SEGURIDAD DE LA INFORMACIÓN

EDICIÓN 2024

ELABORADO POR:

- Ing. Selva Argote Villaroel
- Mgr. Jimena Cecilia Lavayen Maldonado
- Unv. Rodrigo Leonardo Bautista Paganelli
- Unv. Fabian Israel Almendro Torrico

Dirección Universitaria de Evaluación y Acreditación

ÍNDICE

1. INTRODUCCIÓN.....1
1.1. Objetivo del Documento.....1
1.2. Alcance y Aplicabilidad.....1
1.3. Importancia de la Seguridad de la Información.....1
1.4. Costo del Manejo de la Seguridad de la Información.....1
2. MARCO NORMATIVO.....3
2.1. Conceptos Clave.....3
2.2. Normas Internacionales Aplicables.....4
2.2.1. ISO 27001.....4
2.2.2. ISO 27002.....4
2.2.3. ISO 27005.....4
2.3. Legislación Nacional Aplicable.....4
2.3.1. Ley 164 de Bolivia.....4
2.3.2. Reglamento de la OyM UMSS.....4
2.3.2.1. Políticas Específicas de la OyM para la Gestión de la Información.....5
2.4. Sanciones Nacionales e Internacionales.....5
2.4.1. Normas ISO.....5
2.4.2. Ley 164.....6
2.4.3. Código Penal Boliviano.....6
2.4.4. Código de Sistema Penal Boliviano.....6
3. PROPUESTA DE ACCIONES.....8
3.1. Clasificación de la Información.....8
3.1.1. Confidencialidad, Integridad y Disponibilidad.....8
3.1.1.1. Confidencialidad.....8
3.1.1.2. Integridad.....9
3.1.1.3. Disponibilidad.....9
3.2. Manejo de la Información y Dispositivos Nuevos.....10
3.3. Cadena de Custodia.....11
4. CONCLUSIÓN.....12
4.1. Relevancia de la Seguridad de la Información en los Procesos de Acreditación.....12
4.2. Relevancia de la Seguridad de la Información en la UMSS.....13
4.3. Manejo de la Información por los Pares Evaluadores.....13
4.4. Siguientes Pasos.....13
REFERENCIAS.....15

MANEJO Y SEGURIDAD DE LA INFORMACIÓN

PARA PROCESOS DE LA EVALUACIÓN EN LA UMSS

1. INTRODUCCIÓN

1.1. Objetivo del Documento

El presente documento tiene como objetivo proporcionar una guía integral sobre la seguridad de la información en la Universidad Mayor de San Simón (UMSS). Buscando establecer un marco claro para la implementación y gestión de políticas y prácticas que aseguren la protección adecuada de la información de los procesos de evaluación y acreditación dentro de la universidad. Ya que alinear estas prácticas con normas internacionales y legislación nacional es fundamental para garantizar la integridad, confidencialidad y disponibilidad de los datos y sistemas de información.

1.2. Alcance y Aplicabilidad

El alcance de este documento incluye todos los aspectos relacionados con la seguridad de la información dentro de la UMSS, abarcando tanto los sistemas tecnológicos como los procesos administrativos que manejan datos sensibles. Está dirigido a todo el personal administrativo, académico y estudiantil de la universidad, con el fin de sensibilizarlos sobre la importancia de la seguridad de la información y proporcionarles directrices claras para la protección de los datos.

1.3. Importancia de la Seguridad de la Información

La seguridad de la información es esencial para proteger los activos más valiosos de cualquier institución educativa: sus datos y su reputación. En el contexto de la UMSS, la seguridad de la información no solo asegura la protección de datos académicos y administrativos, sino que también resguarda la privacidad de estudiantes, personal y colaboradores. La implementación adecuada de medidas de seguridad ayuda a prevenir accesos no autorizados, pérdida de datos y daños a la infraestructura tecnológica, lo que contribuye a mantener la confianza de la comunidad universitaria y cumplir con las normativas legales y éticas. al ser los procesos de acreditacion y evaluacion colectores de la información de las unidades académicas, y al pasar por varios niveles de procesos, es primordial que todas las instancias conozcan estos lineamientos y políticas para garantizar la seguridad de la información dentro de las acreditaciones y las evaluaciones dando continuidad a estos proceso que son cíclicos.

