REF.: APRUÉBESE MATRIZ DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

DECRETO ALCALDICIO N° 1490

SANTO DOMINGO, 27-07-2023

VISTOS

1. Ley N° 18.695 de fecha 31.03.1988, Ministerio del Interior, ley orgánica constitucional de municipalidades, refundida por Decreto con Fuerza de Ley N° 1 de fecha 26.07.2006, Ministerio del Interior; Subsecretaría de Desarrollo Regional y Administrativo, fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.695, orgánica constitucional de municipalidades;
2. La sentencia de proclamación de Alcaldes dictada por el Tribunal Electoral Regional de Valparaíso, Rol Nº 299-2021, numeral 8º), letra C), de fecha 28 de junio de 2021, que declara como alcalde definitivamente electo en la Comuna de Santo Domingo al Sr. Dino Lotito Flores.
3. El Decreto Alcaldicio N° 800, de fecha 29 de junio de 2021, por el cual asumo como Alcalde de la Ilustre Municipalidad de Santo Domingo, por el período 2021-2024.
4. El Decreto Alcaldicio N° 829, de 31 de mayo de 2022, que aprueba el texto refundido de Reglamento Interno Municipal de la Ilustre Municipalidad de Santo Domingo, en particular en lo referido al ARTÍCULO 29, SOBRE LAS SUBROGANCIAS, en virtud del cual el Administrador Municipal Francisco Devia Castro, subroga al Alcalde Dino Lotito Flores, por encontrarse con feriado legal, desde el 11 al 18 de julio del año en curso.
5. Ley N° 19.628 de fecha 28.08.1999, Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada;
6. Ley N° 19.653 de fecha 14.12.1999, Ministerio Secretaría General de la Presidencia, sobre probidad administrativa aplicable de los órganos de la administración del estado;
7. Ley N° 19.799 de fecha 12.04.2002, Ministerio de Economía, Fomento y Reconstrucción; Subsecretaría de Economía, Fomento y Reconstrucción, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma;
8. Ley N° 19.880 de fecha 29.05.2003, Ministerio Secretaría General de la Presidencia, establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado;
9. Ley N° 20.285 de fecha 20.08.2008, Ministerio Secretaría General de la Presidencia, sobre acceso a la información pública;
10. Ley N° 20.730 de fecha 08.03.2014, Ministerio Secretaría General de la Presidencia, que regula el lobby y las gestiones que representen intereses particulares ante las autoridades y funcionario;
11. Ley N° 20.880 de fecha 05.01.2016, Ministerio Secretaría General de la Presidencia, sobre probidad en la función pública y prevención de los conflictos de intereses;
12. Ley N° 21.180 de fecha 11.11.2019, Ministerio Secretaría General de la Presidencia, Transformación Digital del Estado;
13. Ley N° 21.464 de fecha 09.06.2022, Ministerio Secretaría General de la Presidencia, modifica diversos cuerpos legales en materia de Transformación Digital del Estado;

14. Decreto Alcaldicio N° 729 de fecha 11.05.2022, apruébese políticas de gestión de las tecnologías de la información y la transformación digital de la I. Municipalidad de Santo Domingo;
15. Decreto Alcaldicio N° 2047 de fecha 23.12.2022, apruébese reglamento sobre la seguridad de la información y gestión de riesgos TI de la I. Municipalidad de Santo Domingo.
16. Decreto Alcaldicio N° 2102 de fecha 30.12.2022, aprueba programa de mejoramiento de la gestión municipal para el año 2023.
17. El Decreto Alcaldicio N° 829 del 31 de mayo de 2022, que aprueba el texto refundido de Reglamento Interno Municipal de la Ilustre Municipalidad de Santo Domingo, en particular en lo referido al artículo 29, sobre las subrogancias, en virtud del cual Don Francisco Devia Castro, Administrador Municipal, subroga al alcalde don Dino Lotito Flores, por encontrarse éste haciendo uso de feriado legal desde el día martes 25 al viernes 28 de julio del año 2023, ambas fechas inclusive.

CONSIDERANDO

1. Que, para cumplir con el objetivo de la Ley de Transformación Digital de hacer operativo el funcionamiento administrativo de las diversas Unidades Municipales de manera coordinada, en beneficio del cumplimiento de objetivos públicos y actos administrativos decisorios sobre distintas materias de competencia municipal, a fin de dar ejecución a principios públicos de celeridad, de conclusión, de economía procedimental, y otros que informan el ámbito público en general, y de gestión municipal en particular.
2. Que, de acuerdo a lo establecido en el reglamento municipal sobre la gestión de la seguridad de la información y los riesgos TI, el Departamento de Informática y Gobierno Electrónico mantendrá actualizada anualmente una matriz de riesgos que contenga la ponderación de cada uno de estos y su medición correspondiente.
3. Que, urge la necesidad de contar con instrumentos de gestión actualizados que integren metas, decisiones y acciones que aborden problemáticas y su estrategia para alcanzar su resolución.

DECRETO

1. **APRUÉBESE** la matriz de riesgos en seguridad de la información de la I. Municipalidad de Santo Domingo según indica lo siguiente:

MATRIZ DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN DE LA I. MUNICIPALIDAD DE SANTO DOMINGO

Introducción:

El presente documento tiene como objetivo proporcionar una metodología clara y estructurada para la generación de una matriz de riesgos en seguridad de la información.

En un entorno cada vez más interconectado y dependiente de los sistemas y tecnologías de la información, la protección de la información se ha vuelto fundamental para garantizar la continuidad y la confidencialidad de las operaciones empresariales.

La seguridad de la información abarca un conjunto de medidas, políticas y controles diseñados para proteger la confidencialidad, integridad y disponibilidad de los activos de información. Sin embargo, identificar y evaluar los riesgos asociados a la seguridad de la información es un paso crucial para diseñar e implementar estrategias de mitigación efectivas.

En este contexto, la generación de una matriz de riesgos se convierte en una herramienta fundamental. La matriz de riesgos permite identificar, evaluar y priorizar los riesgos potenciales a los que está expuesta la información en una municipalidad. Proporciona una visión clara y estructurada de los riesgos, lo que facilita la toma de decisiones informadas y la asignación de recursos adecuados para su gestión.

Este documento presenta una metodología basada en las mejores prácticas y los estándares reconocidos internacionalmente, como la norma ISO 27000. La norma ISO 27000 proporciona un marco de referencia completo para la gestión de la seguridad de la información, estableciendo principios y directrices que nos ayudarán en la generación de la matriz de riesgos. Además, se utilizará la norma ISO 31000, que nos brinda una estructura y enfoque sistemático para la gestión de riesgos en general.

A lo largo de este documento, se proporcionarán las etapas clave para la generación de una matriz de riesgos en seguridad de la información. Se abordarán aspectos como la identificación de activos de información, la evaluación de amenazas y vulnerabilidades, la determinación del impacto y la evaluación de la probabilidad de ocurrencia de los riesgos. Asimismo, se explorarán estrategias de tratamiento y mitigación de riesgos, permitiendo a las municipalidades tomar acciones preventivas y correctivas para salvaguardar la información de manera efectiva.

Es importante tener en cuenta que esta metodología puede adaptarse a las necesidades y características específicas de cada municipalidad. Se sugiere consultar a expertos en seguridad de la información y adaptar la metodología a la realidad de la empresa, considerando sus activos de información, riesgos particulares y los recursos disponibles.

En resumen, este documento proporciona una guía práctica para la generación de una matriz de riesgos en seguridad de la información, basada en los estándares ISO 27000 e ISO 31000. La implementación de esta metodología permitirá a las municipalidades identificar y gestionar de manera eficiente los riesgos a los que se enfrenta su información, fortaleciendo así su postura en seguridad y garantizando la protección de sus activos más valiosos.

Objetivo: El objetivo de la presente matriz corresponde a mantener y proteger la confidencialidad, integridad y disponibilidad de la información, valiosa y sensible para la I. Municipalidad de Santo Domingo.

Alcance: Las presentes políticas deberán ser aplicadas por todos los funcionarios y funcionarias municipales, cualquiera sea su jerarquía, escalafón o estamento. Asimismo,

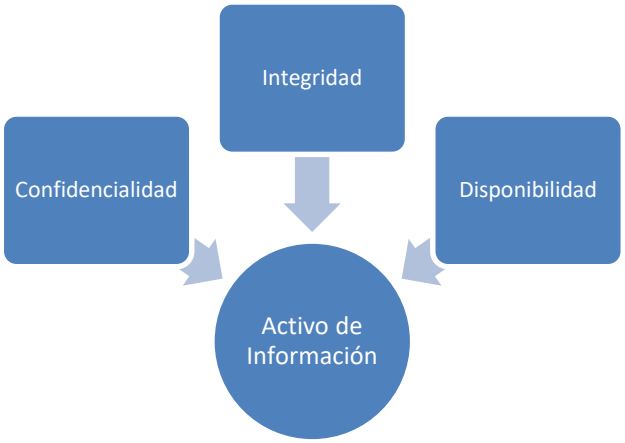
a aquellos prestadores de servicios contratados a honorarios, a proveedores externos y terceros que efectúe el tratamiento de datos personales.

Sin perjuicio de lo anterior, las obligaciones legales respecto a la confidencialidad de los datos y su buen uso por parte de los funcionarios(as) que efectúan su tratamiento o acceden a ellos, no cesan por culminado la relación contractual entre el municipio y este.

Definiciones: Para exponer de manera unívoca y con precisión la comprensión de las cualidades esenciales del tema implicado se detallan las siguientes definiciones:

- **Activos de información:** Cualquier cosa que tenga valor para el municipio como los datos, información, infraestructura TI, periféricos, redes comunicacionales, entre otros.
- **Autenticidad:** Es la propiedad de la información que asegura que esta proviene de una fuente confiable y es auténtica. Se refiere a la protección de la información contra falsificaciones o alteraciones no autorizadas.
- **Confidencialidad:** corresponde a la propiedad que determina que la información no esté disponible o sea revelada a terceros, entidades o procesos no autorizados.
    - Ejemplo: Cifrado de información que no permite que sea entendible para las personas que no disponen de las claves o certificados necesarios, aunque sea interceptada en tránsito o llegue al repositorio donde se encuentre almacenada.
    - Ejemplo: Controles de acceso a las instalaciones (sala de servidor), repositorios y sistemas donde se encuentran los datos o red por la que estos se mueves, evitando accesos no autorizados a la misma.
- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
    - Ejemplo: copias de seguridad de la base de datos, sistemas en clúster, copia de discos.
- **Integridad:** propiedad de resguardar la exactitud, calidad y estado de los activos.
    - Ejemplo: Al crear una base de datos deberá prestar atención a la integridad de los datos y su mantención. Lo anterior promueve la integridad de datos tanto como sea posible. Un usuario puede intentar ingresar por error un número de teléfono en el campo de fecha.
- **Trazabilidad:** Es la capacidad de rastrear y auditar los eventos relacionados con la información, lo que permite detectar y responder a incidentes de seguridad de manera efectiva. Se refiere a la capacidad de registrar y monitorizar los accesos, modificaciones y acciones relacionadas con la información.
- **Riesgo:** Autenticidad: Es la propiedad de la información que asegura que esta proviene de una fuente confiable y es auténtica. Se refiere a la protección de la información contra falsificaciones o alteraciones no autorizadas.

Figura 1. Activos de información



Fuente: Elaboración propia basado en Norma ISO 27000.

I. SOBRE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información, asegurando que esta sea confiable, exacta y esté disponible cuando sea necesario. La norma internacional para la gestión de la seguridad de la información ISO 27000, define la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un enfoque de gestión de riesgos y dando confianza a las partes interesadas.

Es decir, corresponde al proceso de identificación, evaluación y gestión de los activos de información y los riesgos asociados a los mismos, a través de una serie de acciones preventivas que permiten mitigar riesgos protegiendo la información.

La referencia del presente documento está ligada a los estándares ISO 27000 (familia de normas para la seguridad de la información) e ISO 31000 (norma para la gestión de riesgos). A continuación, son presentadas las características más relevantes de ello:

1. El riesgo tiene las siguientes características según ISO 31000:

a) Inherente: El riesgo existe independientemente de si se toman medidas o no para mitigarlo. Es el riesgo tal como se presenta inicialmente antes de implementar medidas de control.
b) Contextual: El riesgo está influenciado por el contexto específico de una organización, incluyendo su entorno, objetivos, recursos y tolerancia al riesgo.
c) Objetivo: El riesgo se relaciona con el logro de los objetivos de una organización. Puede afectar negativamente la capacidad de una municipalidad para cumplir sus objetivos estratégicos, operativos, financieros o de cumplimiento.
d) Incertidumbre: El riesgo está asociado con la incertidumbre, ya que se refiere a eventos futuros que pueden ocurrir o no. La evaluación del riesgo implica considerar la probabilidad de ocurrencia y el impacto de esos eventos.

2. Una amenaza en el contexto de la seguridad de la información es cualquier evento, acción o circunstancia que tiene el potencial de causar daño a los activos de

información. Existen varios tipos de amenazas, entre las cuales se pueden mencionar:

a) Amenazas naturales: Incluyen eventos naturales como terremotos, inundaciones, incendios forestales, tormentas, entre otros, que pueden causar interrupciones en los sistemas y la infraestructura de TI.
b) Amenazas humanas: Engloban las acciones maliciosas o intencionales llevadas a cabo por personas, como el acceso no autorizado a sistemas, el robo de información, la manipulación de datos, el espionaje corporativo o el sabotaje.
c) Amenazas tecnológicas: Se refieren a fallos o deficiencias en la infraestructura tecnológica, como errores de programación, vulnerabilidades en el software, brechas de seguridad, malware, ataques de denegación de servicio, entre otros.
d) Amenazas internas: Son aquellas que provienen de personas dentro de la municipalidad, como empleados descontentos, ex empleados, contratistas o proveedores con acceso privilegiado, que pueden utilizar su conocimiento para llevar a cabo acciones maliciosas o inapropiadas.

3. En tanto, una vulnerabilidad en seguridad de la información es una debilidad o fallo en los sistemas, procesos o controles que puede ser explotado por una amenaza para comprometer la seguridad de la información. Algunos ejemplos de vulnerabilidades son:

a) Fallos de seguridad en software: Errores de programación, falta de validación de datos, puertas traseras involuntarias o intencionadas en el código, que pueden ser aprovechadas por atacantes para comprometer la seguridad de los sistemas.
b) Configuraciones incorrectas: Configuraciones inseguras o incorrectas en los sistemas, servidores, firewalls o dispositivos de red, que pueden permitir a los atacantes obtener acceso no autorizado o comprometer la integridad de la información.
c) Falta de políticas y procedimientos: Ausencia de políticas de seguridad claras, procedimientos de gestión de accesos o controles de seguridad adecuados, lo cual crea oportunidades para que los atacantes exploten las debilidades y accedan a la información.
d) Falta de conciencia de seguridad: La falta de educación y conciencia sobre las mejores prácticas de seguridad de la información entre los empleados puede conducir a acciones no seguras, como el uso de contraseñas débiles o compartir información confidencial sin autorización.

4. El impacto en seguridad de la información se refiere a las consecuencias que se producirían si un riesgo se materializara. ISO 27000 y ISO 31000 ofrecen enfoques para evaluar y categorizar el impacto:

a) Categorías de impacto según ISO 27000:

- Confidencialidad: Se refiere a la pérdida de confidencialidad de la información, lo que puede resultar en la divulgación no autorizada de datos sensibles.

- Integridad: Se refiere a la pérdida de integridad de la información, lo que implica la modificación no autorizada de datos, alterando su exactitud o completitud.
- Disponibilidad: Se refiere a la pérdida de disponibilidad de la información, lo que puede causar interrupciones en los sistemas o la incapacidad de acceder a la información cuando sea necesario.

b) Evaluación del impacto según ISO 31000:

- Impacto en los objetivos: Se evalúa el impacto del riesgo en los objetivos de la municipalidad, como financieros, operativos, reputacionales, legales, entre otros.
- Severidad: Se evalúa la gravedad del impacto, clasificándolo en categorías como insignificante, menor, moderado, mayor o catastrófico.

La evaluación del impacto permite priorizar los riesgos y tomar decisiones informadas sobre las medidas de control y mitigación necesarias para proteger la seguridad de la información y minimizar las consecuencias negativas en caso de que un riesgo se materialice.

II. MARCO METODOLÓGICO

Para lograr el objetivo planteado, es necesario establecer un enfoque metodológico estructurado que permita identificar y abordar de manera sistemática los riesgos y vulnerabilidades asociados a los activos de información dentro del municipio. En este apartado, es descrito detalladamente el marco metodológico utilizado, el cual está basado en las mejores prácticas y estándares reconocidos internacionalmente en materia de seguridad de la información. A través de este enfoque, es establecido un panorama completo y preciso de seguridad de la información, así como brindar recomendaciones para fortalecer y mejorar la protección de los activos de información críticos de la municipalidad.

1. Contexto y alcance de la gestión de riesgos:

a) Establecimiento del contexto de la seguridad de la información:

Antes de comenzar la construcción de la matriz de riesgos, es esencial establecer el contexto de la seguridad de la información en la municipalidad. Esto implica comprender el entorno en el que opera la municipalidad, su estructura, sus objetivos estratégicos y las partes interesadas relevantes.

Algunos aspectos a considerar al establecer el contexto de la seguridad de la información son:

- Identificación de los activos de información críticos: Determine qué activos de información son críticos para la municipalidad y cuáles son esenciales para su funcionamiento y continuidad.
- Análisis de las amenazas y vulnerabilidades: Realice un análisis exhaustivo de las amenazas que podrían afectar a los activos de información y las vulnerabilidades existentes en los sistemas y procesos.

- Evaluación del marco legal y regulatorio: Considere los requisitos legales y normativos aplicables a la seguridad de la información, como la legislación de protección de datos, regulaciones sectoriales u obligaciones de cumplimiento.
- Identificación de las partes interesadas: Identifique las partes interesadas clave en la seguridad de la información, como la alta dirección, los empleados, los clientes, los proveedores y los socios comerciales, y comprenda sus expectativas y requisitos.

b) Determinación del alcance de la gestión de riesgos:

Una vez establecido el contexto de la seguridad de la información, es necesario determinar el alcance de la gestión de riesgos. Esto implica definir los límites dentro de los cuales se llevará a cabo la evaluación y gestión de riesgos.

Algunos aspectos a considerar al determinar el alcance de la gestión de riesgos son:

- Definición de los objetivos de la gestión de riesgos: Establecer claramente los objetivos que se desean lograr con la gestión de riesgos en seguridad de la información. Por ejemplo, proteger los activos críticos de información, garantizar la continuidad del negocio o cumplir con los requisitos legales y normativos.
- Identificación de los activos y procesos incluidos: Determinar los activos de información y procesos estarán incluidos en la matriz de riesgos. Esto puede incluir sistemas de información, bases de datos, infraestructura de red, procesos de negocio críticos y cualquier otro elemento relevante para la seguridad de la información.
- Consideración de los límites temporales: Especificar el período de tiempo para el cual se evaluarán los riesgos. Puede ser a corto plazo, a mediano plazo o a largo plazo, según las necesidades y las características de la municipalidad.
- Delimitación de responsabilidades: Definir las responsabilidades de los equipos y las personas involucradas en la gestión de riesgos. Esto puede incluir roles como el responsable de seguridad de la información, el comité de seguridad de la información o los propietarios de activos de información.

Al establecer el contexto y determinar el alcance de la gestión de riesgos, se sientan las bases para la construcción efectiva de la matriz de riesgos de seguridad de la información. Estos pasos preliminares ayudarán a enfocar y dirigir el proceso de evaluación de riesgos y garantizarán que se tengan en cuenta los aspectos clave de la municipalidad y su entorno [Purser, S. (2016)].

2. Identificación de activos de información:

a) Clasificación de los activos según ISO 27000:

La clasificación de los activos de información es un paso fundamental en la gestión de la seguridad de la información. Según ISO 27000, los activos de información se

pueden clasificar en diferentes categorías, lo que permite identificarlos y tratarlos de manera adecuada en términos de seguridad.

La norma ISO/IEC 27001 establece que los activos de información se pueden clasificar en las siguientes categorías principales:

- Activos tangibles: Son los activos físicos que pueden tocarse o percibirse directamente, como equipos de tecnología, servidores, dispositivos de almacenamiento, infraestructura física, documentos impresos, entre otros.
- Activos intangibles: Incluyen la información en formato electrónico o digital, como bases de datos, software, aplicaciones, códigos fuente, manuales, políticas, procedimientos, patentes, marcas registradas y otros activos de propiedad intelectual.
- Activos humanos: Se refieren a las personas dentro de la municipalidad que tienen conocimientos, habilidades o roles específicos relacionados con la seguridad de la información, como los especialistas en seguridad, administradores de sistemas, personal de soporte técnico, entre otros.

Estas categorías proporcionan un marco básico para clasificar los activos de información de acuerdo con su naturaleza y características. Sin embargo, es importante adaptar esta clasificación a las necesidades y particularidades de cada municipalidad.

b) Evaluación de la importancia y el valor de los activos:

Una vez clasificados los activos de información, es necesario evaluar su importancia y valor. Esta evaluación se realiza para comprender el impacto que tendría la pérdida, el deterioro o el acceso no autorizado de cada activo en el cumplimiento de los objetivos de la municipalidad.

