UNIVERSIDAD MARIANO GÁLVEZ

INGENIERÍA EN SISTEMAS DE
INFORMACIÓN Y CIENCIAS DE LA COMPUTACIÓN

SEGURIDAD Y AUDITORÍA DE SISTEMAS

SECCIÓN B

TAREA #4

POLÍTICAS DE CIBERSEGURIDAD ISO - 27032

ESTUARDO ANTONIO DE JESUS ROMERO REYES	**5190 17 24335**
FRANCISCO JAVIER CARDONA MEDINA	**5190 17 12950**
LUIS ANIBAL ZAPETA DE LEON	**5190 17 5850**
MARIO ROBERTO MANZO ESTRADA	**5190 05 3915**

VILLA NUEVA, GUATEMALA, AGOSTO 2021

Índice

INTRODUCCIÓN

El presente documento pretende demostrar las diferentes razones por las cuales es necesario la implementación de normas y procesos que nos ayuden a gestionar nuestros centros de datos y redes empresariales, esto para poder minimizar los riesgos de sufrir un ataque cibernético. El principal objetivo que tienen los diferentes ataques es la obtención de información, a nivel empresarial esta puede ser información de nuestros empleados, clientes, proveedores o accionistas, teniendo esto como punto de partida, el servicios que empleamos para resguardar toda la información sensible de nuestra empresa u organización es nuestra base de datos.

Por lo general nuestras redes están diseñadas para proteger su acceso, integridad y datos empresariales, se apoyan tanto con software como con hardware orientadas a distintas amenazas y por lo general dejamos nuestros demás servicios sin mayores configuraciones de seguridad. Nuestra tarea está enfocada a un servicio específico, como lo es nuestra base de datos, en la cual aplicaremos servicio de base de datos virtualizado aplicando encapsulamiento para tener una capa adicional de seguridad.

Aunque la norma ISO 27032 no es obligatoria, nos sirve como referencia para poder aplicar una estrategia para minimizar los riesgos, esta estrategia es la detección, respuesta y preparación. En nuestro trabajo nos apoyaremos de la herramienta Docker, el cual nos permite la creación de diferentes contenedores para aplicaciones de software que puedan ser ejecutadas en cualquier equipo que tenga docker, sin importar el sistema operativo que se tenga por debajo.

ISO 27032 GESTIÓN DE LA CIBERSEGURIDAD

La norma ISO / IEC 27032 es una guía sobre el manejo de incidentes de seguridad de la información, sobre el proceso de cómo debemos actuar para la detección, notificación y evaluación de los incidentes de seguridad de la información y las vulnerabilidades.

Dicha norma hace referencia a 'Ciberseguridad' o 'Seguridad del ciberespacio', que se define como la protección de la privacidad, integridad y accesibilidad de la información de datos en el ciberespacio. El ciberespacio es reconocido como el lugar donde interactúan personas, software y servicios tecnológicos a nivel mundial.

El estándar internacional ISO / IEC 27032 está destinado a enfatizar el papel de los diferentes valores en el ciberespacio, con respecto a la seguridad de la información, la seguridad de la red y de Internet, y la protección de la infraestructura de información crítica (CIIP).

ISO / IEC 27032 como estándar internacional proporciona un marco de políticas para implantar en el modelo de negocio confiabilidad, colaboración, intercambio de información y orientación técnica para la integración del sistema entre las partes interesadas en el ciberespacio.