1.4. Costo del Manejo de la Seguridad de la Información

Vivimos en una era de información masiva, donde la posesión y protección de datos se han convertido en sinónimo de poder. La digitalización y el uso generalizado de dispositivos móviles han traído enormes beneficios, empero asimismo han planteado desafíos significativos en términos de seguridad. La información que manejamos a diario, incluye datos cruciales que son esenciales para tomar decisiones estratégicas, proteger activos y garantizar la continuidad de las operaciones. De hecho, los datos se han convertido en uno de los activos más valiosos para cualquier organización, ya sea una universidad, una empresa, o un gobierno.

Los datos personales, financieros, médicos, la propiedad intelectual, y otros tipos de información confidencial son objetivos atractivos para los ciberdelincuentes, ya que contienen información sensible que, en manos equivocadas, puede ser utilizada para el robo de identidad, chantaje, fraudes,

y acceso no autorizado a cuentas bancarias, correos electrónicos, o sistemas empresariales. El acceso no autorizado a la información y datos es particularmente peligroso, ya que la alteración o manipulación de los datos puede afectar decisiones críticas, especialmente en sectores sensibles.

Las consecuencias de la pérdida o el robo de datos son graves tanto a nivel personal como organizacional. Para los individuos, la exposición de datos personales puede llevar al robo de identidad, pérdida financiera, y daños irreparables a su reputación. Para la Universidad, las repercusiones pueden ser aún más devastadoras. Una violación de datos puede resultar en pérdidas financieras significativas debido a multas regulatorias, demandas legales, y la pérdida de confianza por parte de la comunidad universitaria y la sociedad en general. Además, la exposición de datos privados o propiedad intelectual puede debilitar la competitividad de la Universidad, afectando su posición en los diferentes rankings académicos existentes.

La pérdida de datos igualmente puede interrumpir las operaciones diarias de la Universidad, afectando la continuidad de las operaciones y generando costos adicionales para recuperar y proteger la información comprometida. En el caso de sectores críticos, como la información histórica o las finanzas, los datos alterados o manipulados pueden llevar a decisiones erróneas con consecuencias potencialmente catastróficas.

Además de las amenazas externas, al mismo tiempo existen riesgos internos. Los errores humanos, como el envío de información confidencial a destinatarios incorrectos o la eliminación accidental de archivos importantes, pueden comprometer la seguridad de los datos. Por consiguiente, la protección de los datos no solo es una cuestión de tecnología, sino de concienciación y gestión adecuada de los riesgos.

Es importante reconocer que la gestión efectiva de la seguridad de la información conlleva ciertos costos, que pueden clasificarse en dos categorías principales:

- **Costos Directos**: Que incluyen la inversión en tecnologías de seguridad como firewalls, sistemas de detección de intrusiones, herramientas de cifrado y software antivirus. Además, se deben considerar los gastos asociados con la contratación de personal especializado en seguridad de la información y la realización de auditorías y evaluaciones de riesgos.
- **Costos Indirectos**: Que abarcan el tiempo y los recursos dedicados a la capacitación del personal, la implementación de políticas de seguridad, y la gestión continua de incidentes de seguridad. Aunque estos costos pueden parecer elevados, son una inversión esencial para proteger la integridad de la información y prevenir incidentes que podrían resultar en pérdidas financieras y de reputación significativas.

Incorporar un enfoque proactivo hacia la seguridad de la información no solo minimiza los riesgos asociados con posibles brechas de seguridad, sino que también proporciona una base sólida para el crecimiento y la innovación tecnológica en la UMSS. La inversión en seguridad, debe ser vista como un componente crucial de la estrategia institucional para asegurar un entorno educativo seguro y confiable.

2. MARCO NORMATIVO

2.1. Conceptos Clave

¿Qué es una Política? Es un conjunto formal de principios, directrices o normas que una organización adopta para guiar las decisiones y acciones en relación con un tema específico. En términos de seguridad de la información, una política es un documento que establece las expectativas y requisitos relacionados con la protección de la información, detallando cómo se deben gestionar, proteger y usar los recursos de información.

¿Qué es una ISO? ISO (International Organization for Standardization) es una organización internacional no gubernamental que desarrolla y publica normas internacionales. Las normas ISO, abarcan una amplia gama de sectores y disciplinas, proporcionando directrices y especificaciones para asegurar calidad, seguridad y eficiencia en sentido amplio. En el contexto de la seguridad de la información, normas como la **ISO 27001** (primera edición en 2005, revisada en 2013 y 2022), **ISO 27002** (primera edición en 2007, revisada en 2013 y 2022) y **ISO 27005** (primera edición en 2008, revisada en 2011 y 2022), establecen marcos y directrices para la implementación de sistemas de gestión de seguridad de la información, la gestión de riesgos y la protección de datos sensibles.