La evaluación de la importancia y el valor de los activos implica considerar diversos factores, como su contribución a los procesos operativos, su valor económico, su sensibilidad y su relevancia estratégica. Algunas técnicas comunes utilizadas para realizar esta evaluación son:

- Análisis de impacto: Consiste en identificar y evaluar las consecuencias que tendría la pérdida o el daño de un activo en términos de confidencialidad, integridad y disponibilidad de la información. Esta evaluación se basa en el impacto potencial en la municipalidad y sus operaciones.
- Valoración económica: Se refiere a determinar el valor económico de los activos de información, considerando su costo de adquisición, su valor de reemplazo, su valor de mercado o su contribución al negocio. Esta evaluación puede ayudar a priorizar los recursos de protección y asignar presupuestos adecuados para la seguridad de la información.

Es importante destacar que la evaluación de la importancia y el valor de los activos puede variar de acuerdo con el contexto y los objetivos de cada municipalidad. Se recomienda utilizar enfoques y metodologías que se ajusten a las necesidades específicas y contar con la participación de los responsables de los activos y las partes interesadas relevantes.

3. Identificación de amenazas y vulnerabilidades:

a) Análisis de amenazas según ISO 27000

El análisis de amenazas, según ISO 27000, es un proceso fundamental para identificar las fuentes potenciales de peligro que podrían afectar la seguridad de la información. El objetivo principal del análisis de amenazas es determinar qué amenazas podrían materializarse y causar daño a los activos de información.

El estándar ISO/IEC 27001:2013, "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos", brinda orientación sobre cómo realizar el análisis de amenazas. Esta norma recomienda seguir los siguientes pasos:

- Identificación de las amenazas: Consiste en identificar y enumerar todas las fuentes potenciales de amenazas que podrían afectar la seguridad de la información en la municipalidad. Esto puede incluir amenazas internas (como empleados malintencionados) y amenazas externas (como hackers, desastres naturales, etc.).
- Evaluación de las amenazas: Una vez identificadas las amenazas, se debe evaluar su probabilidad de ocurrencia y su impacto potencial en los activos de información. Esto ayudará a priorizar las amenazas y enfocar los esfuerzos de protección en las más críticas.
- Documentación de las amenazas: Es importante documentar las amenazas identificadas, junto con su probabilidad de ocurrencia y su impacto potencial. Esta información será utilizada posteriormente en la construcción de la matriz de riesgos.

b) Evaluación de vulnerabilidades según ISO 27000

La evaluación de vulnerabilidades es un proceso que permite identificar las debilidades en los activos de información y los controles de seguridad existentes. El objetivo principal de la evaluación de vulnerabilidades es determinar qué activos son más vulnerables y qué medidas de protección se requieren para mitigar los riesgos asociados.

La norma ISO/IEC 27002:2013, "Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información", proporciona directrices sobre cómo llevar a cabo la evaluación de vulnerabilidades. Algunos pasos clave incluyen:

- Identificación de las vulnerabilidades: Consiste en identificar y enumerar las debilidades en los activos de información y los controles de seguridad existentes. Esto puede incluir fallos en la configuración de sistemas, falta de parches de seguridad, políticas y procedimientos inadecuados, entre otros.
- Evaluación de las vulnerabilidades: Una vez identificadas las vulnerabilidades, se deben evaluar su gravedad y el riesgo que representan para los activos de información. Esto permitirá priorizar las vulnerabilidades y establecer acciones correctivas y medidas de protección.

- Documentación de las vulnerabilidades: Es importante documentar las vulnerabilidades identificadas, junto con su gravedad y el riesgo asociado. Esta información será utilizada en la construcción de la matriz de riesgos.

4. Evaluación del impacto:

a) Categorización de los impactos potenciales según ISO 27000:

La evaluación del impacto es un paso crítico en el proceso de construcción de una matriz de riesgos de seguridad de la información. Consiste en analizar y determinar las posibles consecuencias que podrían resultar de la materialización de un riesgo en los activos de información de la municipalidad.

ISO 27000 proporciona una clasificación de los impactos potenciales que pueden afectar la seguridad de la información. Esta clasificación ayuda a estandarizar la evaluación del impacto y facilita la comparación entre diferentes riesgos.

- Algunas categorías de impacto comunes según ISO 27000 incluyen:
    - Daño a la reputación: Se refiere a la pérdida de confianza de los clientes, socios comerciales o el público en general debido a la exposición o compromiso de la información sensible.
    - Pérdida financiera: Incluye los costos asociados con la recuperación de incidentes de seguridad, la pérdida de ingresos, las multas o sanciones, y los gastos de reparación de sistemas o infraestructuras dañadas.
    - Interrupción del negocio: Se refiere a la interrupción de las operaciones comerciales normales debido a un incidente de seguridad, lo que puede resultar en pérdida de productividad, retrasos en la entrega de productos o servicios, y pérdida de oportunidades comerciales.
    - Daño a la integridad de la información: Implica la alteración no autorizada o manipulación de la información, lo que puede llevar a decisiones incorrectas o perjudiciales para la municipalidad.

b) Determinación de las consecuencias asociadas a cada impacto:

Una vez que se han identificado las categorías de impacto, es necesario determinar las consecuencias específicas que podrían resultar de cada uno de ellos. Esto implica analizar y comprender las posibles implicaciones y ramificaciones que una situación de riesgo podría tener sobre los activos de información y la municipalidad en su conjunto.

- Las consecuencias pueden variar según el tipo de impacto y la naturaleza de los activos de información involucrados. Algunos ejemplos de consecuencias asociadas a cada impacto podrían incluir:
    - Daño a la reputación: Pérdida de clientes, disminución de la participación en el mercado, pérdida de contratos o asociaciones comerciales.
    - Pérdida financiera: Costos de recuperación, pérdida de ingresos, multas o sanciones legales, disminución del valor de mercado de la municipalidad.

- Interrupción del negocio: Pérdida de productividad, incumplimiento de los acuerdos de nivel de servicio, pérdida de clientes debido a la incapacidad de cumplir con las obligaciones contractuales.
- Daño a la integridad de la información: Deterioro de la calidad de los datos, toma de decisiones incorrectas basadas en información manipulada, pérdida de confianza en los sistemas y procesos de la municipalidad.

Es importante realizar un análisis exhaustivo de las consecuencias asociadas a cada impacto, considerando los diferentes escenarios y contextos en los que puedan ocurrir. Esto ayudará a tener una visión clara de las posibles implicaciones y a establecer medidas de mitigación adecuadas.

5. Evaluación de la probabilidad e impacto del riesgo:

a) Evaluación cualitativa y cuantitativa de la probabilidad e impacto según ISO 31000:

La evaluación de la probabilidad e impacto del riesgo es una etapa esencial en la construcción de una matriz de riesgos de seguridad de la información. Permite asignar valores y calificar la probabilidad de ocurrencia y el impacto potencial de cada riesgo identificado.

- ISO 31000 proporciona directrices para realizar una evaluación tanto cualitativa como cuantitativa de la probabilidad e impacto del riesgo. Estos enfoques pueden utilizarse de manera complementaria para obtener una comprensión más completa del riesgo.

    - Evaluación cualitativa: En este enfoque, se asignan etiquetas o categorías a la probabilidad e impacto del riesgo. Esto implica utilizar escalas predefinidas para calificar la probabilidad de ocurrencia y el impacto potencial en términos de su gravedad. Por ejemplo, se pueden utilizar escalas como "baja", "media" y "alta" para calificar la probabilidad e impacto.
    - Evaluación cuantitativa: Este enfoque implica asignar valores numéricos a la probabilidad e impacto del riesgo. Se utilizan técnicas como el análisis estadístico y el modelado para calcular los valores numéricos. Esto permite realizar cálculos más precisos y proporciona una base sólida para la toma de decisiones.

Es importante seleccionar el enfoque de evaluación más adecuado según la disponibilidad de datos, los recursos disponibles y los requisitos específicos de la municipalidad.

b) Cálculo del nivel de riesgo:

Una vez que se ha evaluado la probabilidad e impacto del riesgo, es posible calcular el nivel de riesgo asociado a cada uno. Esto implica combinar la probabilidad y el impacto asignados para obtener una medida numérica del riesgo.

El cálculo del nivel de riesgo puede realizarse mediante diferentes métodos, como la multiplicación de los valores asignados a la probabilidad y el impacto, o mediante el uso de matrices de riesgo que asignan valores numéricos a cada combinación de probabilidad e impacto.

El nivel de riesgo puede ser expresado en términos de una escala numérica o utilizando categorías como "bajo", "medio" y "alto". Esta medida del riesgo ayudará a priorizar los riesgos identificados y enfocar los esfuerzos en aquellos que presentan un nivel de riesgo más alto.

6. Tratamiento y mitigación de riesgos:

a) Evaluación de opciones de tratamiento de riesgos según ISO 31000:

El tratamiento y mitigación de riesgos es una etapa crítica en el proceso de construcción de una matriz de riesgos de seguridad de la información. Consiste en identificar las opciones de tratamiento de riesgos, definir medidas de mitigación y control, y finalmente implementar estas medidas para reducir la probabilidad de ocurrencia y el impacto potencial de los riesgos identificados.

- ISO 31000 proporciona directrices para evaluar y seleccionar opciones de tratamiento de riesgos. Estas opciones incluyen:

    - Aceptar el riesgo: En algunos casos, puede ser apropiado aceptar el riesgo y decidir no tomar medidas adicionales para mitigarlo. Esta opción se aplica cuando el costo de mitigación supera los beneficios esperados o cuando el riesgo residual es tolerable para la municipalidad.
    - Evitar el riesgo: Esta opción implica tomar medidas para eliminar o evitar completamente el riesgo. Puede involucrar cambios en los procesos, la tecnología o la infraestructura para eliminar la exposición al riesgo.
    - Reducir el riesgo: Consiste en implementar medidas de mitigación y control para reducir la probabilidad de ocurrencia o el impacto del riesgo. Esto puede incluir el uso de controles de seguridad, capacitación del personal, implementación de políticas y procedimientos, entre otros.
    - Compartir el riesgo: En algunos casos, puede ser beneficioso compartir el riesgo con terceros a través de seguros, acuerdos contractuales u otras formas de transferencia de riesgos.
    - Transferir el riesgo: Implica transferir el riesgo a terceros, como proveedores de servicios o socios comerciales, mediante acuerdos contractuales que establezcan responsabilidades y obligaciones claras.

    La evaluación de las opciones de tratamiento de riesgos debe considerar factores como la viabilidad técnica, la viabilidad financiera, las necesidades y objetivos de la municipalidad, y la aceptabilidad de los riesgos residuales.

b) Definición de medidas de mitigación y control basadas en ISO 27000:

ISO 27000 proporciona un conjunto de controles y medidas de seguridad que pueden utilizarse como base para definir las medidas de mitigación y control específicas en el contexto de la seguridad de la información.

- Algunas áreas clave que se deben considerar al definir las medidas de mitigación y control son:

    - Seguridad física: Implementación de medidas para proteger los activos de información físicos, como sistemas, servidores, salas de servidores y otros recursos de tecnología de la información.
    - Seguridad lógica: Implementación de medidas para proteger los activos de información digitales, como contraseñas, cifrado, firewalls, sistemas de detección de intrusos, políticas de acceso y control de privilegios.
    - Gestión de incidentes: Establecimiento de procedimientos y mecanismos para detectar, responder y recuperarse de incidentes de seguridad de la información de manera eficiente y oportuna.
    - Concienciación y capacitación: Desarrollo de programas de concienciación y capacitación para el personal, a fin de fomentar la comprensión de los riesgos de seguridad de la información y promover buenas prácticas de seguridad.

c) Implementación de las medidas de mitigación y control:

Las medidas de mitigación y control deben ser seleccionadas y adaptadas según las necesidades y características específicas de la municipalidad, y deben estar alineadas con los objetivos y requisitos de seguridad de la información establecidos.

- Una vez que se han definido las medidas de mitigación y control, es importante implementarlas de manera efectiva en toda la municipalidad. Esto implica llevar a cabo las siguientes actividades:

    - Asignación de responsabilidades: Designar personas o equipos responsables de la implementación y gestión de las medidas de mitigación y control.
    - Desarrollo de planes de implementación: Establecer un plan detallado que incluya las actividades, los plazos, los recursos necesarios y los hitos de implementación.
    - Capacitación y concienciación: Proporcionar capacitación adecuada al personal sobre las medidas de mitigación y control, así como promover la concienciación continua sobre la importancia de la seguridad de la información.
    - Monitoreo y revisión: Establecer mecanismos de monitoreo y revisión periódica para asegurar que las medidas de mitigación y control estén funcionando de manera efectiva y cumpliendo con los objetivos establecidos.

La implementación de las medidas de mitigación y control debe ser un proceso continuo y adaptable, ya que las amenazas y vulnerabilidades cambian con el tiempo y es necesario mantenerse actualizado para garantizar la seguridad de la información de manera efectiva.

III. SOBRE LA MATRIZ DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

Una matriz de riesgos es una herramienta de gran utilidad para toda institución pública o privada, permitiendo identificar los riesgos a los que puede existir un grado de exposición. Asimismo, este instrumento propicia una adecuada gestión los riesgos, pudiendo cuantificarlos, controlarlos y establecer rutas de derivación como su transferencia o mitigación.

Dentro de las características más reconocibles se encuentra:

1. Comprensión visual
2. Sencillez de lectura.
3. Flexibilidad.
4. Permite comparaciones.
5. Permite un diagnóstico más acabado para el ciclo de mejora continua.
6. Acelera la toma de decisiones.

Para crear una matriz es necesario ubicar los riesgos en un espacio, de ahí la importancia del componente visual. Al momento de situar un riesgo debe ser considerada una dimensión o plano de 2 ejes (x e y), cuyos componentes de la calificación están determinados por la frecuencia e impacto de los mismos.

1. Frecuencia

La frecuencia corresponde a la probabilidad de que ocurra un riesgo. Dentro de una matriz esta eventualidad puede ser determinada mediante escalas de valores cualitativas y cuantitativas.

a) Improbable: la probabilidad de que ocurra un riesgo, es decir, que se materialice, es demasiado baja, casi nula.
b) Posible: su probabilidad es baja, aunque puede existir.
c) Ocasional: el riesgo que pueda materializarse en cualquier momento es posible.
d) Probable: su materialización es alta, de hecho, suele presentarse.
e) Frecuente: es muy alta la probabilidad de ocurrencia de este riesgo.

De acuerdo con lo indicado anteriormente, es realizada una valoración definida en base los objetivos esperados. Por ejemplo:

Tabla 1. Porcentaje y Valor Cualitativo.

PORCENTAJE	VALOR CUALITATIVO
0% a 20%	Muy baja
20.1% a 40%	Baja
40.1% a 60%	Media
60.1% a 80%	Alta
80.1% a 100%	Muy alta

Fuente: Elaboración propia basado en Norma ISO 31000.

2. Impacto

El impacto puede ser explicado como el conjunto de consecuencias que origina la materialización de un riesgo. Es decir, la afectación que éste causaría en la municipalidad, pudiendo ser económicas, legales, reputacionales, entre otras.

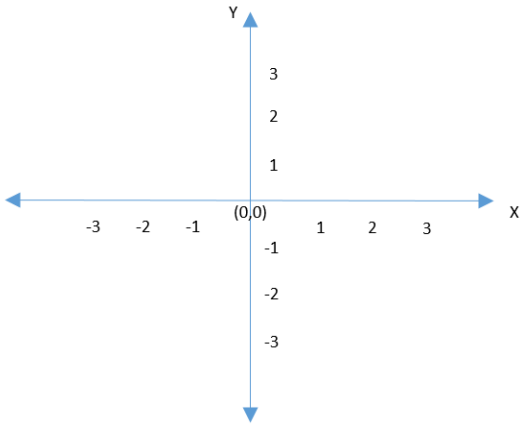
a) Insignificante: su impacto no representa un problema para el municipio.
b) Menor: el impacto que causa su materialización es mínimo.
c) Moderado: la materialización de este riesgo puede causar una pérdida temporal.
d) Mayor: genera retrasos importantes que afectan el cumplimiento de los objetivos.
e) Catastrófico: puede detener la operación de la municipalidad, inclusive, puede tener consecuencias como detener la continuidad del servicio.

3. Mapa de Calor

Este componente del instrumento estará compuesto por:

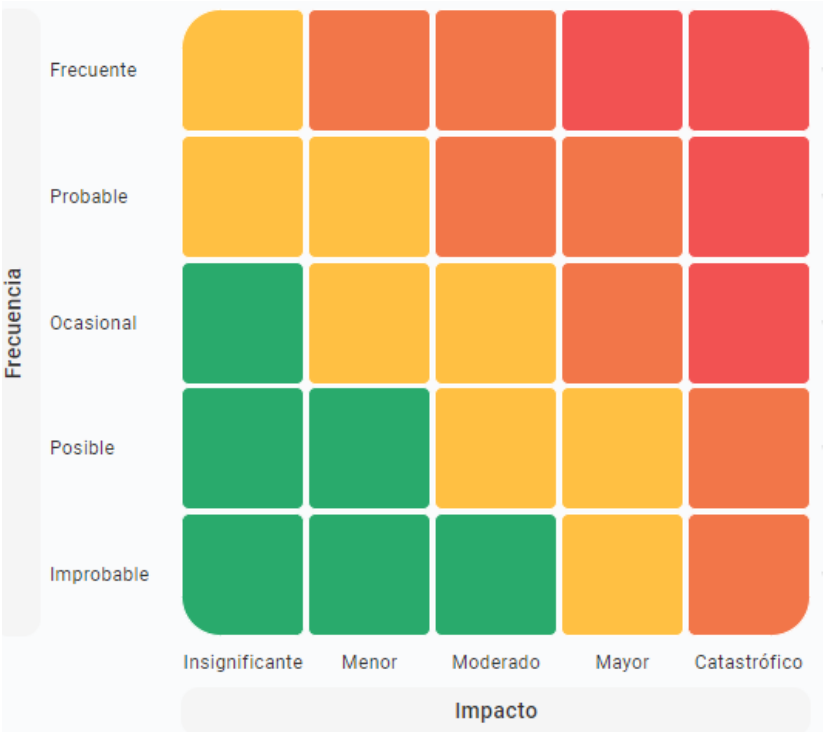
a) Un eje vertical (Y) con los valores de frecuencia.
b) Un eje horizontal (X) con los valores de impacto.

Figura 2. Cuadrantes del Mapa de Calor



Fuente: Elaboración propia basado en Norma ISO 31000.

Figura 3. Mapa de Calor



Fuente: Elaboración propia basado en Norma ISO 31000.

Tabla 2. Clasificación y Ponderación de Impacto.

IMPACTO	
Insignificante	20%
Menor	40%
Moderado	60%
Mayor	80%
Catastrófico	100%

Fuente: Elaboración propia basado en Norma ISO 31000.

Tabla 3. Clasificación y Ponderación de Frecuencia.

FRECUENCIA	
Improbable	20%
Posible	40%
Ocasional	60%
Probable	80%
Frecuente	100%

Fuente: Elaboración propia basado en Norma ISO 31000.

Tabla 4. Nivel de Riesgo.

NOMBRE RIESGO	**COLOR**

Bajo	
Medio	
Alto	
Extremo	

Fuente: Elaboración propia basado en Norma ISO 31000.

Tabla 5. Calificación de Riesgos

NOMBRE	PESO
Legal	20%
Reputacional	20%
Operacional	20%
Financiero	20%
Ambiental	20%

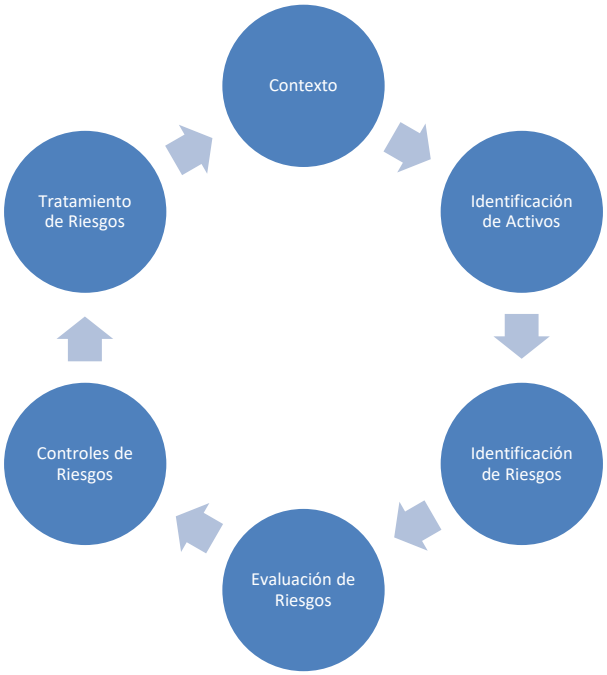
Fuente: Elaboración propia basado en Norma ISO 31000.

IV. ELEMENTOS PARA LA IDENTIFICACIÓN DE LA MATRIZ DE RIESGOS

Inicialmente a partir de ISO 3000 es necesario contextualizar los procesos que definen las actividades, y a partir de ello, declarar los activos de información. Posteriormente, deberán ser identificados aquellos riesgos que derivan de los activos declarados pasando a la evaluación de los mismos. Dentro de esta evaluación serán establecidos el impacto y la frecuencia o la calificación inherente que permite su ubicación dentro del mapa de calor.