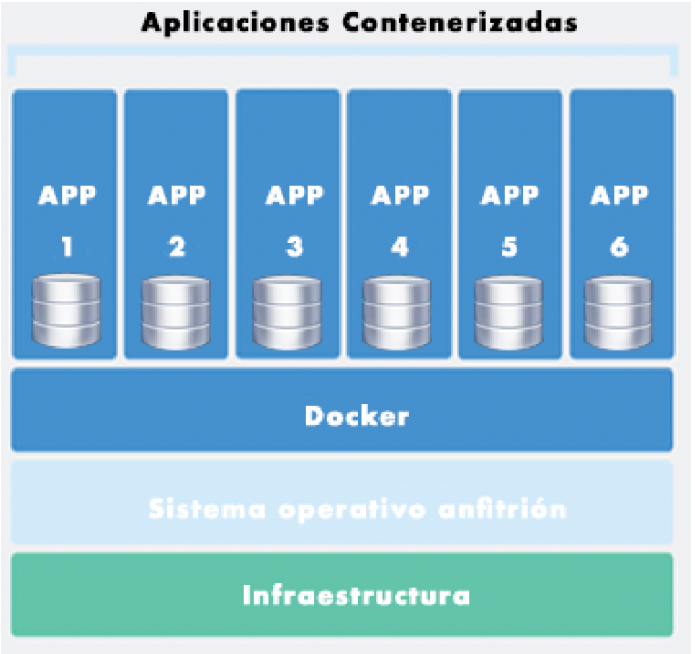
MODELO DE NEGOCIO

La implementación de seguridad hacia las bases de datos es algo que tiene mucha importancia a nivel general pues son muchas las organizaciones que utilizan sus servicios públicos, para poder correr las bases de datos a petición de sus distintos programas web a través de la internet.

El modelo de negocio se basa en un software web que consume el servicio de una base de datos de un CRUD completo, en el que pueden crear registros, leer registros, actualizar registros y borrar algunos registros que están relacionados a la funcionalidad del programa, para ello se utiliza una base de datos en la nube, con un servicio de terceros.

Pero en la organización quieren tener los datos en un servidor propio, para resguardar la seguridad de sus clientes, quienes son principalmente proyectos hidroeléctricos. Dicho esto se piensa implementar una base de datos en la organización y desean publicar el servicio, para que todas las consultas y registros, se tengan de manera local.

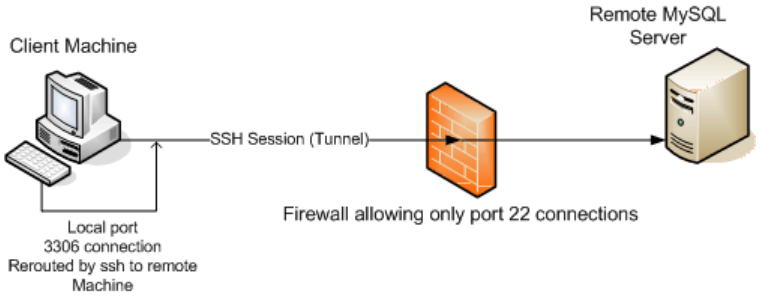
Entonces el objetivo del proyecto es aplicar la seguridad en la publicación de este servicio, realizando una encapsulación que proteja y provea anonimato sobre el verdadero host que contendrá la base de producción.

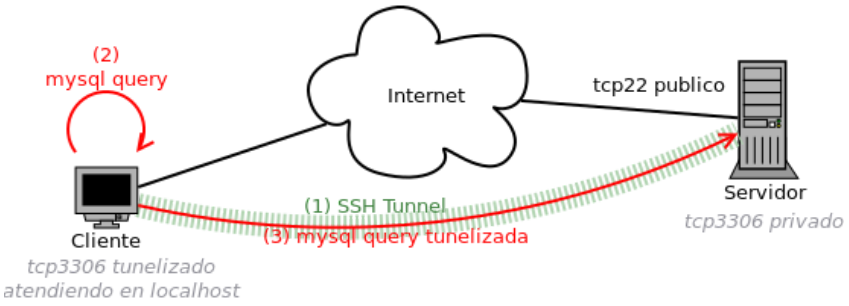


De manera predeterminada MySQL usa conexiones no codificadas inseguras entre el cliente y el servidor, lo que significa que cualquier individuo malintencionado puede ver, y aún modificar los datos que están siendo transmitidos entre éstos. Dependiendo del tipo de información que se está manejando, puede que esta situación resulta bastante preocupante.

Seguridad de la base de datos

El encapsulamiento de la base de datos permite la conexión segura de forma remota a nuestro servicio, como medida de seguridad en eventualidades donde existe el bloqueo del puerto principal,como alternativa y como medida de protección de nuestros servicios y datos.