¿Qué es una Cadena de Custodia? Proceso de documentación y control que asegura que la información o evidencia se mantenga íntegra y sin alteraciones durante su transferencia o almacenamiento. En el ámbito de la seguridad de la información, la cadena de custodia implica mantener un registro detallado de todas las personas y procesos que manejan la información desde su origen hasta su destino final. Eso incluye la documentación de cada transferencia de información, así como las medidas de seguridad implementadas para protegerla durante el proceso.

¿Qué es un Parche de Seguridad? Actualización de software diseñada para corregir vulnerabilidades de seguridad que han sido identificadas en un sistema o aplicación. Los parches de seguridad son importantes para proteger los sistemas de información contra amenazas y ataques cibernéticos. Se aplican para solucionar fallos o debilidades en el código que podrían ser explotados por atacantes, asegurando así que el sistema mantenga su integridad y funcionalidad. La implementación regular de parches de seguridad es una práctica clave en la gestión de la seguridad de la información.

2.2. Normas Internacionales Aplicables

2.2.1. ISO 27001

La ISO 27001 establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información mediante la implementación de un conjunto de controles de seguridad.

2.2.2. ISO 27002

La ISO 27002 proporciona directrices detalladas para la gestión de la seguridad de la información, incluyendo controles específicos que pueden ser implementados para proteger la información sensible.

2.2.3. ISO 27005

La ISO 27005 se centra en la gestión de riesgos relacionados con la seguridad de la información. Proporciona un enfoque sistemático para identificar, evaluar y tratar los riesgos, asegurando así la protección adecuada de la información.

2.3. Legislación Nacional Aplicable

2.3.1. Ley 164 de Bolivia

La Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, promulgada en 2011, regula las telecomunicaciones y tecnologías de información en Bolivia. Entre sus principios destacan:

- **Inviolabilidad (Art. 5):** Protección de las comunicaciones privadas.
- **Calidad (Art. 5):** Asegurar la integridad de la información.
- **Continuidad (Art. 5):** Garantizar el acceso continuo a la información.
- **Protección del Medio Ambiente (Art. 5):** Asegurar que las actividades relacionadas con las tecnologías de información no dañen el medio ambiente.

2.3.2. Reglamento de la OyM UMSS

La Oficina de Organización y Métodos (OyM) de la UMSS establece un marco normativo interno que complementa y apoya el cumplimiento de normas internacionales y leyes nacionales en la gestión de la información. Estos reglamentos definen los procedimientos y responsabilidades para la implementación y monitoreo de las políticas de seguridad de la información en la universidad.

Algunos Documentos:

- **Reglamento de Administración de Almacenes de la UMSS:** Define los procedimientos para la adquisición, configuración y administración de nuevos equipos tecnológicos, asegurando que se mantengan los estándares de seguridad durante la gestión de activos. Aprobado en 2015.

- **Reglamento del Personal de la UMSS:** Establece las responsabilidades del personal en la gestión de la información, incluyendo el control de acceso y la seguridad de la información. Aprobado en 2018.

- **Reglamento de Control y Seguimiento de Objetivos (POA):** Alinea los sistemas y software utilizados con los objetivos estratégicos de la universidad, asegurando que las prácticas de seguridad estén en consonancia con los objetivos institucionales. Aprobado en 2017.

2.3.2.1. Políticas Específicas de la OyM para la Gestión de la Información

Las políticas de la OyM detallan los procedimientos específicos para la implementación de controles de seguridad y la gestión de la información en la UMSS. Estas políticas incluyen:

- **Procedimientos para la Configuración Segura de Dispositivos:** Aseguran que todos los dispositivos nuevos sean configurados de acuerdo con las mejores prácticas de seguridad para proteger la información de la universidad. Implementados en 2019.

- **Controles de Acceso y Privilegios:** Establecen cómo se deben asignar y gestionar los permisos de acceso para garantizar que solo el personal autorizado tenga acceso a la información sensible. Implementados en 2018.

- **Procedimientos de Actualización y Mantenimiento de Software:** Definen cómo se deben implementar y gestionar las actualizaciones de software para mantener la seguridad y funcionalidad de los sistemas. Implementados en 2020.

- **Gestión de la Cadena de Custodia:** Establecen procedimientos para el registro y la protección de la información durante su transferencia dentro de la universidad. Implementados en 2021.