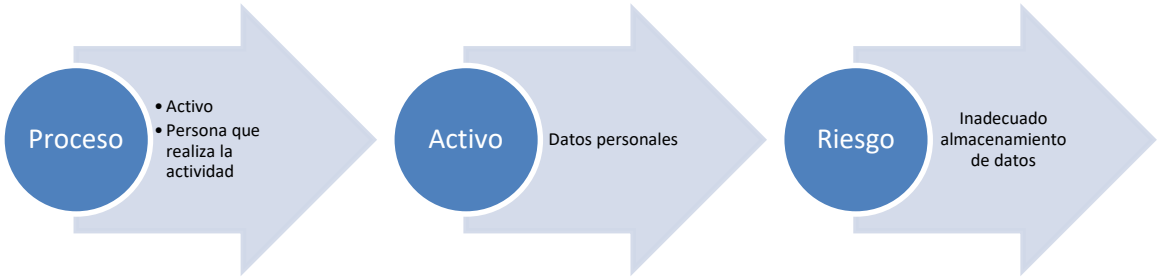
Al ser identificado el cuadrante al que pertenece serán aplicados los controles correspondientes, obteniendo la calificación residual que permite tomar decisiones evidenciando que luego de aplicar una serie de controles continúa en un cuadrante que no es aceptable es posible definir un tratamiento al riesgo. Desde ahí podrá ser transferido, reducirlo, evitarlo, o bien, si está dentro de los riesgos aceptables existe la posibilidad de aceptarlo.

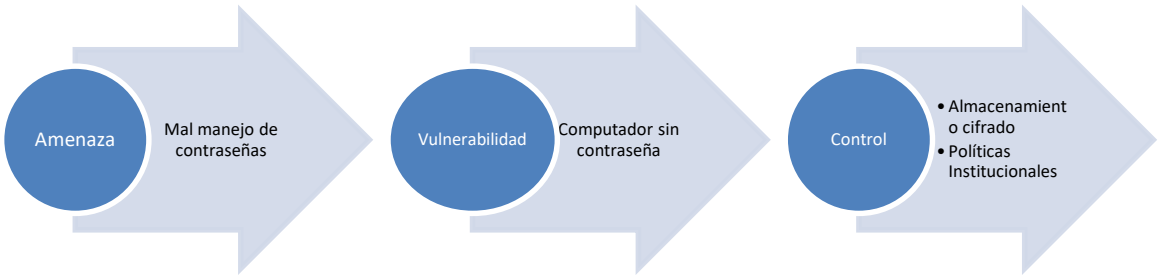
Figura 4. Identificación de la Matriz de Riesgos



Fuente: Elaboración propia basado en Norma ISO 31000.

Figura 5. Ejemplo Cadena del Proceso





Fuente: Elaboración propia basado en Norma ISO 27000/31000.

V. IDENTIFICACIÓN DE PROCESOS CLAVE PARA LA GESTIÓN DE RIESGOS

Al confeccionar una matriz de riesgos en seguridad de la información es importante considerar una serie de procesos clave para garantizar una gestión efectiva de los riesgos.

A continuación, se presenta un listado de procesos clave para la gestión de los mismos:

1. Gestión de acceso y autenticación:

   La gestión de acceso y autenticación se refiere a los procesos y controles utilizados para gestionar y controlar el acceso a los sistemas, aplicaciones, redes y recursos de una organización. Estos procesos aseguran que los usuarios y entidades autorizadas tengan el nivel adecuado de acceso a la información y los activos de la organización, mientras que al mismo tiempo se protege contra accesos no autorizados.

   a) Creación de credenciales de acceso a sistemas computacionales internos.
   b) Administración de cuentas de usuario y privilegios.
   c) Implementación de políticas de contraseñas seguras.
   d) Uso de autenticación de dos factores.
   e) Control de acceso físico a las instalaciones.

2. Protección de datos:

   La protección de datos se refiere a las medidas y prácticas implementadas para salvaguardar la seguridad, privacidad e integridad de la información personal o confidencial de las personas o entidades. Consiste en el conjunto de acciones y controles diseñados para prevenir el acceso no autorizado, la divulgación, modificación o destrucción indebida de los datos.

   a) Clasificación y etiquetado de datos según su confidencialidad.
   b) Implementación de controles de acceso a los datos.
   c) Encriptación de datos sensibles en reposo y en tránsito.
   d) Copias de seguridad y recuperación de datos.
   e) Retención y eliminación segura de datos obsoletos.

3. Gestión de parches y actualizaciones:

   La gestión de parches y actualizaciones se refiere al proceso de administrar y aplicar actualizaciones de software y parches de seguridad en los sistemas y aplicaciones de una organización.

   a) Implementación de un proceso de gestión de parches y actualizaciones para sistemas y aplicaciones.
   b) Evaluación de vulnerabilidades y aplicación de parches de seguridad.
   c) Mantenimiento y actualización de los sistemas operativos y software de seguridad.

4. Monitorización y detección de intrusiones:

   La monitorización y detección de intrusiones se refiere a la vigilancia y supervisión continua de los sistemas informáticos y redes para identificar y responder a posibles actividades maliciosas o no autorizadas.

   a) Implementación de sistemas de detección y prevención de intrusiones.
   b) Monitorización de eventos y registros de seguridad.
   c) Análisis de incidentes de seguridad y respuesta ante intrusiones.
   d) Evaluación de la actividad de la red y sistemas en busca de comportamientos anómalos.

5. Gestión de proveedores y terceros:

   La gestión de proveedores y terceros se refiere al proceso de administrar las relaciones con los proveedores externos y terceros que interactúan con una organización y tienen acceso a sus sistemas, datos o recursos. Esta gestión tiene como objetivo garantizar que los proveedores y terceros cumplan con los requisitos de seguridad y protección de datos establecidos por la organización.

   a) Evaluación de la seguridad de los proveedores y terceros.
   b) Establecimiento de acuerdos de seguridad y cláusulas de confidencialidad.

c) Supervisión y auditoría de los proveedores y terceros.

6. Concientización y formación en seguridad:

   La concientización y formación en seguridad se refiere a los programas y actividades diseñados para educar y capacitar a los empleados de una organización en prácticas seguras de seguridad de la información. Estos programas tienen como objetivo aumentar la conciencia y comprensión de los riesgos de seguridad, así como promover comportamientos y actitudes seguras entre el personal.

   a) Programas de concientización y formación en seguridad de la información para los empleados.
   b) Educación sobre prácticas seguras, políticas y procedimientos.
   c) Promoción de una cultura de seguridad en la organización.

7. Gestión de incidentes de seguridad:

   La gestión de incidentes de seguridad se refiere al proceso de planificación, detección, respuesta y recuperación ante eventos o incidentes de seguridad en una organización. Estos incidentes pueden incluir ataques cibernéticos, intrusiones, fugas de datos, malware, robo de información, entre otros.

   a) Proceso de notificación, registro y manejo de incidentes de seguridad.
   b) Investigación y análisis de incidentes.
   c) Restablecimiento de la seguridad y mitigación de los daños.

VI. ACTIVOS DE INFORMACIÓN

A continuación, son presentados los activos de información relevantes para el proceso de construcción de una matriz de riesgos en seguridad de la información:

1. Bases de datos: Base de datos en servidor institucional, base de datos de clientes, base de datos de empleados, base de datos de proveedores.
2. Sistemas y aplicaciones: Sistema de gestión de recursos humanos, sistema de gestión (CRM), sistema de gestión de inventario, aplicaciones web internas.
3. Infraestructura de red: Servidores, enrutadores, switches, puntos de acceso Wi-Fi, firewalls.
4. Datos sensibles: Información personal identificable (PII), datos financieros-contables, información confidencial de ciudadanos.
5. Documentos y archivos: Contratos, informes financieros-presupuestarios, manuales de procedimientos, documentos legales, resoluciones municipales, archivos de proyectos, procedimientos administrativos.
6. Dispositivos de almacenamiento: Unidades de disco duro, dispositivos USB, discos ópticos, cintas de respaldo, cloud services.
7. Recursos físicos: Equipos de cómputo, servidores físicos, impresoras, escáneres, cámaras de seguridad.

8. Propiedad intelectual: Patentes, derechos de autor.
9. Comunicaciones: Correo electrónico, mensajes instantáneos, voz sobre IP (VoIP), videoconferencias.
10. Activos de software: Licencias de software, código fuente, software personalizado.

VII. RIESGOS

Es importante realizar un análisis exhaustivo de riesgos para identificar y priorizar los riesgos más relevantes para la seguridad de la información.

1. Riesgo de acceso no autorizado: Posibilidad de que personas no autorizadas obtengan acceso a sistemas, aplicaciones o datos confidenciales.
2. Riesgo de pérdida de datos: Posibilidad de que se pierdan datos debido a fallas en el sistema, errores humanos, desastres naturales o ataques cibernéticos.
3. Riesgo de fuga de información: Posibilidad de que la información confidencial sea revelada o filtrada, ya sea de forma intencional o no intencional, por parte de empleados, contratistas o terceros.
4. Riesgo de robo de información: Posibilidad de que la información valiosa sea robada o comprometida por personas externas o internas malintencionadas.
5. Riesgo de interrupción del servicio: Posibilidad de que los sistemas o servicios críticos de la organización sean interrumpidos, ya sea debido a fallas técnicas, desastres naturales o ataques cibernéticos.
6. Riesgo de violación de privacidad: Posibilidad de que la información personal de los clientes o empleados sea utilizada o divulgada de manera inapropiada, incumpliendo las regulaciones de privacidad.
7. Riesgo de fallas en la seguridad física: Posibilidad de que los activos físicos, como servidores, equipos o documentos, sean vulnerados o robados debido a una falta de seguridad física.
8. Riesgo de ataques cibernéticos: Posibilidad de que los sistemas de la organización sean objeto de ataques de malware, phishing, ransomware u otros tipos de ataques cibernéticos.
9. Riesgo de falta de cumplimiento normativo: Posibilidad de incumplir las regulaciones y normativas relacionadas con la seguridad de la información, lo que puede resultar en sanciones legales y daño a la reputación.
10. Riesgo de falta de concientización en seguridad: Posibilidad de que los empleados no estén suficientemente capacitados o no cumplan con las prácticas de seguridad establecidas, lo que puede aumentar la vulnerabilidad de la organización.

VIII. CONTROLES

Es importante seleccionar y adaptar los controles de acuerdo con la naturaleza y el contexto de la organización para garantizar una protección adecuada de la seguridad de la información.

1. Políticas y procedimientos de seguridad de la información: Establecimiento de políticas y procedimientos claros y actualizados que regulen el uso adecuado de los activos de información y promuevan buenas prácticas de seguridad.

2. Acceso controlado y gestión de identidad: Implementación de controles de acceso basados en roles, autenticación de dos factores y gestión adecuada de cuentas de usuario para garantizar que solo las personas autorizadas tengan acceso a la información sensible.
3. Protección de la red: Implementación de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), segmentación de red y filtrado de tráfico para proteger la infraestructura de red contra amenazas y ataques cibernéticos.
4. Encriptación de datos: Uso de técnicas de encriptación para proteger la confidencialidad e integridad de la información durante su almacenamiento, transmisión y procesamiento.
5. Copias de seguridad y recuperación de desastres: Establecimiento de políticas y procedimientos para realizar copias de seguridad periódicas de los datos críticos y para garantizar la disponibilidad y la rápida recuperación en caso de incidentes o desastres.
6. Monitoreo y detección de eventos de seguridad: Implementación de herramientas y sistemas de monitoreo de seguridad que permitan la detección temprana de eventos sospechosos o maliciosos, así como el análisis forense en caso de incidentes.
7. Concientización y capacitación en seguridad: Realización de programas de concientización y capacitación regular para educar a los empleados sobre las amenazas de seguridad, buenas prácticas y políticas internas.
8. Gestión de parches y actualizaciones: Implementación de procesos para garantizar la instalación oportuna de parches de seguridad y actualizaciones de software en todos los sistemas y aplicaciones.
9. Gestión de proveedores y terceros: Establecimiento de procesos para evaluar y seleccionar proveedores confiables, así como para establecer acuerdos contractuales que incluyan requisitos de seguridad de la información.
10. Auditorías y pruebas de seguridad: Realización de auditorías internas y externas de seguridad, así como pruebas de vulnerabilidad y pruebas de penetración para identificar posibles debilidades y evaluar la efectividad de los controles implementados.

IX. MATRIZ DE RIESGOS

La construcción de una matriz de riesgos es un enfoque estructurado para identificar y evaluar los riesgos de seguridad de la información en una organización. Por ello, es presentada una herramienta basada en la interrelación entre los procesos, los activos de información, los riesgos asociados y los controles implementados.

1. Macroproceso – Gestión de acceso y autorización

a) Proceso: Creación de credenciales de acceso a sistemas computacionales internos

- Activo de información: Base de datos en servidor institucional
- Riesgo: Riesgo de acceso no autorizado, Riesgo de pérdida de datos, Riesgo de robo de información, Riesgo de violación de privacidad
- Controles:

- Políticas y procedimientos de seguridad de la información: Establecer políticas claras sobre el manejo de credenciales y el acceso a la base de datos.
- Acceso controlado y gestión de identidad: Implementar autenticación de dos factores y controles de acceso basados en roles para garantizar que solo los usuarios autorizados tengan acceso a la base de datos.
- Protección de la red: Implementar firewalls y sistemas de detección y prevención de intrusiones para proteger el servidor y la base de datos contra ataques externos.
- Encriptación de datos: Aplicar técnicas de encriptación para proteger la confidencialidad de los datos almacenados en la base de datos.
- Monitoreo y detección de eventos de seguridad: Establecer sistemas de monitoreo que alerten sobre intentos de acceso no autorizado o actividad sospechosa en la base de datos.
- Concientización y capacitación en seguridad: Educar a los empleados sobre la importancia de mantener seguras las credenciales y el acceso a la base de datos.
- Auditorías y pruebas de seguridad: Realizar auditorías regulares de seguridad y pruebas de penetración para identificar posibles vulnerabilidades en el acceso a la base de datos.

Esta relación muestra cómo el proceso de creación de credenciales de acceso a sistemas computacionales internos está relacionado con el activo de información (base de datos en servidor institucional) y los riesgos asociados (riesgo de acceso no autorizado, riesgo de pérdida de datos, riesgo de robo de información y riesgo de violación de privacidad). Para mitigar estos riesgos, se han establecido varios controles, como políticas y procedimientos de seguridad, controles de acceso, protección de la red, encriptación de datos, monitoreo, concientización y capacitación, y auditorías de seguridad. Estos controles trabajan en conjunto para proteger la seguridad de la información y mitigar los riesgos identificados.

b) Proceso: Administración de cuentas de usuario y privilegios.

- Activo de información: Sistemas y datos de la organización
- Riesgo: Riesgo de acceso no autorizado, Riesgo de abuso de privilegios, Riesgo de fuga de información, Riesgo de compromiso de la integridad de los datos
- Controles:
  - Políticas y procedimientos de seguridad de la información: Establecer políticas y procedimientos claros para la administración de cuentas de usuario y privilegios.
  - Acceso controlado y gestión de identidad: Implementar controles de acceso basados en roles y gestionar adecuadamente las cuentas de usuario y sus privilegios.
  - Separación de funciones y privilegios: Aplicar el principio de separación de funciones y asignar privilegios de forma controlada y limitada.
  - Revisiones periódicas de cuentas y privilegios: Realizar revisiones regulares de las cuentas de usuario y sus privilegios para garantizar que sean necesarios y estén actualizados.

- Monitoreo y detección de eventos de seguridad: Establecer sistemas de monitoreo para detectar actividades inusuales o maliciosas relacionadas con cuentas de usuario y privilegios.
- Concientización y capacitación en seguridad: Educar a los usuarios sobre la importancia de mantener contraseñas seguras y de utilizar sus privilegios de forma responsable.
- Registro y auditoría de actividades: Implementar registros y auditorías de las actividades relacionadas con la administración de cuentas y privilegios para facilitar la detección y respuesta a incidentes.
- Gestión de proveedores y terceros: Establecer controles y acuerdos contractuales para garantizar que los proveedores y terceros cumplan con las políticas de seguridad en la administración de cuentas y privilegios.

En este caso, el proceso de administración de cuentas de usuario y privilegios está relacionado con el activo de información (sistemas y datos de la organización) y los riesgos asociados (riesgo de acceso no autorizado, riesgo de abuso de privilegios, riesgo de fuga de información y riesgo de compromiso de la integridad de los datos). Para mitigar estos riesgos, se han establecido varios controles, como políticas y procedimientos de seguridad, controles de acceso, separación de funciones, revisiones periódicas, monitoreo, concientización y capacitación, registro y auditoría de actividades, y gestión de proveedores y terceros. Estos controles trabajan en conjunto para garantizar una adecuada administración de las cuentas de usuario y privilegios, protegiendo así la seguridad de los sistemas y datos de la organización.

c) Proceso: Implementación de políticas de contraseñas seguras.

- Activo de información: Cuentas de usuario y sistemas protegidos por contraseñas
- Riesgo: Riesgo de acceso no autorizado, Riesgo de violación de confidencialidad, Riesgo de compromiso de la integridad de los datos
- Controles:
  - Políticas y procedimientos de seguridad de la información: Establecer políticas claras sobre la creación y el uso de contraseñas seguras.
  - Requisitos de complejidad de contraseñas: Definir criterios de complejidad para las contraseñas, como longitud mínima, uso de caracteres especiales, combinación de letras y números, etc.
  - Cambio periódico de contraseñas: Establecer la periodicidad con la que los usuarios deben cambiar sus contraseñas para reducir la exposición al riesgo.
  - Prohibición del uso de contraseñas comunes: Implementar restricciones para evitar el uso de contraseñas comunes o fáciles de adivinar.
  - Autenticación de dos factores: Implementar autenticación de dos factores para agregar una capa adicional de seguridad a las contraseñas.
  - Encriptación de contraseñas: Almacenar las contraseñas de forma segura utilizando técnicas de encriptación fuerte.
  - Monitoreo de contraseñas débiles o comprometidas: Implementar sistemas que detecten contraseñas débiles o comprometidas y soliciten su cambio inmediato.

- Concientización y capacitación en seguridad: Educar a los usuarios sobre la importancia de utilizar contraseñas seguras y proteger su confidencialidad.
- Restricción de intentos de acceso fallidos: Establecer un límite en el número de intentos fallidos de inicio de sesión para prevenir ataques de fuerza bruta.
- Auditorías y pruebas de seguridad: Realizar auditorías regulares de seguridad y pruebas de penetración para identificar posibles vulnerabilidades en la implementación de políticas de contraseñas seguras.

En este caso, el proceso de implementación de políticas de contraseñas seguras se relaciona con el activo de información (cuentas de usuario y sistemas protegidos por contraseñas) y los riesgos asociados (riesgo de acceso no autorizado, riesgo de violación de confidencialidad y riesgo de compromiso de la integridad de los datos). Para mitigar estos riesgos, se han establecido varios controles, como políticas y procedimientos de seguridad, requisitos de complejidad de contraseñas, cambio periódico de contraseñas, prohibición de contraseñas comunes, autenticación de dos factores, encriptación de contraseñas, monitoreo, concientización y capacitación, restricción de intentos de acceso fallidos, y auditorías y pruebas de seguridad. Estos controles trabajan en conjunto para garantizar la implementación y el uso adecuado de contraseñas seguras, protegiendo así la confidencialidad e integridad de los sistemas y datos.

d) Proceso: Uso de autenticación de dos factores

- Activo de información: Cuentas de usuario y sistemas protegidos por autenticación de dos factores
- Riesgo: Riesgo de acceso no autorizado, Riesgo de violación de confidencialidad, Riesgo de compromiso de la integridad de los datos
- Controles:
  - Políticas y procedimientos de seguridad de la información: Establecer políticas claras sobre el uso de autenticación de dos factores.
  - Implementación de autenticación de dos factores: Configurar los sistemas y aplicaciones para requerir una segunda forma de autenticación, además de la contraseña, para acceder a las cuentas de usuario.
  - Tipos de autenticación de dos factores: Utilizar métodos de autenticación de dos factores seguros, como códigos generados en tiempo real, tarjetas inteligentes, biométrica, o aplicaciones de autenticación móvil.
  - Registro y vinculación de dispositivos: Permitir a los usuarios registrar y vincular sus dispositivos para facilitar la autenticación de dos factores en futuros inicios de sesión.
  - Educación y concientización: Capacitar a los usuarios sobre cómo configurar y utilizar correctamente la autenticación de dos factores, así como la importancia de su uso para proteger sus cuentas.
  - Monitoreo y detección de intentos de acceso no autorizados: Implementar sistemas de monitoreo que alerten sobre posibles intentos de acceso no autorizados, incluso después de haber superado la autenticación de dos factores.

- Respuesta a incidentes de seguridad: Establecer planes y procedimientos para responder rápidamente a cualquier incidente relacionado con la autenticación de dos factores, como el robo o pérdida de dispositivos de autenticación.
- Actualización y mantenimiento de la autenticación de dos factores: Mantenerse al día con las actualizaciones y mejoras de las tecnologías de autenticación de dos factores, asegurándose de que sigan siendo eficaces y seguras.