IMPLEMENTACIÓN DE ISO 27032 EN MODELO DE NEGOCIO

1. **Alcance y campo de aplicación**

   El alcance de esta propuesta será únicamente para el backend encargado del almacenamiento de datos, entiéndase la base de datos que se desea publicar como un servicio para ser consumido por la aplicación web en los equipos cliente de cada uno de los usuarios que tienen acceso en proyecto hidroeléctrico, quien fungirá únicamente como la interfaz gráfica de interacción con el usuario o frontend.

2. **Aplicabilidad**

   - Audiencia: Dirigido a la población objetivo del proyecto hidroeléctrico que tiene acceso al programa web para la consulta y manipulación de datos, es decir los usuarios de este.

   - Limitación: Esta aplicación se limita únicamente a la parte del SGDB quien es el encargado de proveer el servicio al programa web del proyecto hidroeléctrico.

3. **Referencias normativas**

   Los siguientes documentos referenciados son indispensables para la aplicación de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para referencias sin fecha, se aplica la última edición del documento de referencia (incluidas las enmiendas).

   ISO / IEC 27000, *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario*

4. **Términos y definiciones**

   Para los propósitos de este documento, se aplican los términos y definiciones dados en ISO / IEC 27000, y los siguientes.

   - Adware: aplicación que impulsa la publicidad a los usuarios y / o recopila el comportamiento de los usuarios en línea.

   - Solicitud: Solución de TI, que incluye software de aplicación, datos y procedimientos de la aplicación, diseñada para ayudar a los usuarios de una organización a realizar tareas particulares o manejar tipos particulares de problemas de TI mediante la automatización de un proceso o función empresarial.

   - Proveedor de servicios de aplicaciones: operador que proporciona una solución de software alojada que proporciona servicios de aplicaciones que incluyen modelos de entrega basados en web o cliente-servidor. De este modelo de negocio: operadores de la planta hidroeléctrica, proveedores de aplicaciones de oficina y proveedores de almacenamiento en línea.

   - Servicios de aplicación: Software con funcionalidad entregada bajo demanda a los suscriptores a través de un modelo en línea que incluye aplicaciones basadas en web o cliente-servidor. Implementación: La BD de MYSQL.

   - Software de la aplicación: software diseñado para ayudar a los usuarios a realizar tareas particulares o manejar tipos particulares de problemas, a

diferencia del software que controla la computadora misma, para este trabajo el programa web de las plantas hidroeléctricas.

- Activo: cualquier cosa que tenga valor para un individuo, una organización o un gobierno

- Avatar: representación de una persona que participa en el ciberespacio, también puede verse como un "objeto" que representa la encarnación del usuario.

- Ataque: Intentar destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo

- Potencial de ataque: Potencial percibido para el éxito de un ataque, en caso de que se lance un ataque, expresado en términos de la experiencia, los recursos y la motivación del atacante

- Vector de ataque: Ruta o medio por el cual un atacante puede obtener acceso a una computadora o servidor de red para entregar un resultado malicioso.

- Ataque combinado: Ataque que busca maximizar la severidad del daño y la velocidad del contagio combinando múltiples métodos de ataque.

- Bot: robot programa de software automatizado utilizado para llevar a cabo tareas específicas, se usa a menudo para describir programas, que generalmente se ejecutan en un servidor, que automatizan tareas como el reenvío o la clasificación de correo electrónico, también se describe como un programa que opera como agente para un usuario u otro programa o simula una actividad humana. En Internet, los bots más ubicuos son los programas, también llamados arañas o rastreadores, que acceden a sitios web y recopilan su contenido para los índices de los motores de búsqueda.

