrollo se establecen programas de prueba para aceptación?* |  |  |  |  |  |  |
| ***14.3*** | ***DATOS DE PRUEBA*** |  |  |  |  |  |  |
| *14.3.1* | *¿Al momento de realizar pruebas se protegen, seleccionan y controlan todos los datos de ensayo?* |  |  |  |  |  |  |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS***

***14.2.4*** *¿Hay una lista de las restricciones existentes al momento de realizar cambios en los paquetes de software?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Durante la auditoría se constató que la organización no cuenta con una lista formal de restricciones al momento de realizar cambios en los paquetes de software. La falta de un registro de estas restricciones puede llevar a modificaciones no controladas o inapropiadas, lo que podría introducir vulnerabilidades, afectar la estabilidad del sistema, o causar incumplimiento de normativas internas y externas.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *ALTO* | *page52image17599872MEDIA* | *MEDIA* |

*Recomendación:*

*14.2.4 Hacer un registro de restricciones al momento de realizar cambios en el software.*

***CATEGORIA 15: RELACIONES CON LOS PROVEEDORES***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| ***15.1*** | ***SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES*** |  |  |  |  |  |  |
| *15.1.1 a* | *¿Los requisitos en seguridad de la información son los adecuados para mitigar los riesgos asociados al acceso de proveedores a los activos de la organización?* |  |  |  |  |  |  |
| *15.1.1 b* | *¿Los requisitos en seguridad de la información son documentados para mitigar los riesgos asociados al acceso de proveedores a los activos de la organización?* |  |  |  |  |  |  |
| *15.1.2* | *¿Se establecen acuerdos documentados con todos los requisitos con los proveedores, para asegurarse que todo proveedor pueda acceder, procesar, almacenar, comunicar y suministrar componentes de infraestructura de TI para la información de la organización?* |  |  |  |  |  |  |
| *15.1.3* | *¿Se han incluido requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación?* |  |  |  |  |  |  |
| ***15.2*** | ***GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES*** |  |  |  |  |  |  |
| *15.2.1* | *¿Se realiza seguimientos, revisión y auditorías frecuentemente para la prestación de servicios de los proveedores?* |  |  |  |  |  | *Se realizan auditorías, pero no de manera frecuente.* |
| *15.2.2 a* | *¿Gestionan los cambios en el suministro de servicios por parte de proveedores, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información?* |  |  |  |  |  |  |
| *15.2.2 b* | *¿Se toma en cuenta la criticidad de la información, sistemas del negocio involucrados y la revaloración de riesgos cuando existen cambios de suministros de servicios por parte de proveedores?* |  |  |  |  |  |  |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: RELACIONES CON LOS PROVEEDORES***

***15.2.1*** *¿Se realiza seguimientos, revisión y auditorías frecuentemente para la prestación de servicios de los proveedores?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Se identificó que la organización no realiza seguimientos, revisiones ni auditorías frecuentes para evaluar la prestación de servicios de los proveedores. Esta ausencia de monitoreo continuo puede resultar en una falta de visibilidad sobre el desempeño y cumplimiento de los proveedores, lo que podría llevar a problemas no detectados que afecten la seguridad, calidad y disponibilidad de los servicios proporcionados.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *ALTO* | *page52image17599872ALTA* | *MEDIA* |

*Recomendación:*

*15.2.1 Realizar auditorías de manera frecuente.*

***CATEGORIA 17: ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN***

***DE CONTINUIDAD DE NEGOCIO***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| *17.1.1* | *¿Ha determinado la organización sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, como durante una crisis o desastre?* |  |  |  |  |  | *Revisar y actualizar los planes de continuidad y seguridad basándose en evaluaciones regulares del impacto y la eficacia de los controles existentes.* |
| *17.1.2* | *¿Ha establecido, documentado, implementado y mantenido la organización los procesos, procedimientos y controles necesarios para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa?* |  |  |  |  |  | *Desarrollar y documentar un plan de acción detallado para la actualización y mantenimiento de controles en situaciones adversas.* |
| *17.1.3* | *¿Verifica la organización, a intervalos regulares, que los controles de continuidad de la seguridad de la información establecidos e implementados son válidos y eficaces durante situaciones adversas?* |  |  |  |  |  | *Establecer un calendario de revisión y pruebas regulares para evaluar la efectividad de los controles.* |
| *17.2.1* | *¿Asegura la organización que las instalaciones de procesamiento de información cuentan con redundancia suficiente para cumplir los requisitos de disponibilidad?* |  |  |  |  |  | *Actualizar todos los manuales técnicos y de usuario y asegurar la redundancia de datos y sistemas para mantener la disponibilidad.* |