En este caso, el proceso de uso de autenticación de dos factores se relaciona con el activo de información (cuentas de usuario y sistemas protegidos por autenticación de dos factores) y los riesgos asociados (riesgo de acceso no autorizado, riesgo de violación de confidencialidad y riesgo de compromiso de la integridad de los datos). Para mitigar estos riesgos, se han establecido varios controles, como políticas y procedimientos de seguridad, implementación de autenticación de dos factores, selección de métodos seguros de autenticación, registro y vinculación de dispositivos, educación y concientización, monitoreo, respuesta a incidentes de seguridad, y actualización y mantenimiento de la autenticación de dos factores. Estos controles trabajan en conjunto para fortalecer la seguridad de las cuentas de usuario y proteger la confidencialidad e integridad de los sistemas y datos.

e) Proceso: Control de acceso físico a las instalaciones

- Activo de información: Instalaciones físicas y equipos dentro de las instalaciones.
- Riesgo: Riesgo de acceso no autorizado a las instalaciones, Riesgo de robo o daño físico a los equipos, Riesgo de violación de la confidencialidad física.
- Controles:
  - Identificación y autenticación de usuarios: Establecer sistemas de identificación y autenticación para garantizar que solo las personas autorizadas tengan acceso a las instalaciones.
  - Cerraduras y sistemas de seguridad física: Implementar cerraduras, sistemas de control de acceso y cámaras de vigilancia para proteger las entradas y salidas de las instalaciones.
  - Zonas de acceso restringido: Definir y establecer zonas de acceso restringido dentro de las instalaciones para limitar el acceso a áreas sensibles o críticas.
  - Tarjetas de acceso y sistemas de control de acceso: Utilizar tarjetas de acceso o sistemas de control de acceso electrónicos para gestionar y registrar el acceso de los empleados y visitantes a las instalaciones.
  - Vigilancia y monitoreo: Mantener una vigilancia constante de las áreas de acceso y utilizar sistemas de monitoreo para detectar cualquier actividad sospechosa o no autorizada.
  - Políticas y procedimientos de acceso físico: Establecer políticas y procedimientos claros para el acceso físico a las instalaciones, incluyendo la autorización de visitantes y contratistas.
  - Capacitación y concientización: Brindar capacitación regular a los empleados sobre las políticas y procedimientos de acceso físico, así como la importancia de la seguridad física.

- Respuesta a incidentes de seguridad: Tener un plan de respuesta a incidentes que incluya acciones específicas para abordar situaciones de acceso no autorizado o emergencias en las instalaciones.
- Auditorías y revisiones periódicas: Realizar auditorías y revisiones periódicas del control de acceso físico para identificar posibles debilidades y realizar mejoras continuas.

En el caso del proceso de control de acceso físico a las instalaciones, el activo de información son las propias instalaciones físicas y los equipos dentro de ellas. Los riesgos asociados incluyen el acceso no autorizado, el robo o daño físico a los equipos y la violación de la confidencialidad física. Para mitigar estos riesgos, se han establecido varios controles, como identificación y autenticación de usuarios, sistemas de seguridad física, zonas de acceso restringido, tarjetas de acceso, vigilancia y monitoreo, políticas y procedimientos de acceso físico, capacitación y concientización, respuesta a incidentes de seguridad, y auditorías periódicas. Estos controles trabajan en conjunto para garantizar que solo las personas autorizadas tengan acceso a las instalaciones, proteger los equipos y prevenir cualquier violación de seguridad física.

2. Macroproceso – Protección de Datos

a) Proceso: Clasificación y etiquetado de datos según su confidencialidad.

- Activo de información: Datos almacenados y transmitidos en diferentes sistemas y medios.
- Riesgo: Riesgo de divulgación no autorizada de información confidencial, Riesgo de uso inadecuado de datos sensibles.
- Controles:
  - Políticas de clasificación de datos: Establecer políticas claras y criterios de clasificación para identificar la confidencialidad de los datos.
  - Procedimientos de etiquetado: Definir procedimientos para etiquetar adecuadamente los datos según su nivel de confidencialidad.
  - Capacitación y concientización: Brindar capacitación a los empleados sobre la importancia de la clasificación y etiquetado correcto de los datos y las implicaciones de la divulgación no autorizada.
  - Sistemas de gestión de datos: Implementar sistemas de gestión de datos que permitan asignar etiquetas de confidencialidad a los archivos y controlar su acceso.
  - Acceso basado en roles: Establecer controles de acceso basados en roles para garantizar que solo las personas autorizadas tengan acceso a los datos confidenciales.
  - Auditorías y revisiones: Realizar auditorías periódicas para asegurar el cumplimiento de las políticas de clasificación y etiquetado de datos y detectar posibles brechas de seguridad.
  - Seguimiento de transferencias de datos: Implementar mecanismos de seguimiento para rastrear las transferencias de datos y garantizar que se realicen de manera segura y controlada.
  - Protección de datos sensibles: Aplicar medidas adicionales de seguridad, como cifrado, para proteger los datos clasificados como altamente confidenciales.

- Actualización y revisión de políticas: Mantener las políticas de clasificación y etiquetado de datos actualizadas y revisarlas regularmente para adaptarse a los cambios en los riesgos y requisitos de seguridad.

En el proceso de clasificación y etiquetado de datos según su confidencialidad, el activo de información son los datos almacenados y transmitidos en diferentes sistemas y medios. Los riesgos asociados incluyen la divulgación no autorizada de información confidencial y el uso inadecuado de datos sensibles. Para mitigar estos riesgos, se han establecido varios controles, como políticas de clasificación de datos, procedimientos de etiquetado, capacitación y concientización, sistemas de gestión de datos, acceso basado en roles, auditorías y revisiones, seguimiento de transferencias de datos, protección de datos sensibles, y actualización y revisión de políticas. Estos controles trabajan en conjunto para asegurar que los datos sean clasificados y etiquetados correctamente según su nivel de confidencialidad, y que se apliquen las medidas de seguridad adecuadas para protegerlos de la divulgación no autorizada.

b) Proceso: Implementación de controles de acceso a los datos

- Activo de información: Datos almacenados en sistemas y bases de datos.
- Riesgo: Riesgo de acceso no autorizado a los datos, Riesgo de modificación o eliminación no autorizada de los datos.
- Controles:
  - Políticas de acceso: Establecer políticas claras sobre quién tiene acceso a los datos y bajo qué condiciones.
  - Autenticación: Implementar métodos de autenticación seguros, como contraseñas, autenticación de dos factores o biometría, para verificar la identidad de los usuarios antes de permitirles el acceso a los datos.
  - Autorización: Definir roles y privilegios de usuario para limitar el acceso a los datos solo a aquellos que necesitan acceder a ellos para realizar sus tareas.
  - Segregación de funciones: Separar las responsabilidades y los roles dentro del sistema para evitar conflictos de interés y minimizar el riesgo de abuso o acceso no autorizado.
  - Control de acceso físico: Implementar medidas de seguridad física, como cerraduras, tarjetas de acceso y sistemas de vigilancia, para proteger los lugares donde se almacenan los datos.
  - Control de acceso lógico: Utilizar tecnologías y herramientas de control de acceso, como firewalls, sistemas de detección de intrusiones y sistemas de gestión de identidad y acceso (IAM), para proteger los datos de amenazas en el entorno digital.
  - Monitoreo y registro de acceso: Establecer mecanismos para registrar y monitorear los intentos de acceso a los datos, así como para detectar y responder a actividades sospechosas o no autorizadas.
  - Actualización y revisión de controles: Mantener los controles de acceso actualizados y revisarlos periódicamente para asegurarse de que sigan siendo efectivos frente a las nuevas amenazas y vulnerabilidades.

- Capacitación y concientización: Brindar capacitación regular a los usuarios sobre las políticas y mejores prácticas de acceso a los datos, así como sobre la importancia de mantener la seguridad de la información.

En el proceso de implementación de controles de acceso a los datos, el activo de información son los datos almacenados en sistemas y bases de datos. Los riesgos asociados incluyen el acceso no autorizado a los datos y la modificación o eliminación no autorizada de los mismos. Para mitigar estos riesgos, se han establecido varios controles, como políticas de acceso, autenticación, autorización, segregación de funciones, control de acceso físico y lógico, monitoreo y registro de acceso, actualización y revisión de controles, y capacitación y concientización. Estos controles trabajan en conjunto para garantizar que solo los usuarios autorizados tengan acceso a los datos y que se implementen medidas de seguridad adecuadas para proteger la confidencialidad, integridad y disponibilidad de la información.

c) Proceso: Encriptación de datos sensibles en reposo y en tránsito.

- Activo de información: Datos sensibles almacenados y transmitidos.
- Riesgo: Riesgo de exposición o compromiso de datos sensibles durante su almacenamiento y transmisión.
- Controles:
  - Políticas de encriptación: Establecer políticas y procedimientos claros para determinar qué datos deben ser encriptados y cómo se debe llevar a cabo el proceso de encriptación.
  - Algoritmos de encriptación: Utilizar algoritmos de encriptación robustos y reconocidos para proteger los datos sensibles. Ejemplos de algoritmos comunes incluyen AES (Advanced Encryption Standard) y RSA (Rivest-Shamir-Adleman).
  - Gestión de claves: Implementar un sistema seguro para la generación, distribución, almacenamiento y rotación de claves de encriptación. Esto incluye el uso de claves fuertes, protección de claves y acceso controlado a las mismas.
  - Encriptación de datos en reposo: Aplicar encriptación a los datos sensibles almacenados en dispositivos de almacenamiento, como discos duros, bases de datos y archivos. Esto garantiza que los datos estén protegidos en caso de acceso no autorizado o pérdida física del dispositivo.
  - Encriptación de datos en tránsito: Aplicar encriptación a los datos sensibles mientras se transmiten a través de redes y comunicaciones. Esto asegura que los datos estén protegidos contra interceptación y manipulación durante su transporte.
  - Certificados y protocolos seguros: Utilizar certificados digitales y protocolos de seguridad, como SSL/TLS, para garantizar la autenticación, integridad y confidencialidad de las comunicaciones en línea.
  - Administración de certificados: Implementar una adecuada gestión de certificados, incluyendo su emisión, renovación y revocación, para garantizar la confianza en los sistemas de encriptación y evitar el uso de certificados comprometidos o expirados.

- Monitoreo y detección de fallas de encriptación: Establecer mecanismos de monitoreo y detección para identificar cualquier falla en los procesos de encriptación, como certificados vencidos o configuraciones inseguras.
- Actualización y parches de seguridad: Mantener actualizados los sistemas y software de encriptación, aplicando parches de seguridad y actualizaciones para corregir posibles vulnerabilidades conocidas.
- Pruebas de seguridad: Realizar pruebas de penetración y evaluaciones de seguridad de forma regular para identificar posibles debilidades en la implementación de la encriptación y corregirlas de manera oportuna.

El proceso de encriptación de datos sensibles en reposo y en tránsito se centra en proteger la confidencialidad e integridad de los datos sensibles almacenados y transmitidos. Se implementan controles como políticas de encriptación, uso de algoritmos de encriptación seguros, gestión de claves, encriptación de datos en reposo y en tránsito, certificados y protocolos seguros, administración de certificados, monitoreo y detección de fallas de encriptación, actualización y parches de seguridad, y pruebas de seguridad. Estos controles aseguran que los datos sensibles estén protegidos contra accesos no autorizados y garantizan que la información se transmita de manera segura a través de redes y comunicaciones.

d) Proceso: Copias de seguridad y recuperación de datos.

- Activo de información: Datos críticos y sensibles almacenados en sistemas y dispositivos.
- Riesgo: Riesgo de pérdida, corrupción o acceso no autorizado a los datos debido a fallos técnicos, desastres naturales, errores humanos o ataques cibernéticos.
- Controles:
  - Políticas de copias de seguridad: Establecer políticas claras para la realización de copias de seguridad periódicas de los datos críticos, definiendo la frecuencia, la metodología y los medios de almacenamiento utilizados.
  - Identificación de datos críticos: Identificar los datos críticos que deben ser respaldados, considerando su importancia y valor para la organización.
  - Plan de recuperación ante desastres: Desarrollar un plan de recuperación ante desastres que incluya procedimientos detallados para restaurar los datos en caso de un evento catastrófico, como incendios, inundaciones o terremotos.
  - Procedimientos de respaldo: Establecer procedimientos claros y documentados para realizar las copias de seguridad de forma segura y eficiente, incluyendo la selección de los sistemas y dispositivos de respaldo, la programación de las copias de seguridad y la verificación de su integridad.
  - Almacenamiento seguro de las copias de seguridad: Garantizar que las copias de seguridad se almacenen en medios seguros y protegidos, como discos duros externos, cintas magnéticas o servicios de almacenamiento en la nube, asegurando su confidencialidad, integridad y disponibilidad.
  - Pruebas de restauración: Realizar pruebas periódicas de restauración de las copias de seguridad para verificar que los datos puedan ser recuperados de manera efectiva y que sean utilizables en caso de necesidad.

- Retención y eliminación de copias de seguridad: Establecer políticas de retención de las copias de seguridad, determinando el período de tiempo durante el cual se conservarán y definir procedimientos seguros para la eliminación de las copias de seguridad obsoletas.
- Seguridad física y lógica: Implementar medidas de seguridad física y lógica para proteger las copias de seguridad de accesos no autorizados, como controles de acceso a los medios de almacenamiento, encriptación de datos y autenticación de usuarios autorizados.
- Capacitación y concientización: Capacitar al personal involucrado en el proceso de copias de seguridad y recuperación de datos, para asegurar una correcta ejecución de los procedimientos y promover la importancia de la protección de los datos.
- Actualización y revisión del plan: Mantener el plan de copias de seguridad y recuperación de datos actualizado, revisándolo periódicamente para garantizar su eficacia y adecuación a los cambios en los sistemas de información y las necesidades de la organización.

El proceso de copias de seguridad y recuperación de datos es esencial para garantizar la disponibilidad y la integridad de los datos críticos de la organización. Los controles implementados, como las políticas de copias de seguridad, el plan de recuperación ante desastres, los procedimientos de respaldo, el almacenamiento seguro de las copias de seguridad y las pruebas de restauración, aseguran que los datos puedan ser recuperados en caso de pérdida o corrupción, minimizando así el impacto en la continuidad del negocio.

e) Proceso: Retención y eliminación segura de datos obsoletos.

- Activo de información: Datos obsoletos almacenados en sistemas y dispositivos.
- Riesgo: Riesgo de violación de la privacidad, pérdida de confidencialidad o incumplimiento de regulaciones debido a la retención prolongada de datos obsoletos.
- Controles:
  - Política de retención de datos: Establecer una política clara que defina el período de retención de los datos, considerando requisitos legales, regulatorios y de la organización.
  - Identificación de datos obsoletos: Identificar y categorizar los datos obsoletos que ya no son necesarios para fines comerciales, legales o regulatorios.
  - Evaluación de riesgos: Evaluar los riesgos asociados con la retención de datos obsoletos, como la exposición a violaciones de seguridad, demandas legales o sanciones regulatorias.
  - Procedimientos de eliminación: Establecer procedimientos seguros y documentados para la eliminación de datos obsoletos, utilizando métodos adecuados como el borrado seguro, la destrucción física o el anonimato de los datos.
  - Cumplimiento legal y regulatorio: Asegurar que la eliminación de datos obsoletos cumpla con los requisitos legales y regulatorios aplicables, como la Ley de Protección de Datos y regulaciones de privacidad.

- Auditoría y seguimiento: Realizar auditorías periódicas para verificar el cumplimiento de los procedimientos de retención y eliminación de datos, y llevar un registro de las acciones realizadas.
- Capacitación y concientización: Capacitar al personal sobre la importancia de la retención y eliminación segura de datos obsoletos, así como sobre los procedimientos y políticas establecidos.
- Gestión de respaldos: Asegurar que los datos obsoletos almacenados en respaldos o archivos de almacenamiento secundario también sean identificados y eliminados de forma segura.
- Colaboración con otras áreas: Establecer una comunicación y colaboración efectiva con los departamentos de cumplimiento, legal y tecnología de la información para asegurar el cumplimiento normativo y garantizar la eliminación segura de los datos.
- Revisión y mejora continua: Realizar revisiones periódicas del proceso de retención y eliminación de datos para identificar áreas de mejora y adaptarse a los cambios en la normativa y las prácticas recomendadas.

El proceso de retención y eliminación segura de datos obsoletos es esencial para mantener la privacidad y la seguridad de la información. La implementación de los controles mencionados, como la política de retención, los procedimientos de eliminación y el cumplimiento legal y regulatorio, ayuda a minimizar los riesgos asociados con la retención prolongada de datos obsoletos y garantiza el cumplimiento de las regulaciones de protección de datos.

3. Macroproceso – Gestión de Parches y Actualizaciones

a) Proceso: Implementación de un proceso de gestión de parches y actualizaciones para sistemas y aplicaciones.

- Activo de información: Sistemas y aplicaciones utilizados en la organización.
- Riesgo: Riesgo de vulnerabilidades y brechas de seguridad debido a la falta de actualizaciones y parches en sistemas y aplicaciones.
- Controles:
  - Identificación de sistemas y aplicaciones: Identificar todos los sistemas y aplicaciones utilizados en la organización que requieren parches y actualizaciones.
  - Monitoreo de avisos de seguridad: Establecer un proceso para monitorear y recibir avisos de seguridad y actualizaciones de los proveedores de sistemas y aplicaciones.
  - Evaluación de impacto y priorización: Evaluar el impacto potencial de las actualizaciones y parches en los sistemas y aplicaciones, y priorizar las acciones de acuerdo con su criticidad y riesgo asociado.
  - Pruebas de compatibilidad: Realizar pruebas de compatibilidad de las actualizaciones y parches en entornos de prueba para verificar su funcionamiento adecuado y evitar conflictos con otras aplicaciones o sistemas.
  - Programación y despliegue de actualizaciones: Establecer un calendario para la implementación de las actualizaciones y parches, considerando

horarios de menor impacto en la operación y coordinando con los responsables de los sistemas y aplicaciones.
- Seguimiento y control: Realizar un seguimiento constante de las actualizaciones y parches implementados, asegurando que se realicen de manera completa y exitosa, y mantener registros actualizados.
- Automatización: Utilizar herramientas de gestión de parches y actualizaciones que faciliten el proceso y permitan automatizar tareas como la descarga, distribución e instalación de los parches.
- Capacitación y concientización: Capacitar al personal involucrado en la gestión de parches y actualizaciones, asegurando que estén familiarizados con los procedimientos y buenas prácticas, y concienciar sobre la importancia de mantener los sistemas y aplicaciones actualizados.
- Monitoreo de cumplimiento: Realizar monitoreo periódico para asegurar que todas las actualizaciones y parches necesarios se implementen de manera oportuna y que no existan sistemas o aplicaciones desactualizadas.
- Mejora continua: Evaluar regularmente el proceso de gestión de parches y actualizaciones, identificar áreas de mejora y actualizar las políticas y procedimientos según sea necesario.

La implementación de un proceso de gestión de parches y actualizaciones es crucial para mantener la seguridad de los sistemas y aplicaciones utilizados en la organización. Los controles mencionados, como la identificación, evaluación, programación, seguimiento y automatización, ayudan a garantizar que los sistemas y aplicaciones estén actualizados y protegidos contra posibles vulnerabilidades y amenazas. Asimismo, la capacitación del personal y el monitoreo de cumplimiento son fundamentales para asegurar que el proceso se lleve a cabo de manera efectiva y consistente, y para fomentar una cultura de seguridad informática en la organización.

b) Proceso: Evaluación de vulnerabilidades y aplicación de parches de seguridad.

- Activo de información: Sistemas y aplicaciones utilizados en la organización.
- Riesgo: Riesgo de explotación de vulnerabilidades y brechas de seguridad debido a la falta de evaluación y aplicación de parches de seguridad.
- Controles:
  - Identificación de sistemas y aplicaciones: Identificar todos los sistemas y aplicaciones utilizados en la organización que requieren evaluación de vulnerabilidades y aplicación de parches de seguridad.
  - Escaneo de vulnerabilidades: Realizar escaneos regulares de vulnerabilidades en los sistemas y aplicaciones utilizando herramientas especializadas, con el fin de identificar posibles brechas de seguridad.
  - Evaluación de riesgos: Evaluar el impacto potencial de las vulnerabilidades identificadas y priorizar las acciones de acuerdo con su criticidad y riesgo asociado.
  - Aplicación de parches: Descargar y aplicar los parches de seguridad proporcionados por los proveedores de los sistemas y aplicaciones para solucionar las vulnerabilidades identificadas.
  - Pruebas de parches: Realizar pruebas de los parches aplicados en entornos de prueba para verificar su funcionamiento adecuado y evitar conflictos con otras aplicaciones o sistemas.

- Planificación y programación: Establecer un calendario para la aplicación de los parches de seguridad, considerando horarios de menor impacto en la operación y coordinando con los responsables de los sistemas y aplicaciones.
- Seguimiento y control: Realizar un seguimiento constante de la aplicación de los parches de seguridad, asegurando que se realicen de manera completa y exitosa, y mantener registros actualizados.
- Capacitación y concientización: Capacitar al personal involucrado en la evaluación de vulnerabilidades y aplicación de parches de seguridad, asegurando que estén familiarizados con los procedimientos y buenas prácticas, y concienciar sobre la importancia de mantener los sistemas actualizados.
- Monitoreo de cumplimiento: Realizar monitoreo periódico para asegurar que todas las evaluaciones de vulnerabilidades y aplicaciones de parches necesarios se realicen de manera oportuna y que no existan sistemas o aplicaciones desactualizadas.
- Mejora continua: Evaluar regularmente el proceso de evaluación de vulnerabilidades y aplicación de parches de seguridad, identificar áreas de mejora y actualizar las políticas y procedimientos según sea necesario.

La evaluación de vulnerabilidades y aplicación de parches de seguridad es esencial para mantener la seguridad de los sistemas y aplicaciones utilizados en la organización. Los controles mencionados, como la identificación, escaneo, evaluación, aplicación y seguimiento de parches de seguridad, ayudan a garantizar que las vulnerabilidades sean identificadas y solucionadas de manera oportuna, reduciendo el riesgo de posibles ataques o explotaciones. Además, la capacitación del personal y el monitoreo de cumplimiento son fundamentales para asegurar que el proceso se lleve a cabo de manera efectiva y consistente, y para promover una cultura de seguridad informática en la organización.

c) Proceso: Mantenimiento y actualización de los sistemas operativos y software de seguridad.