- Botnet: software de control remoto, específicamente una colección de bots maliciosos, que se ejecutan de forma autónoma o automática en computadoras comprometidas

- Cookie: capacidad o ticket en un sistema de control de acceso, también se le denomina a los datos intercambiados por ISAKMP para prevenir ciertos ataques de denegación de servicio durante el establecimiento de una asociación de seguridad o según el caso también pueden ser los datos intercambiados entre un servidor HTTP y un navegador para almacenar información de estado en el lado del cliente y recuperarla más tarde para uso del servidor

- Control: contramedida medios para gestionar el riesgo, incluidas políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- Ciberdelito: actividad delictiva en la que los servicios o aplicaciones en el ciberespacio se utilizan para un delito o son el objetivo de un delito, o donde el ciberespacio es la fuente, herramienta, objetivo o lugar de un delito.

- Ciberseguridad: condición de estar protegido contra las consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, ocupacionales, psicológicas, educativas o de otro tipo de fallas, daños, errores, accidentes, daños o cualquier otro evento en el Ciberespacio que pudiera considerarse no deseable.

- La seguridad cibernética o Seguridad del ciberespacio: es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

5. Términos abreviados

Los términos abreviados son un listado de siglas con sus respectivas definiciones, como lo puede ser CERT: Equipo de Respuesta ante Emergencias Informáticas, AS: Sistema Autónomo o AP: Punto de acceso.

6. Visión general

Una visión general es una pequeña introducción a la norma aplicada, donde se realizan las explicaciones pertinentes a temas como ciberseguridad, dentro de las amenazas existentes en el ciberespacio se analizan en relación a los activos, estas amenazas se pueden dividir en dos categorías: Amenazas a activos personales y amenazas a activos organizacionales

7. Partes interesadas en el Ciberespacio

Son los entes que interactúan en el ciberespacio:

- Los consumidores hacen uso de servicios dispuestos en el ciberespacio. En el caso del proyecto es la organización de la hidroeléctrica y los usuarios que estarán ingresando a revisar otros temas.
- Los Proveedores ponen a disposición servicios para ser utilizados por los consumidores, como servicios de conectividad (ISP) y de acceso a las aplicaciones (ASP)
- Un individuo o una organización se vuelve consumidor cuando accede al Ciberespacio o a cualquier servicio disponible en el ciberespacio

8. Activos en el Ciberespacio

Un Activo es cualquier cosa que tenga valor para un individuo, una organización o Gobierno (cláusula 4.6):

Los activos personales involucran a componentes importantes para las personas en su interacción en el ciberespacio como dispositivos móviles, correo electrónico, fotos, videos, documentos, identidad digital, cuenta bancaria, información crediticias, datos médicos, datos de seguros, pagos en línea, impuestos, etc

Los activos organizacionales involucran a componentes para los procesos de negocios de las organizaciones como servidores, aplicaciones, bases de datos, estrategias, PNPs

Los activos físicos involucran a componentes que poseen presencia física en la realidad como servidores, dispositivos de networking, dispositivos móviles, etc.

Los activos virtuales involucran a componentes únicamente digitales y dependen de un activo físico que los ejecute (Sistemas operativos, Aplicaciones, bases de Datos, etc)

9. Amenazas contra la protección del Ciberespacio

Por definición, una amenaza tiene el potencial de hacer daño a los activos, tales como información, procesos y sistemas y por lo tanto puede causar un perjuicio a las organizaciones . Se asocia con el aspecto negativo del riesgo. La naturaleza de la amenaza es siempre indeseable.

La cláusula 4.46 Amenaza, de la ISO 27032 hace referencia a que esta es una "Causa potencial de un incidente no deseado, que puede resultar en un perjuicio a un sistema, individuo u organización."

Entonces en nuestro modelo de negocio dividiremos esto en dos grupos principales:

a) Amenazas a los activos personales:
b) Amenazas a los activos de la organización:

10. Roles de las partes interesadas en la Ciberprotección

Los roles son importantes para la seguridad de información, ya que permiten la asignación de responsabilidades y/o derechos de acceso que se asignan en base a una función en lugar de tener que asignarlos a las personas individuales.