2.4. Sanciones Nacionales e Internacionales

2.4.1. Normas ISO

Las normas ISO, como la ISO 27001, ISO 27002 y ISO 27005, establecen estándares internacionales para la gestión de la seguridad de la información. Sin embargo, las sanciones por incumplimiento de estas normas no se imponen directamente por la organización que las publica (ISO). En lugar de sanciones, las consecuencias suelen estar relacionadas con:

- **Pérdida de Certificación:** Si una organización no cumple con los requisitos de la norma ISO 27001, puede perder su certificación, lo que puede afectar su reputación y su capacidad para hacer negocios, especialmente con clientes que requieren cumplimiento con estándares internacionales.
- **Impacto en la Competitividad:** La falta de certificación puede reducir la competitividad de la organización en mercados donde el cumplimiento con normas internacionales es un criterio de selección importante.
- **Riesgos Operacionales:** El incumplimiento con las mejores prácticas establecidas por estas normas puede llevar a incidentes de seguridad, pérdidas de datos y daños a la reputación, lo que a su vez puede tener repercusiones financieras y legales.

2.4.2. Ley 164

La Ley 164 de Bolivia, que regula las telecomunicaciones, al igual establece normas relacionadas con la protección de datos y la seguridad de la información. Las sanciones por incumplimiento pueden incluir:

- **Multas Económicas:** La ley puede imponer multas a las organizaciones que no cumplan con las obligaciones establecidas, tales como las relacionadas con la protección de datos personales.
- **Sanciones Administrativas:** Estas pueden incluir la suspensión temporal o definitiva de servicios, licencias o permisos relacionados con telecomunicaciones y servicios de internet.
- **Responsabilidad Legal:** En caso de violaciones graves, las personas responsables o las organizaciones pueden enfrentar acciones legales, que pueden incluir demandas o procedimientos judiciales.
- **Daño a la reputación:** El incumplimiento con la ley puede llevar a la pérdida de confianza por parte de clientes y socios, afectando negativamente la reputación y la posición en el mercado.

2.4.3. Código Penal Boliviano

En Bolivia, las sanciones relacionadas con el incumplimiento de normas de seguridad de la información y protección de datos pueden encontrarse en el Código Penal, en su capítulo XI sobre delitos informáticos, establece sanciones para actividades ilícitas relacionadas con la seguridad de la información. Algunas de las infracciones incluyen:

- **Artículo 363 bis.-** (Manipulación informática).

  El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

- **Artículo 363 ter.-** (Alteración, acceso y uso indebido de datos informáticos).-

  El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

2.4.4. Código de Sistema Penal Boliviano

En Bolivia, el Código de Sistema Penal y otras leyes complementarias, pueden sancionar infracciones relacionadas con la seguridad de la información y la protección de datos en su capítulo VIII, sección 4 sobre delitos informáticos. Las sanciones específicas para el incumplimiento de normas de seguridad y protección de datos incluyen:

- **ARTÍCULO 245. (MANIPULACIÓN INFORMÁTICA)**. **I**. La persona que, con intención de obtener beneficio indebido, para sí o para tercero, manipule un procesamiento de las tecnologías de información y comunicación, para la transferencia de datos o información que conduzca a un resultado incorrecto o evite un proceso tal, cuyo resultado habría sido correcto, será sancionada con prisión de dos (2) a cuatro (4) años y multa sancionadora de doscientos cincuenta y un (251) a cuatrocientos (400) días.

  II. Si como resultado de las conductas descritas en el Parágrafo precedente, se ocasiona una transferencia patrimonial en perjuicio de tercero, se impondrá prisión de dos (2) a cuatro (4) años y reparación económica.

- **ARTÍCULO 246. (USO INDEBIDO DE DATOS AJENOS EN MEDIOS INFORMÁTICOS). I.** La persona que, sin autorización, con intención de obtener beneficio indebido o con el fin de afectar la imagen y dignidad de la víctima, utilice los datos o información confidencial ajena, sea personal, institucional o financiera, consignada en medios informáticos o electrónicos o suplante la identidad de otra a través de un medio electrónico o digital generando perjuicio al titular de la información o a un tercero, será sancionada con prisión de dos (2) a cuatro (4) años y reparación económica.

  II. La sanción será agravada a prisión de tres (3) a seis (6) años y reparación económica, cuando la víctima sea niña, niño o adolescente.