- Activo de información: Sistemas operativos y software de seguridad utilizados en la organización.
- Riesgo: Riesgo de brechas de seguridad y explotación de vulnerabilidades debido a la falta de mantenimiento y actualización de los sistemas operativos y software de seguridad.
- Controles:
  - Inventario de sistemas y software: Realizar un inventario completo de los sistemas operativos y software de seguridad utilizados en la organización.
  - Monitoreo de alertas y actualizaciones: Mantenerse informado sobre las alertas de seguridad y las actualizaciones proporcionadas por los proveedores de los sistemas operativos y software de seguridad.
  - Evaluación de impacto y priorización: Evaluar el impacto potencial de las actualizaciones en los sistemas y software, priorizando las actualizaciones críticas y de seguridad.
  - Planificación y programación: Establecer un calendario para el mantenimiento y actualización de los sistemas operativos y software de

seguridad, considerando horarios de menor impacto en la operación y coordinando con los responsables de los sistemas.
- Pruebas de actualizaciones: Realizar pruebas de las actualizaciones en entornos de prueba para verificar su funcionamiento adecuado y evitar conflictos con otros sistemas o software.
- Implementación de actualizaciones: Aplicar las actualizaciones en los sistemas operativos y software de seguridad de acuerdo con la planificación establecida.
- Verificación de la actualización: Realizar verificaciones posteriores a la actualización para asegurarse de que las actualizaciones se hayan aplicado correctamente y que los sistemas estén funcionando de manera adecuada.
- Monitoreo de cumplimiento: Realizar un monitoreo periódico para asegurarse de que todas las actualizaciones necesarias se realicen de manera oportuna y que no existan sistemas desactualizados.
- Capacitación y concientización: Capacitar al personal involucrado en el mantenimiento y actualización de los sistemas operativos y software de seguridad, asegurando que estén familiarizados con los procedimientos y buenas prácticas, y concienciar sobre la importancia de mantener los sistemas actualizados.
- Mejora continua: Evaluar regularmente el proceso de mantenimiento y actualización de los sistemas operativos y software de seguridad, identificar áreas de mejora y actualizar las políticas y procedimientos según sea necesario.

El mantenimiento y actualización de los sistemas operativos y software de seguridad es fundamental para garantizar un entorno seguro en la organización. Los controles mencionados, como el monitoreo de alertas, evaluación de impacto, planificación, pruebas e implementación de actualizaciones, ayudan a asegurar que los sistemas operativos y software de seguridad estén actualizados y protegidos contra las últimas amenazas y vulnerabilidades. Además, la capacitación del personal y el monitoreo de cumplimiento son importantes para garantizar que el proceso se lleve a cabo de manera efectiva y consistente, y para promover una cultura de seguridad informática en la organización.

4. Macroproceso – Monitorización y Detección de Intrusiones

a) Proceso: Implementación de sistemas de detección y prevención de intrusiones.

- Activo de información: Sistemas de detección y prevención de intrusiones (IDS/IPS) implementados en la infraestructura de seguridad de la organización.
- Riesgo: Riesgo de intrusiones no autorizadas y actividades maliciosas en la red y sistemas de la organización.
- Controles:
  - Selección de soluciones IDS/IPS: Evaluar y seleccionar soluciones de detección y prevención de intrusiones adecuadas para las necesidades de la organización, considerando funcionalidades, compatibilidad con la infraestructura existente y capacidad de respuesta a amenazas conocidas y emergentes.

- Configuración y despliegue de los sistemas IDS/IPS: Implementar y configurar los sistemas de detección y prevención de intrusiones en la infraestructura de la red y sistemas de la organización, considerando las mejores prácticas de configuración y las directrices del fabricante.
- Monitoreo y análisis de eventos: Establecer un proceso de monitoreo continuo de eventos de seguridad capturados por los sistemas IDS/IPS, analizando las alertas generadas y tomando medidas adecuadas ante posibles intrusiones o actividades sospechosas.
- Actualización y mantenimiento: Mantener los sistemas IDS/IPS actualizados con las últimas firmas de amenazas y parches de seguridad proporcionados por los fabricantes, asegurando su eficacia y capacidad de detección.
- Gestión de incidentes: Establecer procedimientos claros para la gestión de incidentes de seguridad detectados por los sistemas IDS/IPS, incluyendo la notificación, la respuesta y la recuperación.
- Integración con otros sistemas de seguridad: Integrar los sistemas IDS/IPS con otros controles de seguridad existentes, como firewalls, sistemas de gestión de registros y sistemas de autenticación, para obtener una visión más completa de la seguridad y mejorar la capacidad de detección y respuesta.
- Capacitación y concientización: Capacitar al personal encargado del monitoreo y análisis de eventos de los sistemas IDS/IPS, así como al personal de respuesta a incidentes, en el uso adecuado de las herramientas y en las técnicas de detección y prevención de intrusiones.
- Evaluación y mejora continua: Realizar evaluaciones periódicas de la eficacia de los sistemas IDS/IPS, revisar los registros de eventos, analizar los incidentes detectados y realizar ajustes y mejoras en la configuración y despliegue de los sistemas para aumentar su eficacia y adaptabilidad.

La implementación de sistemas de detección y prevención de intrusiones es esencial para identificar y mitigar posibles intrusiones y actividades maliciosas en los sistemas y redes de la organización. Los controles mencionados, como la selección de soluciones adecuadas, la configuración y despliegue correctos, el monitoreo y análisis de eventos, la actualización y mantenimiento, la gestión de incidentes, la integración con otros sistemas de seguridad, la capacitación del personal y la evaluación continua, contribuyen a fortalecer la seguridad de la organización y a proteger los activos de información frente a amenazas externas.

b) Proceso: Monitorización de eventos y registros de seguridad.

- Activo de información: Eventos y registros de seguridad generados por los sistemas y aplicaciones de la organización.
- Riesgo: Riesgo de incidentes de seguridad no detectados y actividades maliciosas no identificadas en los sistemas y redes de la organización.
- Controles:
  - Recopilación y centralización de registros: Implementar una solución de gestión de registros (SIEM) que permita recopilar y centralizar los registros de eventos de seguridad generados por los diferentes sistemas y aplicaciones de la organización.

- Configuración de fuentes de registro: Configurar los sistemas y aplicaciones para que generen los registros de eventos de seguridad pertinentes y asegurar que se envíen correctamente a la solución de gestión de registros.
- Monitoreo en tiempo real: Establecer un proceso de monitoreo continuo de los eventos de seguridad en tiempo real, utilizando la solución de gestión de registros para detectar actividades sospechosas, patrones anómalos y posibles incidentes de seguridad.
- Análisis y correlación de eventos: Realizar análisis y correlación de los eventos de seguridad recopilados, utilizando técnicas y herramientas adecuadas, para identificar posibles incidentes y patrones de comportamiento malicioso.
- Respuesta a incidentes: Establecer procedimientos claros para la gestión de incidentes de seguridad detectados a través de los eventos y registros de seguridad, incluyendo la notificación, la respuesta y la recuperación.
- Generación de informes y alertas: Configurar la solución de gestión de registros para generar informes periódicos y alertas automáticas sobre eventos de seguridad relevantes, facilitando la toma de decisiones y la respuesta oportuna a posibles incidentes.
- Mantenimiento y actualización: Mantener la solución de gestión de registros actualizada con las últimas actualizaciones y parches de seguridad, garantizando su funcionamiento óptimo y la capacidad de gestionar de manera eficiente los eventos y registros de seguridad.
- Capacitación y concientización: Capacitar al personal encargado de la monitorización y análisis de eventos de seguridad, así como al personal de respuesta a incidentes, en el uso adecuado de la solución de gestión de registros, las técnicas de análisis de eventos y la detección de incidentes de seguridad.
- Auditoría y revisión: Realizar auditorías periódicas de la eficacia y cumplimiento de los controles de monitorización de eventos y registros de seguridad, revisar los informes generados, analizar los incidentes detectados y realizar ajustes y mejoras en los procesos y configuraciones según sea necesario.

La monitorización de eventos y registros de seguridad es esencial para identificar y responder de manera temprana a posibles incidentes de seguridad en los sistemas y redes de la organización. Los controles mencionados, como la recopilación y centralización de registros, el monitoreo en tiempo real, el análisis y correlación de eventos, la respuesta a incidentes, la generación de informes y alertas, el mantenimiento y actualización de la solución, la capacitación del personal y la auditoría y revisión continua, contribuyen a fortalecer la detección y respuesta ante posibles amenazas de seguridad y a garantizar la integridad y confidencialidad de los activos de información de la organización.

c) Proceso: Análisis de incidentes de seguridad y respuesta ante intrusiones.

- Activo de información: Incidentes de seguridad y eventos de intrusión que afectan los sistemas y la infraestructura de la organización.

- Riesgo: Riesgo de exposición de información confidencial, daño a la reputación de la organización y pérdida de la disponibilidad de los sistemas debido a incidentes de seguridad e intrusiones.
- Controles:
    - Detección de incidentes: Implementar sistemas de detección de intrusiones y herramientas de monitorización que ayuden a identificar de manera proactiva posibles incidentes de seguridad y eventos de intrusión.
    - Notificación y registro: Establecer un proceso claro y eficiente para la notificación y registro de incidentes de seguridad, asegurando que se recolecte toda la información relevante para el análisis posterior.
    - Análisis forense: Realizar un análisis forense de los incidentes de seguridad y eventos de intrusión para determinar su alcance, identificar los puntos de entrada, las técnicas utilizadas y las acciones realizadas por los intrusos.
    - Respuesta y contención: Desarrollar un plan de respuesta ante incidentes que defina las acciones a tomar en caso de una intrusión confirmada, incluyendo la contención del incidente, la minimización del impacto y la preservación de la evidencia.
    - Recuperación y restauración: Establecer procedimientos para la recuperación de los sistemas afectados por incidentes de seguridad, incluyendo la restauración de los datos y la implementación de medidas correctivas para prevenir futuras intrusiones.
    - Comunicación y divulgación: Establecer un proceso de comunicación interna y externa para informar a las partes interesadas sobre los incidentes de seguridad, incluyendo a la alta dirección, el personal afectado, los clientes y las autoridades pertinentes.
    - Aprendizaje y mejora continua: Realizar una revisión post-incidente para identificar las lecciones aprendidas, las áreas de mejora y las recomendaciones para fortalecer la seguridad de la información de la organización.
    - Actualización y prueba de los planes: Mantener los planes de respuesta ante incidentes actualizados y realizar pruebas periódicas para evaluar su efectividad y hacer los ajustes necesarios.
    - Colaboración con equipos externos: Establecer acuerdos de colaboración con equipos de respuesta a incidentes externos, como organismos gubernamentales o proveedores de servicios de ciberseguridad, para recibir apoyo y asesoramiento en el manejo de incidentes graves.

El análisis de incidentes de seguridad y la respuesta ante intrusiones son fundamentales para minimizar el impacto de las amenazas cibernéticas y garantizar la continuidad de los sistemas de información de la organización. Los controles mencionados, como la detección proactiva, el análisis forense, la respuesta y contención, la recuperación y restauración, la comunicación y divulgación, el aprendizaje continuo, la actualización y prueba de los planes, y la colaboración con equipos externos, permiten una respuesta efectiva ante incidentes de seguridad, la mitigación de sus efectos y la mejora continua de las medidas de seguridad implementadas.

d) Proceso: Evaluación de la actividad de la red y sistemas en busca de comportamientos anómalos.

- Activo de información: La red y los sistemas de la organización.
- Riesgo: Riesgo de intrusiones, actividades maliciosas y uso no autorizado de los sistemas y recursos de la organización.
- Controles:
    - Implementación de sistemas de detección de intrusos (IDS): Utilizar herramientas y tecnologías especializadas para monitorear la actividad de la red y sistemas, identificando posibles comportamientos anómalos o actividades sospechosas.
    - Análisis de logs y registros: Examinar de manera regular los registros de actividad de la red y sistemas, en busca de patrones inusuales o eventos que puedan indicar una violación de seguridad.
    - Monitoreo de tráfico de red: Supervisar el tráfico de red en tiempo real para identificar cualquier actividad sospechosa, como comunicaciones no autorizadas o transferencia de datos sensibles.
    - Análisis de comportamiento: Utilizar herramientas y técnicas de análisis de comportamiento para detectar desviaciones significativas de los patrones normales de uso de la red y sistemas.
    - Uso de firmas y reglas de detección: Configurar sistemas de detección con firmas y reglas específicas para identificar actividades maliciosas conocidas o comportamientos anómalos previamente identificados.
    - Generación de alertas y notificaciones: Establecer un mecanismo de generación de alertas y notificaciones en caso de detectarse actividad sospechosa, permitiendo una respuesta rápida y eficiente.
    - Investigación y respuesta: Desarrollar procedimientos para investigar las alertas generadas, determinar la naturaleza y el alcance del incidente, y tomar las medidas necesarias para mitigar los riesgos identificados.
    - Actualización y mejora continua: Mantener actualizados los sistemas de detección y análisis, incorporando nuevas firmas, reglas y técnicas de detección a medida que surjan nuevas amenazas y vulnerabilidades.
    - Capacitación y concienciación: Proporcionar capacitación regular a los usuarios y al personal de TI sobre la detección de comportamientos anómalos y la importancia de informar cualquier actividad sospechosa.

La evaluación de la actividad de la red y sistemas en busca de comportamientos anómalos es esencial para detectar posibles amenazas y actividades maliciosas en tiempo real. Los controles mencionados, como la implementación de sistemas de detección de intrusos, el análisis de logs y registros, el monitoreo de tráfico de red, el análisis de comportamiento, el uso de firmas y reglas de detección, la generación de alertas y notificaciones, la investigación y respuesta, la actualización y mejora continua, y la capacitación y concienciación, ayudan a identificar y responder rápidamente a las amenazas y vulnerabilidades, minimizando el impacto de posibles intrusiones y garantizando la seguridad de los sistemas de información de la organización.

5. Macroproceso – Gestión de Proveedores y Terceros

a) Proceso: Evaluación de la seguridad de los proveedores y terceros.

- Activo de información: Los servicios, productos o datos proporcionados por los proveedores y terceros a la organización.
- Riesgo: Riesgo de comprometer la seguridad de la información y los sistemas de la organización debido a las prácticas de seguridad inadecuadas o insuficientes de los proveedores y terceros.
- Controles:
    - Evaluación de la seguridad de los proveedores: Realizar una evaluación exhaustiva de la seguridad de los proveedores y terceros antes de establecer una relación comercial o de intercambio de información. Esto puede incluir la revisión de sus políticas de seguridad, controles de acceso, gestión de incidentes, cumplimiento normativo, entre otros aspectos relevantes.
    - Acuerdos y contratos de seguridad: Establecer acuerdos y contratos con los proveedores y terceros que incluyan cláusulas de seguridad específicas, tales como la protección de datos, confidencialidad, notificación de incidentes de seguridad y cumplimiento de normas y regulaciones.
    - Evaluación periódica: Realizar evaluaciones periódicas de la seguridad de los proveedores y terceros para garantizar que sigan cumpliendo con los estándares y requisitos de seguridad establecidos.
    - Auditorías de seguridad: Realizar auditorías de seguridad de manera regular para verificar el cumplimiento de los proveedores y terceros con las políticas y estándares de seguridad establecidos.
    - Gestión de incidentes: Establecer un proceso claro para la gestión de incidentes de seguridad relacionados con los proveedores y terceros, incluyendo la notificación de incidentes, la colaboración en la resolución y la implementación de medidas correctivas.
    - Monitorización y reporte: Implementar mecanismos de monitorización continua de las actividades de los proveedores y terceros, así como de la seguridad de la información compartida, y generar informes regulares sobre el estado de la seguridad.
    - Educación y concienciación: Proporcionar capacitación y concienciación a los empleados sobre la importancia de evaluar y gestionar la seguridad de los proveedores y terceros, así como sobre las mejores prácticas en la selección y colaboración con ellos.
    - Plan de contingencia: Desarrollar un plan de contingencia que contemple acciones a seguir en caso de que un proveedor o tercero experimente un incidente de seguridad que pueda afectar a la organización.
    - Evaluación de cumplimiento normativo: Verificar que los proveedores y terceros cumplan con las regulaciones y normativas aplicables, como la protección de datos personales, la privacidad y la seguridad de la información.

La evaluación de la seguridad de los proveedores y terceros es fundamental para garantizar la protección de la información y los sistemas de la organización. Los controles mencionados, como la evaluación de la seguridad de los proveedores, los acuerdos y contratos de seguridad, las evaluaciones periódicas, las auditorías de seguridad, la gestión de incidentes, la monitorización y reporte, la educación y concienciación, el plan de contingencia y la evaluación de cumplimiento normativo, ayudan a mitigar los riesgos asociados con los proveedores y terceros, asegurando

que cumplan con los estándares de seguridad establecidos y protegiendo los intereses de la organización.

b) Proceso: Establecimiento de acuerdos de seguridad y cláusulas de confidencialidad.

- Activo de información: Los datos, información confidencial y propiedad intelectual compartidos con terceros o socios comerciales.
- Riesgo: Riesgo de divulgación no autorizada, acceso no autorizado, uso indebido o mal uso de la información confidencial o propiedad intelectual por parte de terceros.
- Controles:
    - Evaluación de riesgos: Realizar una evaluación de riesgos para identificar los posibles riesgos asociados con el intercambio de información confidencial y propiedad intelectual con terceros.
    - Acuerdos de seguridad: Establecer acuerdos de seguridad claros y detallados con los terceros, que incluyan cláusulas de confidencialidad, protección de datos, responsabilidades y obligaciones de ambas partes en relación con la seguridad de la información.
    - Requisitos de seguridad: Especificar los requisitos de seguridad mínimos que los terceros deben cumplir para proteger la información confidencial y la propiedad intelectual, como la implementación de controles técnicos y organizativos adecuados.
    - Evaluación y selección de terceros: Realizar una evaluación exhaustiva de la seguridad de los terceros antes de establecer una relación comercial, considerando su historial de seguridad, prácticas de seguridad y capacidad para cumplir con los requisitos establecidos.
    - Cláusulas de confidencialidad: Incluir cláusulas de confidencialidad en los acuerdos que obliguen a los terceros a mantener la confidencialidad de la información recibida, así como a no divulgarla o utilizarla para fines no autorizados.
    - Auditorías y revisiones periódicas: Realizar auditorías y revisiones periódicas de los terceros para verificar su cumplimiento con los acuerdos de seguridad y las cláusulas de confidencialidad, y para asegurarse de que siguen implementando las medidas de seguridad requeridas.
    - Gestión de incidentes: Establecer un proceso claro para la gestión de incidentes de seguridad relacionados con los terceros, incluyendo la notificación de incidentes, la colaboración en la resolución y la implementación de medidas correctivas.
    - Capacitación y concienciación: Proporcionar capacitación y concienciación a los empleados sobre la importancia de los acuerdos de seguridad y las cláusulas de confidencialidad, así como sobre las mejores prácticas en la protección de la información confidencial.
    - Actualización y renovación: Revisar y actualizar regularmente los acuerdos de seguridad y las cláusulas de confidencialidad para asegurarse de que sigan siendo adecuados y estén alineados con los cambios en la organización y las regulaciones aplicables.

El establecimiento de acuerdos de seguridad y cláusulas de confidencialidad es esencial para proteger la información confidencial y la propiedad intelectual

compartida con terceros. Los controles mencionados, como la evaluación de riesgos, los acuerdos de seguridad, los requisitos de seguridad, la evaluación y selección de terceros, las cláusulas de confidencialidad, las auditorías y revisiones periódicas, la gestión de incidentes, la capacitación y concienciación, y la actualización y renovación, ayudarán a garantizar que los terceros cumplan con los estándares de seguridad establecidos y protejan los intereses de la organización.

c) Proceso: Supervisión y auditoría de los proveedores y terceros.

- Activo de información: Los datos, información confidencial y propiedad intelectual compartidos con proveedores y terceros.
- Riesgo: Riesgo de incumplimiento de los acuerdos de seguridad, divulgación no autorizada, acceso no autorizado, uso indebido o mal uso de la información confidencial o propiedad intelectual por parte de proveedores y terceros.
- Controles:
    - Planificación de auditorías: Establecer un plan de auditorías periódicas para evaluar el cumplimiento de los proveedores y terceros con los acuerdos de seguridad, requisitos legales y regulaciones aplicables.
    - Evaluación de cumplimiento: Realizar evaluaciones periódicas de cumplimiento, que pueden incluir cuestionarios, revisiones de documentación y pruebas técnicas, para verificar si los proveedores y terceros están cumpliendo con los requisitos de seguridad establecidos.
    - Auditorías en el sitio: Realizar auditorías en el sitio de los proveedores y terceros para evaluar la implementación de controles de seguridad, la protección de la información confidencial y la propiedad intelectual, y la gestión de riesgos asociados.
    - Revisiones de políticas y procedimientos: Revisar las políticas y procedimientos de los proveedores y terceros para asegurarse de que sean adecuados y estén alineados con los requisitos de seguridad.
    - Evaluación de incidentes de seguridad: Evaluar y revisar los incidentes de seguridad que involucren a proveedores y terceros, analizando las causas, el impacto y las medidas de mitigación implementadas para evitar futuros incidentes.
    - Reporte y seguimiento: Generar informes de auditoría que detallen los hallazgos, las recomendaciones y las medidas correctivas necesarias. Realizar un seguimiento de las acciones correctivas para garantizar su implementación oportuna y eficaz.
    - Evaluación de continuidad del servicio: Evaluar la capacidad de los proveedores y terceros para mantener la continuidad del servicio en caso de incidentes de seguridad o interrupciones operativas.
    - Gestión de cambios: Supervisar y evaluar los cambios propuestos por los proveedores y terceros para asegurarse de que no introduzcan riesgos adicionales y cumplan con los requisitos de seguridad establecidos.
    - Reevaluación periódica: Realizar reevaluaciones periódicas de los proveedores y terceros para asegurarse de que sigan cumpliendo con los estándares de seguridad y que se mantenga la confianza en la relación comercial.