Hay roles que admiten funciones de seguridad, la capacidad de asignar autorizaciones de acceso basadas en roles simplifica la administración

- Responsible (Comprometido, realiza la tarea)
- Accountable (Rinde Cuentas, Propietario, Autoriza)
- Consulted (Consultado)
- Informed (Informado)

11. **Directrices para las partes interesada**s

Dirección ejecutiva:

Implementar una estrategia de seguridad de la información efectiva requiere la integración y cooperación de los dueños de los procesos. Un resultado exitoso es la alineación de las actividades de seguridad de la información con los objetivos de negocio. El grado al cual esto se logre determinará la rentabilidad del programa de seguridad de la información para alcanzar el objetivo deseado de brindar un nivel predecible y definido de aseguramiento para los procesos de negocio y un nivel aceptable del impacto que pueden tener los incidentes adversos

Comité directivo:

Para asegurar la participación de todos aquellos que tengan un interés en la empresa y que se vean afectados por las consideraciones de la seguridad, muchas organizaciones recurren a un comité directivo que esté conformado por representantes de nivel superior de los grupos afectados. Ello facilita llegar a un consenso sobre las prioridades, ventajas y desventajas. También sirve como un canal efectivo de comunicaciones y provee una base continua para asegurar la alineación del programa de seguridad con los objetivos de negocio. También puede ser fundamental para alcanzar la modificación del comportamiento hacia una cultura más conducente a una seguridad adecuada.

CISO (Chief Information Security Officer) Director / Gerente de Seguridad de la Información:

- Reporta al ejecutivo principal CEO (Chief Executive Officer)

- El alcance y la amplitud de la seguridad de la información hoy en día es tal que la autoridad requerida y la responsabilidad asumida recaerá inevitablemente en un responsable de mando ejecutivo (Gerente/Director).
- La responsabilidad legal se extiende hasta la estructura de mando y en última instancia residirá en la alta dirección y el consejo de dirección.
- Todas las organizaciones tienen un Chief Information Security Officer (CISO), aún si nadie ostenta el título. Puede ser el CIO, oficial de seguridad (CSO-Chief Security Officer), oficial de finanzas (CFO-Chief Financial Officer) o en algunos casos, el oficial ejecutivo principal CEO (Chief Executive Officer)
- La gerencias están ascendiendo el puesto de Oficial de Seguridad de la Información a un puesto de mando intermedio o ejecutivo, ya que las organizaciones empiezan a darse cuenta d que dependen de la información y de las crecientes amenazas a las que está expuesta

Gerente de Seguridad:

- El Desarrollo de la estrategia de seguridad
- Supervisar el programa y las iniciativas de Seguridad
- Coordinar con los propietarios de los procesos de negocio
- Asegurarse de llevar a cabo evaluaciones de riesgo e impacto
- Desarrollar la estrategia de mitigación de riesgo
- Hacer cumplir las políticas y el cumplimiento normativo
- Monitorear la utilización y eficacia de los recursos de seguridad
- Desarrollar e implementar una monitorización de métricas
- Dirigir y monitorear actividades de seguridad
- Gestionar incidentes de Ciberseguridad y su solución, lecciones aprendidas

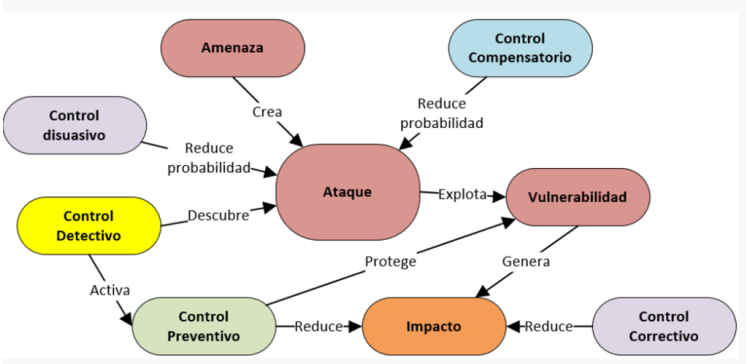
Profesional de ciberseguridad:

- El análisis de políticas, tendencias e inteligencia.
- Utiliza habilidades de detección y resolución de problemas
- Se esfuerza por comprender mejor cómo puede pensar o comportarse un adversario.