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO***

***17.1.1*** *¿Ha determinado la organización sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, como durante una crisis o desastre?*

***17.1.2*** *¿Ha establecido, documentado, implementado y mantenido la organización los procesos, procedimientos y controles necesarios para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa?*

***17.1.3*** *¿Verifica la organización, a intervalos regulares, que los controles de continuidad de la seguridad de la información establecidos e implementados son válidos y eficaces durante situaciones adversas?*

***17.2.1*** *¿Asegura la organización que las instalaciones de procesamiento de información cuentan con redundancia suficiente para cumplir los requisitos de disponibilidad?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*La auditoría descubrió que la organización no ha definido claramente sus requisitos para la seguridad de la información y la continuidad en situaciones adversas, como crisis o desastres.*

*Se identificó que los procesos, procedimientos y controles necesarios para asegurar la continuidad de la seguridad de la información durante situaciones adversas no están suficientemente documentados, implementados ni mantenidos.*

*La revisión reveló que no se realizan verificaciones regulares para asegurar que los controles de continuidad de la seguridad de la información sean válidos y eficaces durante situaciones adversas.*

*Se observó que las instalaciones de procesamiento de información no cuentan con la redundancia adecuada para cumplir con los requisitos de disponibilidad.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *ALTO* | *page52image17599872ALTA* | *ALTA* |

*Recomendación:*

*17.1.1 Revisar y actualizar los planes de continuidad y seguridad basándose en evaluaciones regulares del impacto y la eficacia de los controles existentes.*

*17.1.2 Desarrollar y documentar un plan de acción detallado para la actualización y mantenimiento de controles en situaciones adversas.*

*17.1.3 Establecer un calendario de revisión y pruebas regulares para evaluar la efectividad de los controles.*

*17.2.1 Actualizar todos los manuales técnicos y de usuario y asegurar la redundancia de datos y sistemas para mantener la disponibilidad.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***No. Control*** | **Descripción del Control**  **ISO 27002** | ***Control Considerado en las Políticas de Seguridad*** | | ***Control Actualmente Implementado*** | | | ***Observaciones y Acciones Recomendadas*** |
| ***Si*** | ***A incorporar*** | ***Si*** | ***No*** | ***En proceso*** |
| *18.1.1* | *¿La organización ha identificado todos los requisitos legales, reglamentarios y contractuales pertinentes?* |  |  |  |  |  |  |
| *18.1.2* | *¿La organización tiene procedimientos para asegurar el cumplimiento de los requisitos relacionados con los derechos de propiedad intelectual?* |  |  |  |  |  | *Implementar procedimientos formales para asegurar la protección y cumplimiento de los derechos de propiedad intelectual.* |
| *18.1.3* | *¿La organización considera todos los riesgos al proteger los registros?* |  |  |  |  |  | *Desarrollar e implementar políticas para la clasificación, almacenamiento y protección eficaz de registros.* |
| *18.1.4* | *¿La organización asegura la privacidad y la protección de la información de datos personales?* |  |  |  |  |  | *Reforzar las medidas de protección de datos personales, incluyendo auditorías y capacitaciones regulares sobre privacidad.* |
| *18.1.5* | *¿La organización cumple con las leyes y reglamentaciones relacionadas con el uso de controles criptográficos?* |  |  |  |  |  | *Asegurar el cumplimiento con las leyes y reglamentaciones sobre el uso de la criptografía y realizar revisiones regulares.* |
| *18.2.1* | *¿La organización realiza revisiones independientes de la seguridad de la información?* |  |  |  |  |  |  |
| *18.2.2* | *¿Los directores revisan periódicamente el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad?* |  |  |  |  |  | *Establecer un sistema más riguroso para revisiones regulares y garantizar el cumplimiento de las políticas y normas de seguridad.* |
| *18.2.3* | *¿La organización revisa periódicamente el cumplimiento técnico de los sistemas de información?* |  |  |  |  |  | *Implementar herramientas automáticas para mejorar la eficiencia y precisión de las revisiones de cumplimiento técnico.* |