La supervisión y auditoría de los proveedores y terceros es esencial para garantizar su cumplimiento con los acuerdos de seguridad y proteger la información confidencial y la propiedad intelectual compartida. Los controles mencionados, como la planificación de auditorías, la evaluación de cumplimiento, las auditorías en el sitio, las revisiones de políticas y procedimientos, la evaluación de incidentes de seguridad, el reporte y seguimiento, la evaluación de continuidad del servicio, la gestión de cambios y la reevaluación periódica, ayudarán a mantener un monitoreo constante y garantizar un alto nivel de seguridad en las relaciones con proveedores y terceros.

6. Macroproceso – Concientización y Formación en Seguridad

a) Proceso: Programas de concientización y formación en seguridad de la información para los empleados.

- Activo de información: Los empleados y su conocimiento sobre las prácticas adecuadas de seguridad de la información.
- Riesgo: Riesgo de violaciones de seguridad de la información debido a la falta de conciencia y conocimiento por parte de los empleados.
- Controles:
    - Desarrollo de programas de capacitación: Diseñar programas de capacitación en seguridad de la información que aborden temas como la protección de datos, contraseñas seguras, uso adecuado del correo electrónico, navegación segura por Internet y detección de amenazas.
    - Sesiones de concientización: Realizar sesiones periódicas de concientización para educar a los empleados sobre las políticas y prácticas de seguridad de la información de la organización, destacando los riesgos asociados y las medidas de mitigación.
    - Materiales de formación: Proporcionar materiales de formación, como guías, manuales y recursos en línea, que los empleados puedan consultar para obtener información adicional sobre seguridad de la información.
    - Simulaciones y ejercicios prácticos: Realizar simulaciones y ejercicios prácticos, como pruebas de phishing y simulacros de incidentes de seguridad, para ayudar a los empleados a identificar y responder adecuadamente a posibles amenazas.
    - Evaluaciones de conocimientos: Realizar evaluaciones periódicas para medir el nivel de conocimiento de los empleados sobre seguridad de la información y identificar áreas de mejora.
    - Comunicación continua: Mantener una comunicación regular y abierta con los empleados sobre las actualizaciones y cambios en las políticas y prácticas de seguridad de la información, fomentando la participación activa y el intercambio de información.
    - Participación en programas de certificación: Promover la participación de los empleados en programas de certificación en seguridad de la información, que les brinden habilidades y conocimientos avanzados en el campo.

- Reconocimiento y recompensas: Reconocer y recompensar a los empleados que demuestren un alto nivel de conciencia y cumplimiento de las políticas de seguridad de la información, fomentando una cultura de seguridad positiva.
- Retroalimentación y mejora continua: Recopilar comentarios de los empleados sobre los programas de capacitación y realizar ajustes y mejoras periódicas para garantizar su efectividad y relevancia.

Los programas de concientización y formación en seguridad de la información son fundamentales para crear una cultura de seguridad sólida en la organización y mitigar los riesgos asociados a la falta de conocimiento y conciencia de los empleados. Los controles mencionados, como el desarrollo de programas de capacitación, sesiones de concientización, materiales de formación, simulaciones y ejercicios prácticos, evaluaciones de conocimientos, comunicación continua, participación en programas de certificación, reconocimiento y recompensas, y retroalimentación y mejora continua, ayudarán a fortalecer el conocimiento y la conciencia de seguridad de los empleados, reduciendo así el riesgo de violaciones de seguridad de la información.

b) Proceso: Educación sobre prácticas seguras, políticas y procedimientos.

- Activo de información: El conocimiento y comprensión de los empleados sobre las prácticas seguras, políticas y procedimientos de seguridad de la información.
- Riesgo: Riesgo de violaciones de seguridad de la información debido a la falta de conocimiento o comprensión de las prácticas seguras, políticas y procedimientos establecidos.
- Controles:
  - Desarrollo de materiales educativos: Crear materiales educativos, como manuales, guías y recursos en línea, que expliquen las prácticas seguras, políticas y procedimientos de seguridad de la información de la organización.
  - Sesiones de capacitación: Realizar sesiones de capacitación periódicas para educar a los empleados sobre las prácticas seguras, políticas y procedimientos relevantes. Estas sesiones pueden ser presenciales, en línea o una combinación de ambas.
  - Comunicación clara de las políticas: Asegurarse de que las políticas y procedimientos de seguridad de la información estén claramente documentados y disponibles para todos los empleados.
  - Orientación para nuevos empleados: Incluir capacitación sobre las prácticas seguras, políticas y procedimientos de seguridad de la información como parte del programa de orientación para nuevos empleados.
  - Pruebas de conocimientos: Realizar pruebas periódicas para evaluar el conocimiento y comprensión de los empleados sobre las prácticas seguras, políticas y procedimientos de seguridad de la información.
  - Actualizaciones regulares: Mantener los materiales educativos y las políticas actualizadas para reflejar los cambios en el entorno de seguridad de la información y comunicar estas actualizaciones a los empleados.

- Promoción de la responsabilidad individual: Fomentar la responsabilidad individual de los empleados en la adhesión a las prácticas seguras, políticas y procedimientos establecidos, resaltando la importancia de su papel en la seguridad de la información de la organización.
- Retroalimentación y consultas: Establecer canales de retroalimentación y consultas para que los empleados puedan plantear preguntas o inquietudes sobre las prácticas seguras, políticas y procedimientos, y recibir orientación adicional si es necesario.
- Monitoreo y cumplimiento: Realizar un monitoreo regular para asegurarse de que los empleados sigan las prácticas seguras, políticas y procedimientos establecidos, y tomar medidas correctivas en caso de incumplimiento.

La educación sobre prácticas seguras, políticas y procedimientos es esencial para garantizar que los empleados estén bien informados y comprendan cómo proteger la información de la organización de manera efectiva. Los controles mencionados, como el desarrollo de materiales educativos, sesiones de capacitación, comunicación clara de las políticas, orientación para nuevos empleados, pruebas de conocimientos, actualizaciones regulares, promoción de la responsabilidad individual, retroalimentación y consultas, y monitoreo y cumplimiento, contribuirán a mejorar el conocimiento y la adherencia de los empleados a las prácticas seguras, políticas y procedimientos de seguridad de la información.

c) Proceso: Promoción de una cultura de seguridad en la organización.

- Activo de información: La conciencia y el compromiso de los empleados con la seguridad de la información.
- Riesgo: Riesgo de comportamientos inseguros, falta de conciencia o actitudes negligentes que puedan comprometer la seguridad de la información.
- Controles:
  - Programa de concienciación: Implementar un programa integral de concienciación en seguridad de la información que incluya sesiones de capacitación, materiales educativos y actividades interactivas para educar a los empleados sobre las mejores prácticas de seguridad.
  - Comunicación regular: Mantener una comunicación constante y clara sobre la importancia de la seguridad de la información, los riesgos asociados y las responsabilidades individuales de los empleados.
  - Liderazgo comprometido: Fomentar un liderazgo comprometido con la seguridad de la información, en el cual los líderes de la organización demuestren su apoyo y adhesión a las políticas y prácticas de seguridad.
  - Participación activa de los empleados: Incentivar a los empleados a participar activamente en la promoción de la seguridad de la información, alentarlos a reportar incidentes o posibles vulnerabilidades, y reconocer y recompensar su contribución.
  - Integración en procesos y procedimientos: Integrar la seguridad de la información en los procesos y procedimientos de la organización, de manera que se convierta en parte intrínseca de las actividades diarias de los empleados.
  - Evaluación y retroalimentación: Realizar evaluaciones periódicas para medir el nivel de cultura de seguridad en la organización y brindar

retroalimentación a los empleados sobre su desempeño en materia de seguridad.
- Mejora continua: Establecer mecanismos de mejora continua en la cultura de seguridad, mediante el análisis de brechas, la identificación de áreas de mejora y la implementación de acciones correctivas.
- Ejemplo y reconocimiento: Establecer ejemplos positivos y reconocer a aquellos empleados que demuestren un compromiso destacado con la seguridad de la información.

Promover una cultura de seguridad en la organización es fundamental para asegurar que todos los empleados comprendan la importancia de proteger la información y adopten comportamientos seguros en su trabajo diario. Los controles mencionados, como el programa de concienciación, la comunicación regular, el liderazgo comprometido, la participación activa de los empleados, la integración en procesos y procedimientos, la evaluación y retroalimentación, la mejora continua, y el ejemplo y reconocimiento, contribuirán a promover una cultura de seguridad sólida en la organización.

7. Macroproceso – Gestión de Incidentes de Seguridad

a) Proceso: Proceso de notificación, registro y manejo de incidentes de seguridad.

- Activo de información: Los incidentes de seguridad que afectan a los sistemas, datos y recursos de la organización.
- Riesgo: Riesgo de sufrir incidentes de seguridad que comprometan la confidencialidad, integridad y disponibilidad de la información.
- Controles:
  - Procedimientos de notificación: Establecer procedimientos claros y accesibles para que los empleados notifiquen cualquier incidente de seguridad que identifiquen.
  - Registro de incidentes: Mantener un registro centralizado de todos los incidentes de seguridad reportados, incluyendo detalles como la fecha, hora, descripción, impacto y acciones tomadas.
  - Evaluación de incidentes: Realizar una evaluación inicial de cada incidente notificado para determinar su gravedad, alcance y posibles consecuencias.
  - Clasificación de incidentes: Clasificar los incidentes de seguridad en función de su impacto potencial y la criticidad de los activos de información afectados.
  - Manejo y respuesta: Establecer un proceso de manejo y respuesta de incidentes que incluya la asignación de responsabilidades, la implementación de acciones correctivas, la mitigación de los impactos y la restauración de la normalidad.
  - Investigación de incidentes: Realizar investigaciones exhaustivas para determinar la causa raíz de los incidentes, identificar posibles vulnerabilidades y tomar medidas preventivas para evitar recurrencias.

- Comunicación y notificación: Establecer mecanismos de comunicación efectivos para informar a las partes interesadas sobre los incidentes de seguridad, tanto interna como externamente según corresponda.
- Mejora continua: Utilizar los incidentes de seguridad como oportunidades de aprendizaje para mejorar los controles y fortalecer la postura de seguridad de la organización.

El proceso de notificación, registro y manejo de incidentes de seguridad es fundamental para garantizar una respuesta oportuna y efectiva ante eventos de seguridad. Los controles mencionados, como los procedimientos de notificación, el registro de incidentes, la evaluación, clasificación y manejo de incidentes, la investigación, la comunicación y la mejora continua, contribuirán a una gestión eficiente de los incidentes de seguridad y a minimizar su impacto en la organización.

b) Proceso: Investigación y análisis de incidentes.

- Activo de información: Los incidentes de seguridad reportados que requieren investigación y análisis detallados.
- Riesgo: Riesgo de no identificar la causa raíz de los incidentes, lo que podría llevar a la repetición de eventos similares y a la persistencia de vulnerabilidades en el sistema.
- Controles:
  - Recopilación de datos: Recopilar y preservar la evidencia relacionada con el incidente, incluyendo registros de actividad, registros de seguridad, archivos de registro y otros datos relevantes.
  - Análisis forense: Realizar análisis forenses para determinar cómo se produjo el incidente, identificar las técnicas y herramientas utilizadas, y recopilar pruebas digitales para su uso en acciones legales o medidas disciplinarias.
  - Identificación de la causa raíz: Investigar a fondo el incidente para identificar la causa raíz, que puede ser una vulnerabilidad en los sistemas, una brecha en los controles de seguridad, una mala configuración o un error humano.
  - Evaluación del impacto: Evaluar el impacto del incidente en términos de la confidencialidad, integridad y disponibilidad de la información, así como en la reputación y operatividad de la organización.
  - Informe de incidentes: Preparar un informe detallado que documente los hallazgos de la investigación, incluyendo la descripción del incidente, la causa raíz identificada, las lecciones aprendidas y las recomendaciones para prevenir incidentes similares en el futuro.
  - Mejora continua: Utilizar los resultados de la investigación de incidentes para mejorar los controles de seguridad, fortalecer las políticas y procedimientos, y proporcionar capacitación adicional a los empleados en áreas de riesgo identificadas.

La investigación y análisis de incidentes desempeña un papel crucial en la respuesta efectiva a los incidentes de seguridad, permitiendo una comprensión más profunda de los eventos ocurridos y la implementación de medidas correctivas adecuadas. Los controles mencionados, como la recopilación de datos, el análisis forense, la identificación de la causa raíz, la evaluación del impacto, el informe de

incidentes y la mejora continua, ayudarán a fortalecer la postura de seguridad de la organización y a prevenir futuros incidentes.

c) Proceso: Restablecimiento de la seguridad y mitigación de los daños.

- Activo de información: Los sistemas y datos afectados por incidentes de seguridad que requieren restablecimiento y mitigación de los daños.
- Riesgo: Riesgo de interrupción prolongada de los servicios, pérdida o corrupción de datos, y daño a la reputación de la organización si no se restablece rápidamente la seguridad y no se mitigan los daños.
- Controles:
    - Contención y aislamiento: Identificar y aislar el alcance del incidente para evitar su propagación y limitar el daño adicional.
    - Restablecimiento de sistemas y datos: Restaurar los sistemas afectados a un estado seguro y funcional, utilizando copias de seguridad actualizadas y verificadas.
    - Parches y actualizaciones: Aplicar parches de seguridad y actualizaciones en los sistemas afectados para cerrar las vulnerabilidades explotadas y prevenir futuros incidentes similares.
    - Recuperación de datos: Recuperar y restaurar los datos afectados por el incidente, utilizando técnicas de recuperación de datos y copias de seguridad.
    - Mitigación de daños: Implementar medidas para mitigar los daños causados por el incidente, como la notificación a los usuarios afectados, la implementación de controles adicionales de seguridad y la revisión de las políticas y procedimientos existentes.
    - Pruebas de seguridad: Realizar pruebas de seguridad exhaustivas para asegurarse de que los sistemas restablecidos estén protegidos contra posibles brechas o vulnerabilidades.
    - Seguimiento y revisión: Realizar un seguimiento continuo y revisar las acciones tomadas para restablecer la seguridad y mitigar los daños, con el fin de evaluar su efectividad y realizar mejoras si es necesario.

El restablecimiento de la seguridad y la mitigación de los daños son procesos críticos para minimizar el impacto de los incidentes de seguridad y garantizar una rápida recuperación. Los controles mencionados, como la contención y aislamiento, el restablecimiento de sistemas y datos, la aplicación de parches y actualizaciones, la recuperación de datos, la mitigación de daños, las pruebas de seguridad y el seguimiento y revisión, son fundamentales para restaurar la seguridad de los activos de información afectados y reducir los efectos negativos en la organización.

X. MATRIZ DE RIESGOS – IMPACTO Y FRECUENCIA

La frecuencia y el impacto contenidos en una matriz de riesgo pueden variar dependiendo del tamaño de la organización, el tipo de activos de información involucrados y el nivel de riesgo al que esté expuesto el municipio. Es fundamental contar con personal capacitado

y experto en la investigación y análisis de incidentes, así como disponer de herramientas y recursos adecuados para llevar a cabo este proceso de manera efectiva.

1. Gestión de acceso y autenticación:

a) Creación de credenciales de acceso a sistemas computacionales internos.

- Frecuencia de referencia:
  - Frecuencia: Media (por ejemplo, mensualmente). Este valor puede variar según las necesidades y características específicas de tu organización.
- Impacto en valor cualitativo de referencia:
  - Impacto: Medio. Esto implica que un proceso inadecuado o incorrecto puede generar riesgos significativos, pero con un alcance limitado. Puede permitir accesos no autorizados a información menos sensible o tener un impacto moderado en la disponibilidad o integridad de los sistemas.

b) Administración de cuentas de usuario y privilegios.

- Frecuencia de referencia:
  - Frecuencia: Alta (por ejemplo, diariamente o semanalmente). La administración de cuentas de usuario y privilegios es un proceso continuo que implica la creación, modificación y eliminación de cuentas, así como la asignación y revocación de privilegios. Es necesario llevar a cabo estas actividades de forma regular para mantener un control adecuado sobre los accesos y privilegios de los usuarios.
- Impacto en valor cualitativo de referencia:
  - Impacto: Alto. La administración inadecuada de cuentas de usuario y privilegios puede tener un impacto significativo en la seguridad de la información. La falta de control sobre las cuentas y privilegios puede permitir accesos no autorizados, facilitar el abuso de privilegios o exponer la organización a riesgos de compromiso de la integridad, disponibilidad y confidencialidad de los datos.

c) Implementación de políticas de contraseñas seguras.

- Frecuencia de referencia:
  - Frecuencia: Alta (por ejemplo, mensualmente o trimestralmente). La implementación y actualización de políticas de contraseñas seguras es un proceso continuo que requiere mantenerse al día con las mejores prácticas de seguridad. Se deben revisar regularmente las políticas existentes, realizar cambios si es necesario y comunicar y capacitar a los usuarios sobre los requisitos de las contraseñas seguras.
- Impacto en valor cualitativo de referencia:
  - Impacto: Medio. La implementación de políticas de contraseñas seguras tiene un impacto significativo en la seguridad de la información. Al establecer

requisitos fuertes para las contraseñas, se reduce el riesgo de acceso no autorizado a los sistemas y datos. Sin embargo, el impacto puede considerarse medio en comparación con otros procesos, ya que una implementación inadecuada o falta de cumplimiento de las políticas puede debilitar la seguridad y aumentar el riesgo de violaciones de seguridad.

d) Uso de autenticación de dos factores.

- Frecuencia de referencia:
  - Frecuencia: Alta (por ejemplo, en cada inicio de sesión). El uso de autenticación de dos factores es un proceso que debe aplicarse en cada inicio de sesión para garantizar una capa adicional de seguridad. Los usuarios deben autenticarse proporcionando dos tipos de información, como una contraseña y un código generado en tiempo real, un token de seguridad, una huella dactilar, entre otros.
- Impacto en valor cualitativo de referencia:
  - Impacto: Alto. El uso de autenticación de dos factores tiene un impacto significativo en la seguridad de la información. Al agregar una segunda capa de autenticación, se reduce el riesgo de acceso no autorizado a los sistemas y datos. Esto dificulta que los atacantes puedan comprometer las cuentas de usuario incluso si obtienen acceso a las contraseñas.

e) Control de acceso físico a las instalaciones.

- Frecuencia de referencia:
  - Frecuencia: Media. El control de acceso físico a las instalaciones generalmente se lleva a cabo de manera regular, como parte de las políticas de seguridad de la organización. Por ejemplo, puede incluir el uso de tarjetas de identificación o llaves para acceder a las áreas restringidas, registros de ingreso y salida, monitoreo de cámaras de seguridad, entre otros.
- Impacto en valor cualitativo de referencia:
  - Impacto: Alto. El control de acceso físico a las instalaciones tiene un impacto significativo en la seguridad de la información y los activos de la organización. Garantizar que solo las personas autorizadas tengan acceso a las áreas restringidas reduce el riesgo de intrusiones, robo de información y daños a los activos físicos.

2. Protección de datos:

a) Clasificación y etiquetado de datos según su confidencialidad.

- Frecuencia de referencia:
  - Frecuencia: Alta. La clasificación y etiquetado de datos según su confidencialidad es un proceso continuo que debe llevarse a cabo de manera regular, especialmente cuando se generan, modifican o comparten nuevos

datos. Por ejemplo, cada vez que se crea un nuevo documento, se debe asignar una clasificación de confidencialidad y etiquetarlo adecuadamente.

- Impacto en valor cualitativo de referencia:
    - Impacto: Medio. La clasificación y etiquetado de datos tiene un impacto significativo en la seguridad de la información y la protección de la confidencialidad de los datos. Al asignar una clasificación adecuada y etiquetar los datos de manera correspondiente, se facilita su manejo y se garantiza que se apliquen las medidas de seguridad adecuadas para protegerlos.

b) Implementación de controles de acceso a los datos.

- Frecuencia de referencia:
    - Frecuencia: Alta. La implementación de controles de acceso a los datos es un proceso continuo que debe llevarse a cabo de manera regular para garantizar la protección adecuada de la información. Esto implica configurar y mantener los controles de acceso, como permisos de usuario, roles y políticas de acceso, y revisarlos periódicamente para adaptarlos a las necesidades cambiantes de la organización.
- Impacto en valor cualitativo de referencia:
    - Impacto: Alto. La implementación de controles de acceso a los datos tiene un impacto crítico en la seguridad de la información y la protección de la confidencialidad, integridad y disponibilidad de los datos. Un control deficiente o inadecuado puede dar lugar a accesos no autorizados, filtraciones de información o modificaciones no autorizadas, lo que podría causar daños significativos a la organización, como pérdida de datos, daño a la reputación y sanciones legales.

c) Encriptación de datos sensibles en reposo y en tránsito.