- La complejidad inherente de su trabajo requiere que la fuerza laboral de ciberseguridad posea no solo una amplia gama de habilidades técnicas de TI, sino también capacidades analíticas avanzadas.
- Un profesional de ciberseguridad puede ser parte de la alta dirección.

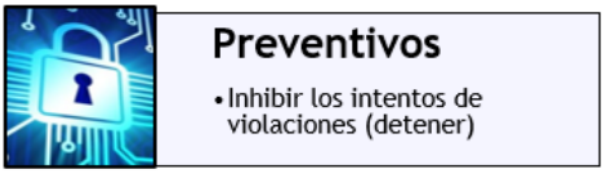
12. Controles de Ciberprotección

Los controles son los componentes principales que se deben tener en cuenta cuando se desarrolla una estrategia de seguridad de la información.



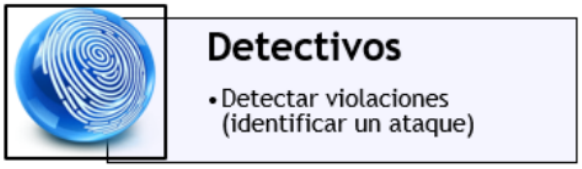
Categorías de Controles (por su propósito):

Preventivos:



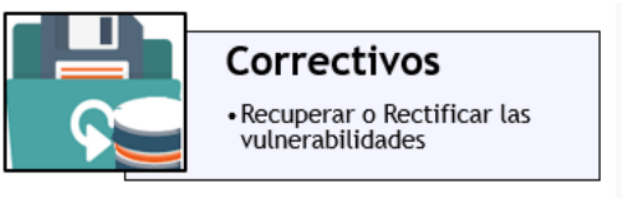
Inhiben los intentos de violaciones a la política de seguridad e incluyen controles como ejecución de control de acceso, encriptación y autenticación (detener)

Detectivos:



Advierten acerca de violaciones o intentos de violación a la política de seguridad e incluyen controles como pistas de auditoría, métodos de detección de intrusos y sumas de control (checksum)

Correctivos:

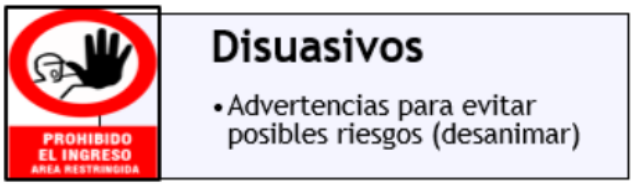


Recuperan o rectifican las vulnerabilidades. Los procedimientos de respaldo y restablecimiento son una medida correctiva porque permiten recuperar un sistema en caso de que el daño haya sido tan extenso que no se puede continuar con el procesamiento si no se recurre a medidas correctivas

Compensatorios:

Compensan por un aumento en el riesgo, al añadir pasos de control que mitigan el riesgo; por ejemplo, agregar un componente de pregunta/respuesta o doble factor de autenticación de seguridad a controles de acceso débiles puede compensar la deficiencia

Disuasivos:



Generan advertencias que desaniman al atacante, pueden evitar posibles riesgos como letreros de advertencia en las pantallas de inicio de sesión o recompensas por el arresto de intrusos (hackers).

13. Marco del intercambio y coordinación de información

    Framework 4.5 v3

14. Anexos
    - Disposición de la Ciberseguridad
    - Recursos adicionales
    - Ejemplos de documentos relacionados

CONCLUSIONES

Entre las cosas que mejora la implantación de este estándar ISO podemos concluir tenemos muchos beneficios entre ellos es proteger los datos y la privacidad de la organización de las amenazas cibernéticas. Fortalezca sus habilidades en el establecimiento y mantenimiento de un programa de ciberseguridad Desarrollar las mejores prácticas para gestionar las políticas de ciberseguridad.

Mejorar el sistema de seguridad de la organización y su continuidad comercial. Genere confianza en las partes interesadas para sus medidas de seguridad. Responda y recupere más rápido en caso de incidente.

REFERENCIAS

- ISO / IEC 27032:2021 Information technology — Security techniques — Guidelines for cybersecurity (2012) Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en