***CATEGORIA 18: CUMPLIMIENTO***

***DETALLE DE EVALUACIÓN ISO 27002***

***DOMINIO: CUMPLIMIENTO***

***18.1.2*** *¿La organización tiene procedimientos para asegurar el cumplimiento de los requisitos relacionados con los derechos de propiedad intelectual?*

***18.1.3*** *¿La organización considera todos los riesgos al proteger los registros?*

***18.1.4*** *¿La organización asegura la privacidad y la protección de la información de datos personales?*

***18.1.5*** *¿La organización cumple con las leyes y reglamentaciones relacionadas con el uso de controles criptográficos?*

***18.2.2*** *¿Los directores revisan periódicamente el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad?*

***18.2.3*** *¿La organización revisa periódicamente el cumplimiento técnico de los sistemas de información?*

***SITUACIÓN ENCONTRADA (Hallazgo):***

*Se identificó que la organización no cuenta con procedimientos formales y documentados para asegurar el cumplimiento de los derechos de propiedad intelectual.*

*La auditoría reveló que la organización no considera todos los riesgos asociados con la protección de los registros.*

*Se encontró que las medidas para proteger la información de datos personales no son suficientemente robustas.*

*La organización no realiza revisiones regulares para asegurar el cumplimiento con las leyes y reglamentaciones relacionadas con el uso de controles criptográficos.*

*Se observó que los directores no revisan de manera sistemática el cumplimiento de los procedimientos de procesamiento de información dentro de sus áreas de responsabilidad.*

*La organización no realiza revisiones periódicas del cumplimiento técnico de sus sistemas de información.*

|  |  |  |
| --- | --- | --- |
| *Nivel de Riesgo* | *page52image17611776Nivel de Prioridad* | *Nivel de Complejidad* |
| *ALTO* | *page52image17599872ALTA* | *MEDIA* |

*Recomendación:*

*18.1.2 Implementar procedimientos formales para asegurar la protección y cumplimiento de los derechos de propiedad intelectual.*

*18.1.3 Desarrollar e implementar políticas para la clasificación, almacenamiento y protección eficaz de registros.*

*18.1.4 Reforzar las medidas de protección de datos personales, incluyendo auditorías y capacitaciones regulares sobre privacidad.*

*18.1.5 Asegurar el cumplimiento con las leyes y reglamentaciones sobre el uso de la criptografía y realizar revisiones regulares.*

*18.2.2 Establecer un sistema más riguroso para revisiones regulares y garantizar el cumplimiento de las políticas y normas de seguridad.*

*18.2.3 Implementar herramientas automáticas para mejorar la eficiencia y precisión de las revisiones de cumplimiento técnico.*

***CONCLUSIONES Y RECOMENDACIONES GENERALES***

***Conclusiones:***

1. Se identificaron varias áreas donde las políticas de seguridad de la información y los procedimientos relacionados no están suficientemente documentados o implementados. Esto incluye la falta de documentación para la protección de derechos de propiedad intelectual, la gestión de registros y el cumplimiento de regulaciones sobre criptografía.
2. La organización carece de planes detallados y actualizados para garantizar la continuidad de la seguridad de la información durante situaciones adversas. La falta de verificación regular de estos controles puede comprometer la capacidad de la organización para enfrentar crisis efectivamente.
3. Existen deficiencias en la gestión de accesos a sistemas y en la protección física de los equipos informáticos. La ausencia de procedimientos formales para la asignación y revocación de derechos de acceso, junto con controles físicos insuficientes, aumenta el riesgo de accesos no autorizados y compromete la seguridad de la infraestructura tecnológica.
4. Las medidas para proteger datos personales y garantizar el cumplimiento con las leyes y regulaciones vigentes no son adecuadas. Esto incluye la falta de procedimientos para asegurar la privacidad de los datos y la insuficiencia en el seguimiento de las prácticas criptográficas.
5. La organización no realiza seguimientos adecuados a los proveedores ni mantiene programas de capacitación continua para el personal en materia de seguridad de la información. La falta de estas prácticas puede llevar a un aumento en los riesgos asociados con terceros y la falta de preparación del personal frente a amenazas emergentes.

***Recomendaciones:***

1. **Formalizar y Documentar Políticas y Procedimientos:**

**Desarrollar y documentar políticas claras** para la gestión de derechos de propiedad intelectual, la protección de registros y el uso de controles criptográficos.

**Implementar procedimientos formales** para asegurar que las políticas sean efectivas y se cumplan de manera consistente.