- Frecuencia de referencia:
    - Frecuencia: Alta. La encriptación de datos sensibles en reposo y en tránsito debe ser aplicada de manera continua y consistente en todos los sistemas y comunicaciones que manejan información crítica. Es una medida esencial para proteger los datos y prevenir la exposición no autorizada tanto en almacenamiento como durante su transmisión.
- Impacto en valor cualitativo de referencia:
    - Impacto: Alto. La encriptación de datos sensibles proporciona un nivel de protección adicional y reduce el riesgo de acceso no autorizado, divulgación o modificación indebida de la información. Su falta o implementación inadecuada puede dar lugar a brechas de seguridad, robo de datos sensibles, violación de la privacidad y daños a la reputación de la organización. Por lo tanto, la encriptación de datos es crucial para salvaguardar la confidencialidad e integridad de la información.

d) Copias de seguridad y recuperación de datos.

- Frecuencia de referencia:
    - Frecuencia: Regular. Las copias de seguridad y la recuperación de datos deben realizarse de manera programada y periódica para garantizar la disponibilidad y la integridad de la información. La frecuencia puede variar según los requerimientos y la criticidad de los datos, pero generalmente se realiza de forma diaria, semanal o mensual, dependiendo de las necesidades y el volumen de los datos generados y modificados.
- Impacto en valor cualitativo de referencia:
    - Impacto: Alto. Las copias de seguridad y la recuperación de datos son fundamentales para garantizar la continuidad del negocio y la recuperación de información en caso de incidentes o desastres. En caso de pérdida, corrupción o eliminación accidental de datos, la ausencia de copias de seguridad adecuadas puede resultar en la pérdida irreversible de información valiosa y crítica para la organización. La falta de un proceso sólido de copias de seguridad y recuperación puede tener un impacto significativo en la operatividad, la reputación y la confianza de la organización.

e) Retención y eliminación segura de datos obsoletos.

- Frecuencia de referencia:
    - Frecuencia: Regular. La retención y eliminación segura de datos obsoletos debe realizarse de manera planificada y periódica para mantener un entorno de información limpio y seguro. La frecuencia puede variar según las políticas y regulaciones aplicables, pero generalmente se lleva a cabo de forma periódica, como trimestral o anualmente, dependiendo del volumen de datos generados y la tasa de obsolescencia de la información.
- Impacto en valor cualitativo de referencia:
    - Impacto: Moderado. La retención y eliminación segura de datos obsoletos es crucial para reducir el riesgo de divulgación no autorizada, el incumplimiento normativo y la acumulación innecesaria de información confidencial. El impacto de no llevar a cabo este proceso de manera adecuada puede resultar en la exposición de datos sensibles, la violación de la privacidad de los individuos y posibles sanciones legales o daños a la reputación de la organización. Además, la retención excesiva de datos obsoletos puede dificultar la gestión eficiente de la información y aumentar los costos asociados al almacenamiento y protección de datos.

3. Gestión de parches y actualizaciones:

a) Implementación de un proceso de gestión de parches y actualizaciones para sistemas y aplicaciones.

- Frecuencia de referencia:

- Frecuencia: Alta. La implementación de un proceso de gestión de parches y actualizaciones implica la aplicación regular y oportuna de las actualizaciones de seguridad y correcciones de software. La frecuencia puede variar según la disponibilidad de parches y actualizaciones por parte de los fabricantes y la criticidad de los sistemas y aplicaciones en la organización. En general, se recomienda realizar evaluaciones y aplicar los parches de seguridad tan pronto como estén disponibles, siguiendo una programación regular para garantizar la protección continua de los activos de información.

- Impacto en valor cualitativo de referencia:

  - Impacto: Alto. La implementación efectiva de un proceso de gestión de parches y actualizaciones es crucial para mitigar vulnerabilidades conocidas y proteger los sistemas y aplicaciones contra amenazas cibernéticas. El impacto de no realizar estas actualizaciones de manera adecuada puede resultar en la explotación de vulnerabilidades, ataques exitosos de malware, pérdida de datos, interrupciones en la disponibilidad de los servicios y posibles daños a la reputación de la organización. Por lo tanto, es fundamental establecer y seguir un proceso robusto de gestión de parches y actualizaciones para garantizar la seguridad y estabilidad de los sistemas y aplicaciones.

b) Evaluación de vulnerabilidades y aplicación de parches de seguridad.

- Frecuencia de referencia:

  - Frecuencia: Media a Alta. La evaluación de vulnerabilidades y la aplicación de parches de seguridad deben llevarse a cabo de manera regular para identificar y corregir posibles vulnerabilidades en los sistemas y aplicaciones. La frecuencia puede depender de diversos factores, como el entorno tecnológico, el nivel de criticidad de los sistemas y aplicaciones, y la disponibilidad de actualizaciones y parches por parte de los fabricantes. Se recomienda realizar evaluaciones de vulnerabilidades de forma periódica y aplicar los parches tan pronto como estén disponibles, priorizando aquellos que solucionen vulnerabilidades críticas o de alto impacto.

- Impacto en valor cualitativo de referencia:

  - Impacto: Alto. La evaluación de vulnerabilidades y la aplicación de parches de seguridad son fundamentales para prevenir y mitigar riesgos en la seguridad de la información. No realizar estas actividades de manera adecuada puede exponer los sistemas y aplicaciones a ataques y explotaciones de vulnerabilidades conocidas, lo que puede resultar en la pérdida de datos, interrupciones en los servicios, daños a la reputación y posibles consecuencias legales. Por lo tanto, es esencial realizar evaluaciones de vulnerabilidades de forma regular y aplicar los parches de seguridad de manera oportuna para garantizar la protección y la integridad de los sistemas y aplicaciones.

c) Mantenimiento y actualización de los sistemas operativos y software de seguridad.

- Frecuencia de referencia:

- Frecuencia: Alta. El mantenimiento y la actualización de los sistemas operativos y software de seguridad deben realizarse de manera regular y oportuna. Los fabricantes lanzan actualizaciones y parches de seguridad para abordar vulnerabilidades y mejorar el rendimiento de sus productos. Se recomienda seguir las recomendaciones y las mejores prácticas del fabricante, que pueden incluir actualizaciones periódicas programadas, y aplicar los parches y actualizaciones tan pronto como estén disponibles.

- Impacto en valor cualitativo de referencia:

  - Impacto: Medio a Alto. El mantenimiento y la actualización de los sistemas operativos y software de seguridad son esenciales para mantener la estabilidad y la seguridad de los sistemas y aplicaciones. No realizar estas actividades de manera adecuada puede exponer los sistemas a vulnerabilidades conocidas, fallos de seguridad y problemas de rendimiento. Esto puede resultar en la pérdida de datos, interrupciones en los servicios, daños a la reputación y posibles consecuencias legales. Por lo tanto, es fundamental realizar el mantenimiento y las actualizaciones de forma regular y oportuna para garantizar la protección y el correcto funcionamiento de los sistemas y aplicaciones.

4. Monitorización y detección de intrusiones:

a) Implementación de sistemas de detección y prevención de intrusiones.

- Frecuencia de referencia:

  - Frecuencia: Continua. Los sistemas de detección y prevención de intrusiones deben funcionar de manera constante para monitorear y proteger los sistemas y redes de posibles ataques. Se recomienda contar con mecanismos de detección en tiempo real y análisis de eventos de seguridad de forma continua, así como actualizaciones regulares de las firmas de detección y las reglas de prevención.

- Impacto en valor cualitativo de referencia:

  - Impacto: Medio a Alto. La implementación de sistemas de detección y prevención de intrusiones es fundamental para identificar y bloquear actividades sospechosas o maliciosas en los sistemas y redes. Estos sistemas pueden detectar intentos de intrusión, ataques de malware, comportamientos anómalos y violaciones de políticas de seguridad. Si no se implementan adecuadamente o no se les presta la debida atención, se corre el riesgo de no detectar y mitigar los ataques de manera oportuna, lo que puede resultar en la pérdida de datos confidenciales, la interrupción de servicios críticos, la violación de la privacidad de los usuarios y daños a la reputación de la organización.

b) Monitorización de eventos y registros de seguridad.

- Frecuencia de referencia:

- Frecuencia: Continua. La monitorización de eventos y registros de seguridad debe realizarse de manera constante para identificar posibles incidentes de seguridad, comportamientos anómalos y actividades sospechosas en los sistemas y redes. Se recomienda implementar soluciones de monitorización en tiempo real, configurar alertas y realizar análisis periódicos de los registros de seguridad.

- Impacto en valor cualitativo de referencia:

  - Impacto: Medio a Alto. La monitorización de eventos y registros de seguridad es esencial para detectar y responder de manera oportuna a posibles amenazas y ataques a los sistemas y redes. Al identificar y analizar los eventos de seguridad, se puede prevenir la pérdida de datos confidenciales, la interrupción de servicios, la violación de políticas de seguridad y otros impactos negativos para la organización. Además, la monitorización adecuada puede ayudar en la recolección de evidencia forense en caso de incidentes y facilitar la respuesta y recuperación posterior.

c) Análisis de incidentes de seguridad y respuesta ante intrusiones.

- Frecuencia de referencia:

  - Frecuencia: Variable. La frecuencia de los incidentes de seguridad puede variar según la organización, su exposición al riesgo y el nivel de sofisticación de los posibles atacantes. Se recomienda establecer un equipo o función dedicada para el análisis de incidentes de seguridad y la respuesta ante intrusiones, que esté preparado para actuar de manera proactiva y reactiva ante los incidentes que ocurran.

- Impacto en valor cualitativo de referencia:

  - Impacto: Medio a Alto. Los incidentes de seguridad y las intrusiones pueden tener un impacto significativo en la confidencialidad, integridad y disponibilidad de los sistemas y datos de la organización. El análisis de incidentes de seguridad y la respuesta adecuada son fundamentales para minimizar los daños, investigar la causa raíz, contener el incidente, restaurar los sistemas afectados y prevenir futuros incidentes. Además, una respuesta efectiva puede ayudar a proteger la reputación de la organización y mantener la confianza de los clientes y socios.

d) Evaluación de la actividad de la red y sistemas en busca de comportamientos anómalos.

- Frecuencia de referencia:

  - Frecuencia: Regular. La evaluación de la actividad de la red y sistemas en busca de comportamientos anómalos debe realizarse de manera periódica para detectar posibles actividades maliciosas o inusuales. La frecuencia específica dependerá de factores como el tamaño de la organización, el nivel de exposición al riesgo y la criticidad de los sistemas y redes involucrados.

- Impacto en valor cualitativo de referencia:
    - Impacto: Medio a Alto. La detección temprana de comportamientos anómalos en la red y sistemas puede ayudar a prevenir ataques cibernéticos, intrusiones no autorizadas y fugas de información. Un impacto negativo puede incluir la interrupción de servicios, el robo de datos confidenciales, la pérdida de reputación y el incumplimiento de regulaciones. La evaluación y detección adecuadas permiten una respuesta oportuna y mitigación de riesgos.

5. Gestión de proveedores y terceros:

a) Evaluación de la seguridad de los proveedores y terceros.

- Frecuencia de referencia:
    - Frecuencia: Periódica. La evaluación de la seguridad de los proveedores y terceros debe realizarse de manera regular para garantizar que cumplen con los requisitos de seguridad establecidos. La frecuencia específica dependerá de factores como la naturaleza de la relación con los proveedores y terceros, la criticidad de los servicios que brindan y el nivel de riesgo asociado.
- Impacto en valor cualitativo de referencia:
    - Impacto: Medio a Alto. La seguridad de los proveedores y terceros puede tener un impacto significativo en la seguridad de la información de tu organización. Un proveedor o tercero con deficiencias de seguridad podría exponer a tu organización a riesgos como brechas de datos, fugas de información confidencial o interrupción de servicios. La evaluación adecuada y la implementación de controles de seguridad sólidos pueden ayudar a mitigar estos riesgos y garantizar la protección de los activos de información.

b) Establecimiento de acuerdos de seguridad y cláusulas de confidencialidad.

- Frecuencia de referencia:
    - Frecuencia: Inicial y periódica. El establecimiento de acuerdos de seguridad y cláusulas de confidencialidad se realiza al inicio de la relación con proveedores y terceros, y posteriormente se deben revisar y actualizar de forma periódica para adaptarse a los cambios en los riesgos y requisitos de seguridad. La frecuencia específica dependerá de la naturaleza de la relación con los proveedores y terceros, la criticidad de los servicios que brindan y el nivel de riesgo asociado.
- Impacto en valor cualitativo de referencia:
    - Impacto: Medio a Alto. Los acuerdos de seguridad y cláusulas de confidencialidad son fundamentales para establecer las expectativas y obligaciones relacionadas con la protección de la información confidencial y los activos de tu organización. Un incumplimiento en estos acuerdos podría resultar en la divulgación no autorizada de información, pérdida de

confidencialidad o daños reputacionales. Es esencial asegurarse de que los acuerdos sean sólidos y adecuados para mitigar estos riesgos y proteger la información sensible.

c) Supervisión y auditoría de los proveedores y terceros.

- Frecuencia de referencia:
    - Frecuencia: Periódica. La supervisión y auditoría de los proveedores y terceros debe realizarse de manera regular para garantizar el cumplimiento de los acuerdos de seguridad, políticas y requisitos establecidos. La frecuencia específica dependerá de la criticidad de la relación con los proveedores y terceros, la sensibilidad de la información compartida y los riesgos asociados.
- Impacto en valor cualitativo de referencia:
    - Impacto: Medio a Alto. La supervisión y auditoría de los proveedores y terceros es esencial para asegurarse de que cumplan con los estándares de seguridad acordados y protejan adecuadamente la información confidencial de tu organización. Un incumplimiento por parte de los proveedores o terceros podría resultar en la exposición de información sensible, violaciones de seguridad o interrupción de los servicios. Por lo tanto, es fundamental realizar una supervisión efectiva y auditorías periódicas para mitigar estos riesgos y garantizar el cumplimiento.

6. Concientización y formación en seguridad:

a) Programas de concientización y formación en seguridad de la información para los empleados.

- Frecuencia de referencia:
    - Frecuencia: Regular. Los programas de concientización y formación en seguridad de la información deben llevarse a cabo de forma continua para asegurar que los empleados estén actualizados sobre las mejores prácticas de seguridad, las políticas y los procedimientos relevantes. La frecuencia específica dependerá de la naturaleza de tu organización, el tamaño, el nivel de riesgo y los cambios en las amenazas y tecnologías.
- Impacto en valor cualitativo de referencia:
    - Impacto: Medio. Los programas de concientización y formación en seguridad de la información tienen un impacto significativo en la mitigación de riesgos y la protección de los activos de información. Al capacitar y educar a los empleados sobre las amenazas, las prácticas seguras y los protocolos de respuesta, se fortalece la cultura de seguridad y se reduce la posibilidad de incidentes causados por errores humanos o falta de conocimiento. Además, un personal bien informado y consciente de la seguridad es capaz de detectar y reportar posibles incidentes de manera oportuna.

b) Educación sobre prácticas seguras, políticas y procedimientos.

- Frecuencia de referencia:
    - Frecuencia: Regular. La educación sobre prácticas seguras, políticas y procedimientos debe llevarse a cabo de forma periódica para garantizar que los empleados estén al tanto de las últimas prácticas de seguridad, las políticas y los procedimientos establecidos. La frecuencia específica dependerá de la naturaleza de tu organización, el tamaño, el nivel de riesgo y los cambios en las amenazas y tecnologías.
- Impacto en valor cualitativo de referencia:
    - Impacto: Alto. La educación sobre prácticas seguras, políticas y procedimientos tiene un impacto significativo en la mitigación de riesgos y la protección de los activos de información. Al proporcionar a los empleados el conocimiento necesario sobre las prácticas adecuadas de seguridad de la información, las políticas y los procedimientos, se fortalece la cultura de seguridad y se reduce la posibilidad de incidentes causados por errores o desconocimiento. Además, los empleados estarán mejor preparados para tomar decisiones informadas y seguir los protocolos establecidos, lo que contribuye a la protección general de la organización contra amenazas de seguridad.

c) Promoción de una cultura de seguridad en la organización.

- Frecuencia de referencia:
    - Frecuencia: Continua. La promoción de una cultura de seguridad en la organización debe ser un esfuerzo constante y permanente. No se trata de un evento único, sino de un proceso continuo de concientización, comunicación y promoción de las mejores prácticas de seguridad en todos los niveles de la organización.
- Impacto en valor cualitativo de referencia:
    - Impacto: Muy alto. La promoción de una cultura de seguridad en la organización tiene un impacto fundamental en la protección de la información y la mitigación de riesgos. Al crear una cultura en la que la seguridad de la información sea valorada y prioritaria, se fomenta la adopción de comportamientos seguros por parte de todos los empleados. Esto implica la integración de la seguridad en la mentalidad y las prácticas diarias de trabajo, lo que reduce la probabilidad de incidentes de seguridad causados por descuidos, errores o malas prácticas. Además, una cultura de seguridad sólida también promueve la responsabilidad compartida, la colaboración y la comunicación efectiva en relación con la seguridad de la información en toda la organización.

7. Gestión de incidentes de seguridad:

a) Proceso de notificación, registro y manejo de incidentes de seguridad.

- Frecuencia de referencia:

- Frecuencia: Eventual. La frecuencia de los incidentes de seguridad puede variar según la organización y su exposición a amenazas. Sin embargo, es importante tener en cuenta que los incidentes de seguridad pueden ocurrir en cualquier momento. Por lo tanto, se debe establecer un proceso sólido y bien definido para notificar, registrar y manejar los incidentes de seguridad de manera oportuna y eficiente.

- Impacto en valor cualitativo de referencia:

  - Impacto: Variable. El impacto de los incidentes de seguridad puede variar desde bajo hasta muy alto, dependiendo de la naturaleza del incidente, los activos de información afectados y las consecuencias resultantes. Algunos incidentes pueden tener un impacto mínimo, mientras que otros pueden causar interrupciones significativas en las operaciones de la organización, pérdida de datos, daño a la reputación o incumplimiento de regulaciones.

b) Investigación y análisis de incidentes.

- Frecuencia de referencia:

  - Frecuencia: Ocasional. La frecuencia de la investigación y análisis de incidentes puede variar dependiendo de la cantidad y gravedad de los incidentes que ocurran en la organización. Es necesario contar con un proceso establecido para investigar y analizar cada incidente de seguridad de manera exhaustiva, con el objetivo de identificar su causa raíz, evaluar su alcance y determinar las acciones correctivas necesarias.

- Impacto en valor cualitativo de referencia:

  - Impacto: Moderado. El impacto de la investigación y análisis de incidentes puede considerarse moderado, ya que implica la asignación de recursos, tiempo y esfuerzo para llevar a cabo una evaluación completa de los incidentes de seguridad. Esto implica la recolección de evidencias, el análisis forense, la identificación de vulnerabilidades o debilidades en los controles de seguridad, y la implementación de medidas correctivas o preventivas para evitar incidentes similares en el futuro.

c) Restablecimiento de la seguridad y mitigación de los daños.

- Frecuencia de referencia:

  - Frecuencia: Eventual. La frecuencia del proceso de restablecimiento de la seguridad y mitigación de los daños puede variar dependiendo de la ocurrencia de incidentes de seguridad en la organización. Este proceso se activa cuando se detecta un incidente y tiene como objetivo restablecer la seguridad de los sistemas y mitigar los daños causados por el incidente.

- Impacto en valor cualitativo de referencia:

  - Impacto: Significativo. El impacto del proceso de restablecimiento de la seguridad y mitigación de los daños se considera significativo, ya que implica

tomar medidas rápidas y efectivas para contener el incidente, minimizar el impacto en los activos de información y restablecer la seguridad de los sistemas afectados. Esto implica la asignación de recursos, tiempo y esfuerzo para llevar a cabo acciones de respuesta, como la eliminación de malware, la restauración de sistemas desde copias de seguridad, la aplicación de parches de seguridad, entre otros.

XI. MATRIZ DE RIESGOS – REPORTERÍA

Tabla 6. Preparación Mapa de Calor.