- **ARTÍCULO 247. (ACCESO ILEGÍTIMO A SISTEMAS).** La persona que, sin estar autorizada o excediendo la autorización que posea, deliberadamente acceda a todo o parte de un sistema informático con el fin de apoderarse de los datos, publicarlos u ocasionar perjuicio, será sancionada con prisión de dos (2) a cuatro (4) años y reparación económica.
- **ARTÍCULO 248. (ATAQUE A LA INTEGRIDAD DE LOS DATOS).** La persona que deliberadamente, sin estar autorizada o excediendo la autorización que posea, se apodere, utilice, dañe, modifique o suprima datos o información consignada en medios informáticos o electrónicos, ocasionando perjuicio al titular de la información, será sancionada con prisión de dos (2) a cuatro (4) años y reparación económica.
- **ARTÍCULO 249. (ATAQUE A LA INTEGRIDAD DEL SISTEMA).** La persona que de manera deliberada obstaculice el funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, será sancionada con prisión de dos (2) a cuatro (4) años y reparación económica.
- **ARTÍCULO 250. (AGRAVANTES EN DELITOS INFORMÁTICOS).** La sanción prevista en cada uno de los Artículos precedentes, será agravada a prisión de tres (3) a seis (6) años y reparación económica, cuando:
  - El sistema o los datos informáticos pertenecen a una entidad estatal, un proveedor de servicios de salud o un proveedor de servicios financieros.
  - Los datos ilegítimamente obtenidos sean transferidos, a cualquier título, a terceros.
  - La persona autora tenga el deber de resguardar el sistema o los datos informáticos.
  - La persona autora sea servidora o servidor público.
  - La persona autora abusó de un vínculo sentimental, afectivo, emocional o de confianza para cometer el hecho.

3. PROPUESTA DE ACCIONES

3.1. Clasificación de la Información

La UMSS, debe implementar políticas de clasificación de la información para proteger adecuadamente los datos según su sensibilidad. Las categorías pueden incluir:

- **Información Pública:** Datos accesibles al público general.
- **Información Interna:** Información restringida al personal de la UMSS.
- **Información Confidencial:** Datos que requieren protección adicional debido a su sensibilidad.
- **Información Secreta:** Información altamente sensible con acceso estrictamente controlado.

Respaldo:

- **ISO 27001:** Anexo A.8.2 sobre la clasificación de la información para asegurar que los activos de información reciban un nivel adecuado de protección. (Neira, ISO27000.ES, 2005)
- **Ley 164 de Bolivia:** Principio de inviolabilidad (Art. 5) para asegurar que la información confidencial se mantenga protegida. (ESTADO PLURINACIONAL DE BOLIVIA, 2011)

3.1.1. Confidencialidad, Integridad y Disponibilidad

3.1.1.1. Confidencialidad

Se debe garantizar que solo las personas autorizadas tengan acceso a la información sensible. Esto puede lograrse mediante:

- **Controles de acceso basados en roles:** Asignar permisos según las funciones y responsabilidades del personal.
- **Cifrado de datos:** Proteger la información confidencial durante la transmisión y almacenamiento.

Respaldo:

- **ISO 27002:** Sección 9.1 sobre el control de acceso y sección 10.1 sobre el uso de controles criptográficos. (GrouP, 2017)
- **Ley 164 de Bolivia:** Principio de inviolabilidad (Art. 5) para asegurar que las comunicaciones y la información privada estén protegidas. (ESTADO PLURINACIONAL DE BOLIVIA, 2011)

3.1.1.2. Integridad

La información debe ser precisa y estar completa. Para mantener la integridad de los datos:

- **Controles de versión:** Asegurar que se mantenga un registro de todas las modificaciones realizadas a la información.
- **Verificación de datos:** Implementar mecanismos de verificación para detectar y corregir errores.

Respaldo:

- **ISO 27001:** Anexo A.14 sobre el control de cambios y la integridad del sistema. (Neira, ISO27000.ES, 2005)
- **Ley 164 de Bolivia:** Principio de calidad (Art. 5) para asegurar la precisión y completitud de la información. (ESTADO PLURINACIONAL DE BOLIVIA, 2011)

3.1.1.3. Disponibilidad

La información debe estar disponible cuando se necesite. Para asegurar la disponibilidad:

- **Procedimientos de respaldo y recuperación:** Establecer procesos regulares de copia de seguridad y planes de recuperación ante desastres.
- **Redundancia de sistemas:** Implementar sistemas redundantes para evitar interrupciones en el acceso a la información.