1. **Fortalecer la Gestión de Continuidad del Negocio:**

**Actualizar y mantener un plan de continuidad** detallado que incluya todos los aspectos de la seguridad de la información en situaciones adversas.

**Establecer un calendario de revisiones y pruebas regulares** para asegurar la eficacia de los controles de continuidad.

1. **Mejorar los Controles de Acceso y Seguridad Física:**

**Implementar procedimientos formales** para la asignación y revocación de derechos de acceso, y asegurar que se mantengan registros detallados.

**Reforzar los controles físicos** para proteger los equipos informáticos y garantizar que solo el personal autorizado tenga acceso a áreas seguras.

1. **Reforzar la Protección de Datos y el Cumplimiento Regulatorio:**

**Desarrollar políticas robustas** para la protección de datos personales y realizar auditorías periódicas para asegurar el cumplimiento.

**Revisar y actualizar regularmente** las prácticas criptográficas para alinearse con las leyes y regulaciones vigentes.

1. **Optimizar la Gestión de Proveedores y la Capacitación del Personal:**

**Realizar auditorías y seguimientos frecuentes** de los proveedores para asegurar el cumplimiento con los acuerdos de servicio.

**Implementar programas de capacitación continua** en seguridad de la información para todo el personal, actualizando los contenidos regularmente para reflejar las últimas amenazas y mejores prácticas.

***ANEXOS***

*Anexar papeles de trabajo*

*- Solicitudes de información (Ejemplo organigrama, perfiles de puestos, manual de politicas, contraros firmados, copia de inventarios de equipos, procedimientos de altas y bajas de usuarios, etc.) se elabora un cuadro ejemplo:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *#* | *Requerimiento Solicitado* | *Entrego* | | | *Observación* |
| *SI* | *NO* | *Parcial* |
| *1* | *Organigrama de Infotecnología* | *X* |  |  |  |
| *2* | *Perfiles de Puestos de Infotecnología* | *X* |  |  |  |
| *3* | *Diagrama de la Red Lan con información detallada (Servidores, IP, equipos de Comunicación, etc.)* | *X* |  |  |  |
| *4* | *Manual de Políticas de Seguridad* | *X* |  |  |  |
| *5* | *Manual de Análisis de Riesgos* |  | *X* |  | *Este documento no se ha elaborado* |
| *6* | *Acuerdos de Seguridad firmados con entidades* |  | *X* |  | *No existe* |
| *7* | *Copia de inventarios de activos* | *X* |  |  |  |
| *8* | *Documento de clasificación de información de acuerdo a su confidencialidad y criticidad* |  | *X* |  | *No existe* |
| *9* | *Plan de concientización de usuarios en seguridad de la información* |  | *X* |  | *No existe* |
| *10* | *Procedimiento formal para altas y bajas de empleados* | *X* |  |  | *Está en la política de Seguridad* |
| *11* | *Procedimiento formal para gestión de cambios en equipos de producción* |  | *X* |  | *No existe* |
| *12* | *Plan de Respuesta a Incidentes de Seguridad* |  | *X* |  | *No existe* |
| *13* | *Registro de Acceso a Sistemas y Aplicaciones* |  | *X* |  | *No existe* |
| *14* | *Procedimientos de Seguridad para el Teletrabajo* |  | *X* |  | *No existe* |
| *15* | *Auditorías Internas de Seguridad* |  | *X* |  | *No se han realizado auditorías internas formales* |
| *16* | *Registro y Gestión de Contraseñas* |  | *X* |  | *No existe* |
| *17* | *Procedimiento de Evaluación y Selección de Proveedores* |  | *X* |  | *No existe* |
| *18* | *Documentación de Controles de Seguridad Física* |  |  | *X* | *Parcialmente documentado* |
| *19* | *Plan de Continuidad del Negocio* |  | *X* |  | *No existe* |
| *20* | *Procedimientos de Protección de Datos Personales* |  | *X* |  | *No existe* |
| *21* | *Revisión de Cumplimiento Regulatorio* |  | *X* |  | *No existe* |
| *22* | *Procedimiento Formal para la Gestión de Medios Removibles* |  | *X* |  | *No existe* |
| *23* | *Revisión y Actualización de Políticas de Seguridad* |  | *X* |  | *No existe* |

*- Formatos de pruebas de consentimiento y cumplimiento*

*- Evidencias encontradas (pantallas, codigo malicioso, etc) – Aplica en auditoria en sitio*