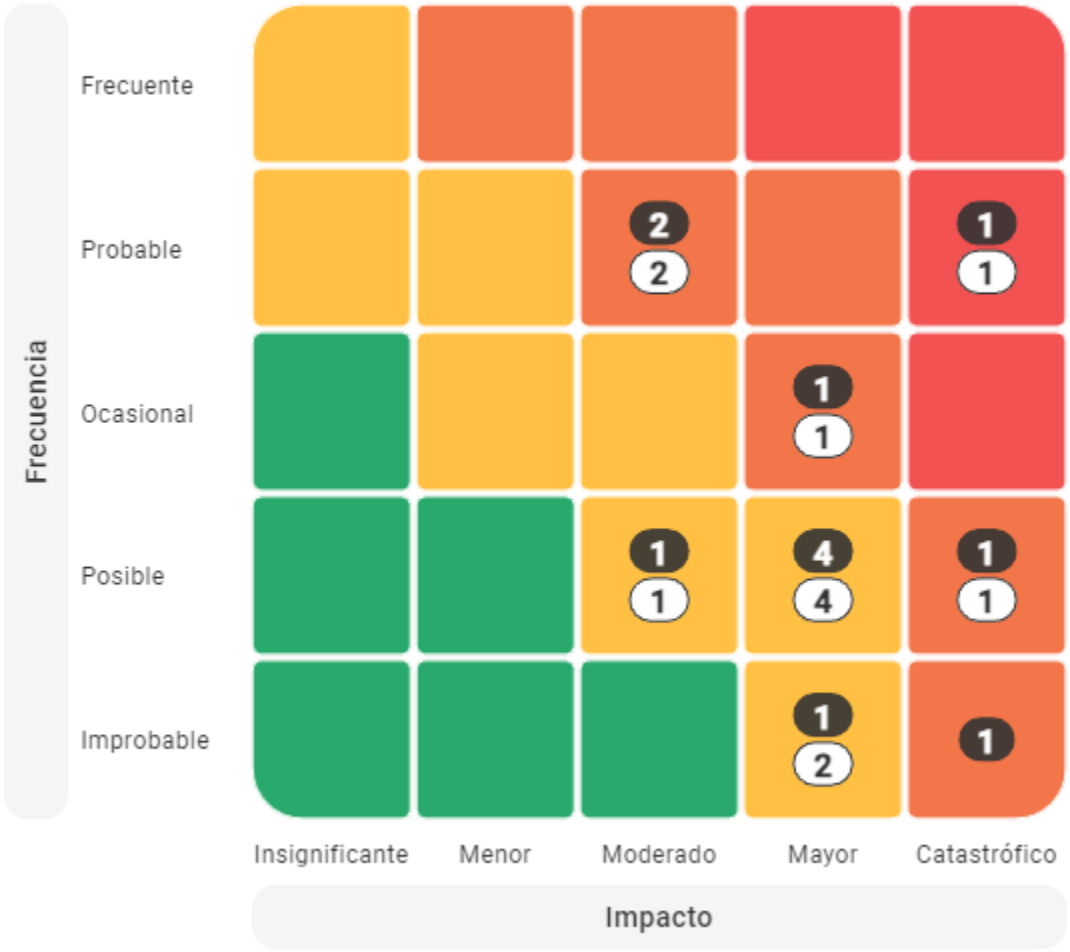
Nombre Riesgo	Descripción Riesgo	Frecuencia Inherente	Impacto Inherente	Severidad Inherente	Frecuencia Residual	Impacto Residual	Severidad Residual
01.Riesgo de acceso no autorizado	Posibilidad de que personas no autorizadas obtengan acceso a sistemas, aplicaciones o datos confidenciales.	Improbable	Catastrófico	Alto	Improbable	Mayor	Medio
02.Riesgo de pérdida de datos	Posibilidad de que se pierdan datos debido a fallas en el sistema, errores humanos, desastres naturales o ataques cibernéticos.	Posible	Mayor	Medio	Posible	Mayor	Medio
03.Riesgo de fuga de información	Posibilidad de que la información confidencial sea revelada o filtrada, ya sea de forma intencional o no intencional, por parte de empleados, contratistas o terceros.	Ocasional	Mayor	Alto	Ocasional	Mayor	Alto
04.Riesgo de robo de información	Posibilidad de que la información valiosa sea robada o comprometida por personas externas o internas malintencionadas.	Posible	Mayor	Medio	Posible	Mayor	Medio
05.Riesgo de interrupción del servicio	Posibilidad de que los sistemas o servicios críticos de la organización sean interrumpidos, ya sea debido a fallas técnicas, desastres naturales o	Probable	Moderado	Alto	Probable	Moderado	Alto

	ataques cibernéticos.						
06.Riesgo de violación de privacidad	Posibilidad de que la información personal de los clientes o empleados sea utilizada o divulgada de manera inapropiada, incumpliendo las regulaciones de privacidad.	Improbable	Mayor	Medio	Improbable	Mayor	Medio
07.Riesgo de fallas en la seguridad física	Posibilidad de que los activos físicos, como servidores, equipos o documentos, sean vulnerados o robados debido a una falta de seguridad física.	Probable	Catastrófico	Extremo	Probable	Catastrófico	Extremo
08.Riesgo de ataques cibernéticos	Posibilidad de que los sistemas de la organización sean objeto de ataques de malware, phishing, ransomware u otros tipos de ataques cibernéticos.	Posible	Catastrófico	Alto	Posible	Catastrófico	Alto
09.Riesgo de falta de cumplimiento normativo	Posibilidad de incumplir las regulaciones y normativas relacionadas con la seguridad de la información, lo que puede resultar en sanciones legales y daño a la reputación	Posible	Mayor	Medio	Posible	Mayor	Medio
10.Riesgo de falta de concientización en seguridad	Posibilidad de que los empleados no estén suficientemente capacitados o no cumplan con las prácticas de seguridad establecidas, lo que puede aumentar la vulnerabilidad de la organización.	Probable	Moderado	Alto	Probable	Moderado	Alto
11.Riesgo disponibilidad de la información	Posibilidad de sufrir incidentes de seguridad que comprometan la confidencialidad, integridad y disponibilidad de la información.	Posible	Mayor	Medio	Posible	Mayor	Medio

12.Riesgo no identificación causa raíz del problema	Posibilidad de no identificar la causa raíz de los incidentes, lo que podría llevar a la repetición de eventos similares y a la persistencia de vulnerabilidades en el sistema.	Posible	Moderado	Medio	Posible	Moderado	Medio

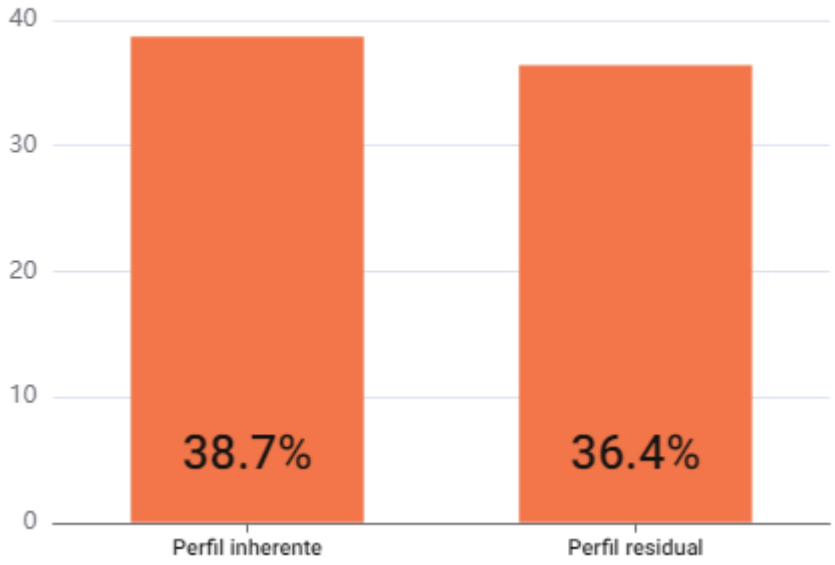
Fuente: Elaboración propia basado en Norma ISO 31000.

Figura 6. Mapa de Calor



Fuente: Elaboración propia basado en Norma ISO 27000/31000.

Figura 7. Perfil de Riesgo Organizacional



Fuente: Elaboración propia basado en Norma ISO 27000/31000.

Riesgo inherente

NIVEL DE RIESGO	RIESGOS	DISTRIBUCIÓN	PROMEDIO RI
Medio	6	50%	28%
Alto	5	41.7%	40.8%
Bajo	0	0%	0%
Extremo	1	8.3%	80%

Riesgo residual

NIVEL DE RIESGO	RIESGOS	DISTRIBUCIÓN	PROMEDIO RR
Medio	7	58.3%	24.6%
Alto	4	33.3%	46%
Bajo	0	0%	0%
Extremo	1	8.3%	80%

Fuente: Elaboración propia basado en Norma ISO 27000/31000.

Tabla 7. Preparación Perfil de Riesgo por Procesos.

Nombre Proceso	Nombre Riesgo	Frecuencia Inherente	Impacto Inherente	Severidad Inherente	Frecuencia Residual	Impacto Residual	Severidad Residual
1.GESTIÓN DE ACCESO Y AUTENTICACIÓN	2.Riesgo de pérdida de datos	Posible	Mayor	Medio	Posible	Mayor	Medio
1.GESTIÓN DE ACCESO Y AUTENTICACIÓN	5.Riesgo de interrupción del servicio	Probable	Moderado	Alto	Probable	Moderado	Alto
1.GESTIÓN DE ACCESO Y AUTENTICACIÓN	1.Riesgo de acceso no autorizado	Improbable	Catastrófico	Alto	Improbable	Mayor	Medio
1.GESTIÓN DE ACCESO Y AUTENTICACIÓN	3.Riesgo de fuga de información	Ocasional	Mayor	Alto	Ocasional	Mayor	Alto
1.GESTIÓN DE ACCESO Y AUTENTICACIÓN	7.Riesgo de fallas en la seguridad física	Probable	Catastrófico	Extremo	Probable	Catastrófico	Extremo
1.GESTIÓN DE ACCESO Y AUTENTICACIÓN	4.Riesgo de robo de información	Posible	Mayor	Medio	Posible	Mayor	Medio
1.GESTIÓN DE ACCESO Y AUTENTICACIÓN	6.Riesgo de violación de privacidad	Improbable	Mayor	Medio	Improbable	Mayor	Medio
2.PROTECCIÓN DE DATOS	2.Riesgo de pérdida de datos	Posible	Mayor	Medio	Posible	Mayor	Medio
2.PROTECCIÓN DE DATOS	6.Riesgo de violación de privacidad	Improbable	Mayor	Medio	Improbable	Mayor	Medio
2.PROTECCIÓN DE DATOS	9.Riesgo de falta de cumplimiento normativo	Posible	Mayor	Medio	Posible	Mayor	Medio
2.PROTECCIÓN DE DATOS	1.Riesgo de acceso no autorizado	Improbable	Catastrófico	Alto	Improbable	Mayor	Medio
2.PROTECCIÓN DE DATOS	3.Riesgo de fuga de información	Ocasional	Mayor	Alto	Ocasional	Mayor	Alto
2.PROTECCIÓN DE DATOS	8.Riesgo de ataques cibernéticos	Posible	Catastrófico	Alto	Posible	Catastrófico	Alto
2.PROTECCIÓN DE DATOS	4.Riesgo de robo de información	Posible	Mayor	Medio	Posible	Mayor	Medio
3.GESTIÓN DE PARCHES Y ACTUALIZACIONES	5.Riesgo de interrupción del servicio	Probable	Moderado	Alto	Probable	Moderado	Alto
3.GESTIÓN DE PARCHES Y ACTUALIZACIONES	9.Riesgo de falta de cumplimiento normativo	Posible	Mayor	Medio	Posible	Mayor	Medio
3.GESTIÓN DE PARCHES Y ACTUALIZACIONES	8.Riesgo de ataques cibernéticos	Posible	Catastrófico	Alto	Posible	Catastrófico	Alto
4.MONITORIZACIÓN Y DETECCIÓN DE INTRUSIONES	9.Riesgo de falta de cumplimiento normativo	Posible	Mayor	Medio	Posible	Mayor	Medio

4.MONITORIZACIÓN Y DETECCIÓN DE INTRUSIONES	5.Riesgo de interrupción del servicio	Probable	Moderado	Alto	Probable	Moderado	Alto
4.MONITORIZACIÓN Y DETECCIÓN DE INTRUSIONES	1.Riesgo de acceso no autorizado	Improbable	Catastrófico	Alto	Improbable	Mayor	Medio
4.MONITORIZACIÓN Y DETECCIÓN DE INTRUSIONES	7.Riesgo de fallas en la seguridad física	Probable	Catastrófico	Extremo	Probable	Catastrófico	Extremo
4.MONITORIZACIÓN Y DETECCIÓN DE INTRUSIONES	8.Riesgo de ataques cibernéticos	Posible	Catastrófico	Alto	Posible	Catastrófico	Alto
5.GESTIÓN DE PROVEEDORES Y TERCEROS	9.Riesgo de falta de cumplimiento normativo	Posible	Mayor	Medio	Posible	Mayor	Medio
5.GESTIÓN DE PROVEEDORES Y TERCEROS	5.Riesgo de interrupción del servicio	Probable	Moderado	Alto	Probable	Moderado	Alto
5.GESTIÓN DE PROVEEDORES Y TERCEROS	2.Riesgo de pérdida de datos	Posible	Mayor	Medio	Posible	Mayor	Medio
5.GESTIÓN DE PROVEEDORES Y TERCEROS	1.Riesgo de acceso no autorizado	Improbable	Catastrófico	Alto	Improbable	Mayor	Medio
5.GESTIÓN DE PROVEEDORES Y TERCEROS	10.Riesgo de falta de concientización en seguridad	Probable	Moderado	Alto	Probable	Moderado	Alto
5.GESTIÓN DE PROVEEDORES Y TERCEROS	8.Riesgo de ataques cibernéticos	Posible	Catastrófico	Alto	Posible	Catastrófico	Alto
5.GESTIÓN DE PROVEEDORES Y TERCEROS	3.Riesgo de fuga de información	Ocasional	Mayor	Alto	Ocasional	Mayor	Alto
5.GESTIÓN DE PROVEEDORES Y TERCEROS	6.Riesgo de violación de privacidad	Improbable	Mayor	Medio	Improbable	Mayor	Medio
6.CONCIENTIZACIÓN Y FORMACIÓN EN SEGURIDAD	9.Riesgo de falta de cumplimiento normativo	Posible	Mayor	Medio	Posible	Mayor	Medio
6.CONCIENTIZACIÓN Y FORMACIÓN EN SEGURIDAD	10.Riesgo de falta de concientización en seguridad	Probable	Moderado	Alto	Probable	Moderado	Alto
7.GESTIÓN DE INCIDENTES DE SEGURIDAD	8.Riesgo de ataques cibernéticos	Posible	Catastrófico	Alto	Posible	Catastrófico	Alto
7.GESTIÓN DE INCIDENTES DE SEGURIDAD	11.Riesgo disponibilidad de la información	Posible	Mayor	Medio	Posible	Mayor	Medio
7.GESTIÓN DE INCIDENTES DE SEGURIDAD	6.Riesgo de violación de privacidad	Improbable	Mayor	Medio	Improbable	Mayor	Medio
7.GESTIÓN DE INCIDENTES DE SEGURIDAD	9.Riesgo de falta de cumplimiento normativo	Posible	Mayor	Medio	Posible	Mayor	Medio
7.GESTIÓN DE INCIDENTES DE SEGURIDAD	5.Riesgo de interrupción del servicio	Probable	Moderado	Alto	Probable	Moderado	Alto
7.GESTIÓN DE INCIDENTES DE SEGURIDAD	2.Riesgo de pérdida de datos	Posible	Mayor	Medio	Posible	Mayor	Medio

7.GESTIÓN DE INCIDENTES DE SEGURIDAD	10.Riesgo de falta de concientización en seguridad	Probable	Moderado	Alto	Probable	Moderado	Alto
7.GESTIÓN DE INCIDENTES DE SEGURIDAD	12.Riesgo no identificación causa raíz del problema	Posible	Moderado	Medio	Posible	Moderado	Medio

Fuente: Elaboración propia basado en Norma ISO 27000/31000.

Figura 8. Perfil de Riesgo por Procesos

Fuente: Elaboración propia basado en Norma ISO 27000/31000.

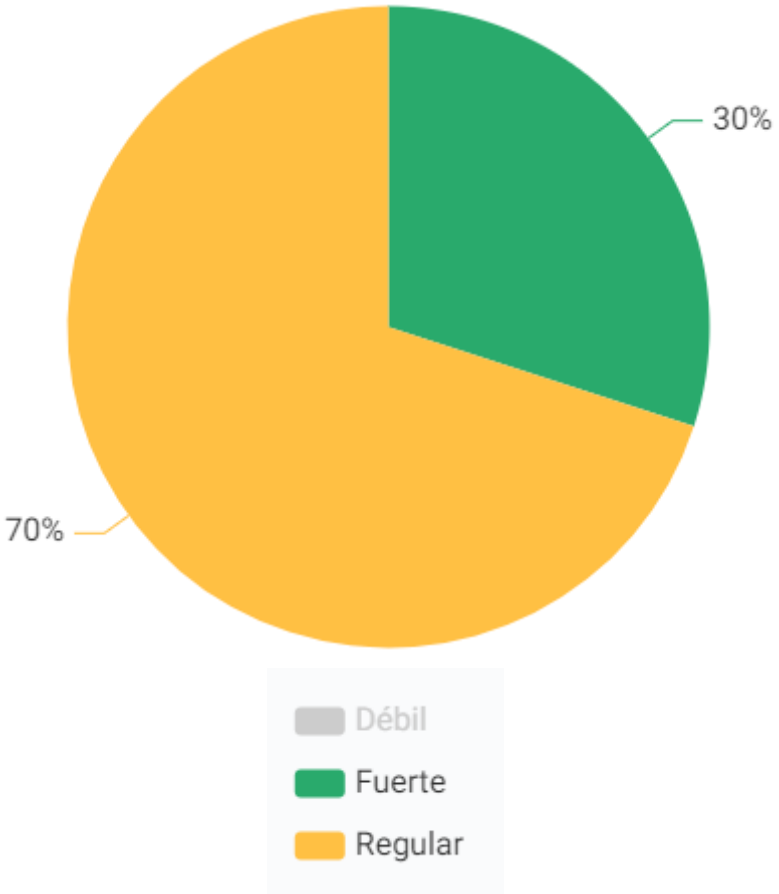
Tabla 8. Preparación Solidez del Control.

Nombre	Calificación cuantitativa	Calificación cualitativa	Tipo de control	Tipo de ejecución	¿Se ejecuta con alguna frecuencia?	¿Está documentado?
01.Políticas y procedimientos de seguridad de la información	70.00%	regular	Detectivo	Combinado	Si	Documentado
02.Acceso controlado y gestión de identidad	82.50%	fuerte	Preventivo	Automático	Si	Documentado
03.Protección de la red	80.00%	regular	Preventivo	Automático	Si	Parcialmente Documentado
04.Encriptación de datos	64.00%	regular	Preventivo	Manual	No	Sin Documentar
05.Copias de seguridad y recuperación de desastres	82.50%	fuerte	Preventivo	Automático	Si	Documentado

06.Monitoreo y detección de eventos de seguridad	75.00%	regular	Preventivo	Combinado	Si	Parcialmente Documentado
07.Concientización y capacitación en seguridad	45.50%	regular	Preventivo	Combinado	No	Sin Documentar
08.Gestión de parches y actualizaciones	54.00%	regular	Preventivo	Manual	Si	Sin Documentar
09.Gestión de proveedores y terceros	71.50%	regular	Preventivo	Manual	No	Sin Documentar
10.Auditorías y pruebas de seguridad	85.50%	fuerte	Preventivo	Combinado	No	Sin Documentar

Fuente: Elaboración propia basado en Norma ISO 27000/31000.

Figura 8. Solidez del Control



Fuente: Elaboración propia basado en Norma ISO 27000/31000.

XII. BIBLIOGRAFÍA

- ISO/IEC 27001: International Organization for Standardization. (2013). ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements.
- ISO/IEC 27002: International Organization for Standardization. (2013). ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls.
- ISO/IEC 27005: International Organization for Standardization. (2018). ISO/IEC 27005: Information technology - Security techniques - Information security risk management.
- ISO 31000: International Organization for Standardization. (2018). ISO 31000: Risk management - Guidelines.
- ISO/IEC 27001:2013. (2013). Information technology - Security techniques - Information security management systems - Requirements.
- Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.
- Siponen, M., Vance, A., & Willison, R. (2019). Cultivating a cybersecurity culture: Implications for misunderstanding and data breaches. Journal of Management Information Systems, 36(1), 346-373. doi:10.1080/ 07421222.2019.1575037.
- Talabis, M., Martin, J., & Gaudet, S. (2014). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress.
- Purser, S. (2012). Information Security Management: A Practitioner's Guide. BCS, The Chartered Institute for IT.
- Pritchard, C. L., & Freeman, K. S. (2014). Risk Management: Concepts and Guidance. CRC Press.
- Head, G. L. (2015). Risk Assessment: A Practical Guide to Assessing Operational Risks. Rothstein Publishing.
- Esteves, J. B. (2019). Information Security Management Systems: A Novel Approach for Securing Critical Infrastructure. IEEE Systems Journal, 13(1), 453-460.
- Vacca, J. R. (2012). Computer and Information Security Handbook (2nd ed.). Morgan Kaufmann.
- Nikkel, B. (2017). Incident Response and Computer Forensics (3rd ed.). Jones & Bartlett Learning.
- Jones, A., & Valli, C. (2014). Incident Response: A Strategic Guide to Handling System and Network Security Breaches. Syngress.

2. **DEJESE** sin efecto cualquier documento metodológico, herramienta y recomendaciones sobre esta misma materia. Siendo este un documento actualizado con las nuevas recomendaciones de seguridad.
3. La matriz de riesgos en seguridad de la información y su implementación comenzará a regir a contar de la fecha de publicación de la presente resolución municipal.

Anótese, comuníquese, regístrese y archívese.

ILUSTRE MUNICIPALIDAD SECRETARIO MUNICIPAL SANTO DOMINGO

RENZZO ROJAS TRONCOSO
SECRETARIO MUNICIPAL

ILUSTRE MUNICIPALIDAD ALCALDE SANTO DOMINGO

FRANCISCO DEVIA CASTRO
ALCALDE(S)

DRC/LRV/jva
DISTRIBUCIÓN DIGITAL: Dirección de Desarrollo Comunitario; Dirección de Administración y Finanzas (Tesorería); Archivo Asesoría Jurídica; Dirección de Control Interno; y Archivo Municipal.
INT-DEC-1925-MUNI-2023

Susan Ramírez Osorio
Firmado digitalmente por Susan Ramírez Osorio
Fecha: 2023.07.27 11:48:24 -04'00'

Este es un documento oficial de la I. Municipalidad de Santo Domingo. Puede verificar su autenticidad escaneando este código QR o ingresando directamente a la página web: **decretos.santodomingo.cl**