Respaldo:

- **ISO 27001:** Anexo A.17 sobre la planificación de la continuidad del negocio y la recuperación de desastres. (Neira, ISO27000.ES, 2005)
- **Ley 164 de Bolivia:** Principio de continuidad (Art. 5) para garantizar el acceso continuo a la información. (ESTADO PLURINACIONAL DE BOLIVIA, 2011)

3.2. Manejo de la Información y Dispositivos Nuevos

Al recibir dispositivos nuevos, se deben seguir procedimientos específicos para asegurar su configuración segura y cumplimiento con las políticas de seguridad de la UMSS. Estos procedimientos incluyen:

- **Configuración segura:** Asegurar que todos los dispositivos nuevos estén configurados con las medidas de seguridad adecuadas desde el momento en que el dispositivo es puesto en operación. Esto incluye:
    - Desactivar servicios no necesarios y eliminar software preinstalado que no sea esencial para la operación.
    - Configurar el cifrado de datos en el disco para proteger la información en reposo.
    - Instalar y mantener actualizado software de protección contra virus y malware.
    - Asegurar que las actualizaciones de seguridad se apliquen de manera oportuna para proteger contra vulnerabilidades conocidas.

  Respaldo:

  - ISO 27002, sección 9.2, sobre la gestión de activos y la configuración segura de los dispositivos. (GrouP, 2017)
  - Reglamento de Administración de Almacenes de la UMSS, que establece procedimientos para la adquisición y configuración de nuevos equipos tecnológicos. (Departamento de Organización y Métodos, 2008)

- **Control de acceso:** Implementar controles para asegurar que solo el personal autorizado pueda acceder a los dispositivos o información en cualquier formato.

  Respaldo:

  - ISO 27001, Anexo A.9, sobre el control de acceso y la gestión de privilegios de usuario. (Neira, ISO27000.ES, 2005)
  - Reglamento del Personal de la UMSS, que define las responsabilidades del personal y los controles de acceso a la información. (Celier, 1984)

- **Actualización de software:** Garantizar que todos los dispositivos estén actualizados con los últimos parches de seguridad.

  Respaldo:

  - ISO 27002, sección 12.6, sobre la gestión de actualizaciones y parches de software. (Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la Información, 2017, pág. 70)
  - Reglamento de Control y Seguimiento de Objetivos (POA) de la UMSS, que asegura que los sistemas y software utilizados están alineados con los objetivos estratégicos de la universidad. (Métodos, 2007)

3.3. Cadena de Custodia

La cadena de custodia es crucial para mantener la integridad de la información durante su transferencia. Los procedimientos deben incluir:

- **Registro de transferencia:** Mantener un registro detallado de todas las transferencias de información.

  Respaldo:

  - ISO 27002, sección 8.3, sobre la gestión de activos y el registro de transferencias. (Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la Información, 2017, pág. 31)
  - Manual de Procedimientos para la Extensión de Títulos y Certificados de la UMSS, que detalla los registros necesarios para la emisión y transferencia de títulos y certificados. (ISSU, s.f.)

- **Responsabilidad clara:** Definir claramente las responsabilidades de cada individuo en el proceso de transferencia y asignación de información como activo.

  Respaldo:

  - Ley 164, Art. 5 sobre la responsabilidad y la inviolabilidad de las comunicaciones. (ESTADO PLURINACIONAL DE BOLIVIA, 2011)
  - Reglamento del Personal de la UMSS, que define claramente las responsabilidades del personal en la gestión de la información. (Celier, 1984)

- **Medidas de seguridad durante la transferencia:** Asegurar que la información esté protegida adecuadamente durante la transferencia.

  Respaldo:

  - ISO 27001, Anexo A.13, sobre la seguridad en las comunicaciones y la transferencia de información. (Neira, ISO27000.ES, 2005)

  Respaldo:

  - ISO 27002, Sección 8.3 sobre la gestión de activos y el registro de transferencias. (Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la Información, 2017, pág. 31)
  - Ley 164 de Bolivia, Art. 5 sobre la responsabilidad y la inviolabilidad de las comunicaciones. (ESTADO PLURINACIONAL DE BOLIVIA, 2011)
  - Reglamento de Administración de Almacenes de la UMSS, que asegura la protección adecuada de los bienes durante su traslado. (Departamento de Organización y Métodos, 2008)

4. CONCLUSIÓN

4.1. Relevancia de la Seguridad de la Información en los Procesos de Acreditación

La seguridad de la información desempeña un rol central en el proceso de acreditación, que evalúa el cumplimiento de los estándares nacionales e internacionales en cuanto a la calidad de los procesos y resultados de una unidad en el ámbito universitario - académico. Al adherirse a normas como la ISO 27001 y la ISO 27002, la UMSS reafirma su compromiso con las mejores prácticas en la gestión de la seguridad de la información. Esto es primordial para mantener la confianza de las agencias acreditadoras, como el CEUB, y para asegurar que la universidad cumpla con los estrictos requisitos de acreditación de esta y otras entidades relevantes. Además, una protección adecuada de los datos previene incidentes que podrían comprometer la reputación de la universidad y afectar su posición en los rankings académicos.

En un entorno cada vez más digitalizado, la implementación de medidas robustas de seguridad informática es clave para prevenir amenazas, mitigar riesgos y fortalecer la resiliencia de la UMSS frente a posibles incidentes de seguridad. La confianza de la comunidad y la continuidad operativa dependen de estas acciones, y la adopción de normas internacionales asegura que se sigan los mejores estándares de protección de la información.

Dado que en la UMSS los cambios de personal son frecuentes, es vital establecer y seguir políticas claras para el manejo y la transferencia de información. Estas políticas deben incluir:

- **Clasificación de la Información**: Asegurar que todos los datos sean clasificados adecuadamente según su nivel de confidencialidad (Confidencial, Restringido, Uso Interno, Público).
- **Cadena de Custodia**: Mantener una cadena de custodia estricta para que los datos no se pierdan ni se manipulen indebidamente durante cualquier cambio de personal o reasignación de dispositivos.
- **Manejo de Dispositivos Nuevos**: Implementar procedimientos estándar para garantizar que cualquier dispositivo nuevo se integre de manera segura al sistema, sin riesgo de pérdida de información.
- **Transferencia Segura de Información**: Seguir protocolos específicos cuando el personal se retira o se reasignan dispositivos, asegurando que toda la información relevante sea transferida de manera segura y accesible para la siguiente persona en el cargo, evitando el reinicio innecesario de procesos.

En resumen, la rigurosa implementación de políticas de seguridad de la información no solo protege los activos más valiosos de la universidad, sino que igualmente respalda la calidad de los procesos de evaluación y acreditación. De este modo, la UMSS continuará cumpliendo con los más altos estándares de excelencia educativa, estando preparada para enfrentar los desafíos de la era digital.

4.2. Relevancia de la Seguridad de la Información en la UMSS

La seguridad de la información es esencial para la Universidad Mayor de San Simón (UMSS). Dado el valor y la sensibilidad de la información manejada, su protección es vital no sólo para salvaguardar los derechos y la privacidad de los datos académicos y administrativos, sino también para proteger los activos y la reputación de la universidad. Esto garantiza el cumplimiento de leyes y regulaciones, como el Código Penal y el Código de Sistema Penal de Bolivia, que imponen sanciones severas para quienes violen la integridad de los sistemas informáticos y los datos que manejan.

La UMSS debe fomentar una cultura organizacional en la que la seguridad de la información sea vista como una responsabilidad compartida. El personal debe estar capacitado para manejar los datos de acuerdo con las políticas establecidas, comprendiendo la importancia de la conservación y protección de la información.

4.3. Manejo de la Información por los Pares Evaluadores

Es importante destacar que los pares evaluadores, en el marco del proceso de acreditación, manejan información crítica a lo largo de diversas etapas, tanto de manera virtual como física. Antes de la visita, los pares realizan un análisis exhaustivo de documentos, como el Informe de Autoevaluación y otros anexos, los cuales son accesibles a través de plataformas en la nube. Durante la visita, los evaluadores revisan documentación adicional de manera presencial y coordinan con el Técnico Coordinador la elaboración de informes cruciales, como el Informe Resumen de Salida y el Informe de Conformidad de Visita. Posteriormente, se encargan de la elaboración y envío de informes preliminares y finales, respetando los plazos establecidos. En todo este proceso, los pares evaluadores aplican sus propios métodos y protocolos para garantizar la seguridad y confidencialidad de la información manejada, alineándose con la importancia que la seguridad de la información tiene en la Universidad Mayor de San Simón (UMSS).

4.4. Siguientes Pasos

Para fortalecer la gestión de la seguridad de la información y apoyar los procesos de acreditación, se recomienda implementar las siguientes acciones a futuro:

- **Desarrollo e Implementación de Nuevas Políticas**: Elaborar y poner en práctica políticas adicionales para abordar las nuevas amenazas y desafíos en seguridad de la información. Estas políticas, deben incluir directrices sobre la protección de datos en entornos emergentes y el uso de tecnologías avanzadas.
- **Capacitación Continua del Personal**: Realizar programas de formación periódica para el personal administrativo, académico y estudiantil sobre las mejores prácticas en seguridad de la información. Esta capacitación debe enfocarse principalmente en la importancia de la protección de datos y la correcta aplicación de las políticas y procedimientos establecidos.
- **Auditorías y Evaluaciones Periódicas**: Establecer un calendario para la realización de auditorías internas y evaluaciones de riesgos de manera regular. Esto permitirá identificar y corregir vulnerabilidades antes de que puedan ser explotadas, y asegurará que los controles de seguridad permanezcan efectivos y actualizados.

- **Actualización de Sistemas y Tecnologías**: Asegurar que la totalidad de los sistemas tecnológicos y software utilizados en la UMSS se mantengan actualizados con los últimos parches de seguridad y mejoras. La implementación de tecnologías avanzadas, como soluciones de inteligencia artificial para la detección de amenazas, puede fortalecer la defensa contra ciberataques.
- **Monitoreo Continuo de Incidentes**: Implementar sistemas de monitoreo continuo para la detección y respuesta rápida a incidentes de seguridad. Un enfoque proactivo en la gestión de incidentes ayudará a mitigar el impacto de cualquier brecha de seguridad y a mantener la integridad de los datos.

REFERENCIAS

Celier, C. L. (1984). *Reglamento del Personal de la UMSS*. Obtenido de https://www.fce.umss.edu.bo/webpage/sites/default/files/2024-06/REGLAMENTO%20DEL%20PERSONAL%20DE%20LA%20UMSS.pdf

Departamento de Organización y Métodos, U. (Octubre de 2008). *REGLAMENTO ADMINISTRACIÓN DE ALMACENES UMSS*. Obtenido de https://www.fce.umss.edu.bo/webpage/sites/default/files/2024-06/REGLAMENTO%20ADMINISTRACION%20DE%20ALMACENES%20DE%20LA%20UMSS.pdf

ESTADO PLURINACIONAL DE BOLIVIA, G. O. (08 de Agosto de 2011). *GACETA OFICIAL*. Obtenido de http://www.gacetaoficialdebolivia.gob.bo/edicions/view/287NEC

Codigo Penal Boliviano. (16 de Julio de 2022). Obtenido de Capítulo XI Delitos Informaticos https://facilitacionlegal.com/wp-content/uploads/2023/05/Codigo-Penal.pdf

Código de Sistema Penal Boliviano. (15 de Diciembre de 2017). Obtenido de Capitulo VIII, Seccion 4 Delitos Informaticos https://oig.cepal.org/sites/default/files/2017_cspnuevo_bol.pdf

GrouP, E. I. (31 de Agosto de 2017). *Norma ISO 27002: control de accesos*. Obtenido de Anexo 9 - ISO 27002: https://www.pmg-ssi.com/2017/08/norma-iso-27002-control-de-accesos/

ISSU. (s.f.). *UMSS - Manual procedimientos extender titulos y certificados*. Obtenido de https://issuu.com/fach-umss/docs/manual_procedimientos_extender_titu

Métodos, D. d. (2007). *REGLAMENTO - CONTROL SEGUIMIENTO Y EVALUACION DE OBJETIVOS (POA) UMSS*. Obtenido de https://www.fce.umss.edu.bo/webpage/sites/default/files/2024-06/REGLAMENTO%20-%20CONTROL%20SEGUIMIENTO%20Y%20EVALUACION%20DE%20OBJETIVOS%20%28POA%29%20UMSS%202007.PDF

Neira, A. L. (01 de Agosto de 2005). *ISO27000.ES*. Obtenido de Anexo 8 - ISO 27001: https://www.iso27000.es/iso27002_8.html

Neira, A. L. (01 de Agosto de 2005). *ISO27000.ES*. Obtenido de Anexo 14 - ISO 27001: https://www.iso27000.es/iso27002_14.html

Neira, A. L. (01 de Agosto de 2005). *ISO27000.ES*. Obtenido de Anexo 17 ISO - 27001: https://www.iso27000.es/iso27002_17.html

Neira, A. L. (01 de Agosto de 2005). *ISO27000.ES*. Obtenido de Anexo 9 - ISO 27001: https://www.iso27000.es/iso27002_9.html

Neira, A. L. (Agosto de 2005). *ISO27000.ES*. Obtenido de Anexo 13 - ISO 27001: https://www.iso27000.es/iso27002_13.html

Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la Información. (Mayo de 2017). Obtenido de Sección 12.6 - ISO 27002: https://static.eoi.es/inline/une-en_iso-iec_27002_norma_mincotur.pdf