**Plan de contingencia**

En este documento se presentara el plan de contingencia respecto a todos los fallos o caidas con respecto a los servidores que se tienen montados para el proyecto, se mostraran como se aplicaran las soluciones respecto a cierto tipo de fallas que se pueden encontrar ya sea a nivel fisico o a nivel logico, tambien explicaremos algunas recomendaciones y prevenciones para que sepa como intervenir en este tipo de casos, que si bien es cierto nadie esta seguro, pero permitira tener una mayor prevencion al respecto.

Cualquier cosa puede ser expuesta a un ataque informatica desde una red o un servidor completo hasta el mas minimo dispositivo de la empresa, por eso, hay que generar estrategias para prevenir estos errores que suelen no ser por algun proceso o demas de hardware, si no, con errores humanos tambien, por eso, es que es necesario contar con la experiencia para dar solucion ante este tipo de casos. Despues de cada explicacion de las posibles fallas se daran recomendaciones al respecto de cada una.

Tambien se dara una breve definicion de los conceptos que se utilizaran aca alrededor de todas las explicaciones para tener un contexto mas acorde al tema y ademas tener en cuenta los conceptos para aplicarlos en este plan.

# Glosario

A continuacion se presentaran los siguientes signifcados que se utilizaran en el documento.

**Amenaza:** Una amenaza se refiere a un incidente nuevo o recién descubierto que tiene el potencial de dañar un sistema o su empresa en general. Una amenaza es un evento hipotético en el que un atacante usa la vulnerabilidad.[1]

**Contingencia:** nos referimos a la posibilidad de que algo acontezca, es decir, a la posibilidad de que algo ocurra, o no ocurra. Es un término de uso muy común en áreas como la prevención y los seguros, en los cuales se utiliza, además, como sinónimo de riesgo.[2]

**Elementos en riesgo:** Son los elementos los cuales son los causantes de las fallas o caidas del sistema, que en este caso pueden ser de nivel fisico o logico.[3]

**Vulnerabilidad:** Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos.[3]

**Riesgo:** Los riesgos se producen al existir una amenaza que tenga consecuencias negativas para los sistemas de información de la empresa. El análisis de riesgos debe recoger información detallada de todos los riesgos a los que se ve expuestos y cómo afectan a la empresa. [4]

**Gravedad:** Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).[5]

**Seguridad:** Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. [6]

**Datos:** Es una representación simbólica ya sea numérica o alfabética, cuyo valor está listo para ser procesado por un ordenador y mostrarlo a un usuario en modo de información.[7]

**Incidente:** Es un proceso de identificar, administrar, registrar y analizar las amenazas o incidentes de seguridad ocurridos en una organización. Este proceso busca ofrecer una visión sólida y completa de cualquier problema de seguridad informática dentro de la plataforma tecnológica.[8]

**Activo:** Hace referencia a recursos tecnológicos del entorno de la información comunicativa que forman parte de las empresas y tienen como objetivo la difusión de información. Estamos hablando por ejemplo de hardware y software.[9]

**Plan de contingencia:** Define cómo responderás si eventos imprevistos te hacen desviar de tu plan original, por ejemplo, qué medidas tomarás si pierdes un cliente clave o si tu servicio de software se cae durante más de tres horas.[10]

# Evaluacion de los riesgos y recomendaciones

## Riesgos en nivel fisico y de hardware

Dentro de este enunciado se mencionaran algunas de las problematicas fisicas que se presentarian las cuales danarian el sistema y provocaria fallos de tal manera que el sistema no sirva, cabe recalcar, que la empresa Eva Beauty y baby estara trabajando con dos servidores en los cuales se manejaran las copias de seguridad, se manejaran tres copias de seguridad, en donde:

1. En las maquinas virtuales se les hara una copia de seguridad tanto local como del computador como tal en donde estan instaladas, tambien dentro de los archivos de las maquinas se haran copias de seguridad.
2. En donde se montara un servidor padre y otro hijo, se anadiran las copias de seguridad, aparte de las bases de datos del sistema en las cuales estaran funcionando disponibles todo el tiempo y el esclavo sera el que tendra las copias de las maquinas virtuales, mas la del pc, mas la base de datos del proyecto completo.

Como bien sabemos los danos fisicos casi siempre son producidos por errores humanos, en los cuales puede salir o resultar muy costoso si no se preveen de la mejor manera, por eso se van a explicar unos de los ejemplos mas comunes, de los riesgos que existen y que comprometen no solo el hardware de los servidores si no tambien, la seguridad fisica debido a que puede generar danos de hardware.

* **Corto circuito:** Este es uno de los caso mas comunes de los que se suelen ver en los errores humanos, lo cual significa que hay una mala instalacion del sistema electrico o que algun componente se encuentra danado, por lo tanto, esto genera una inestabilidad en la corriente electrica y que genera un corto circuito.
  + **Accion preventiva:** La solucion para este tipo de cosas son varias, la primera es revisar bien el sistema de instalacion electrica que este corriendo el voltaje adecuado y que ademas, haya una buena conexión e instalacion de los puntos de corriente. Tambien, puede ser causado por un dano en algun componente de los servidores o demas, lo ideal es estar haciendo revisiones seguidas de la infraestructura fisica para evitar estos danos.
* **Incendio**: Los incendios son casos tambien que pasan en la infraestrcutura fisica debido a que se genera por fallas como la mencionada anteriormente que es el corto circuito, o a veces por una mala infraestructura fisica, dado que estos dispositivos necesitan contar con un aire acondicionado de precision, el cual permite regular la temperatura del cuarto donde se encuentra, al no tenerlo se sobrecalientan y pueden generar tanto calor que crean un incendio.
  + **Accion preventiva:** Tener siempre a la mano un extintor en caso de emergencia que se encuentre directamente en el cuarto donde estan los servidores, y tambien contar con la instalacion adecuada del aire acondicionado debido a que esto evita a que el servidor se sobrecaliente.
* **Errores humanos:** Esta es siempre la razon por la cual se dana algo asi todo el servidor se encuentre funcionando, las razones aca abarcan muchisimas opciones, pero las mas principales siempre suelen ser:
  + Accesos no autorizados de gente no especializada en el ambito inofrmatico al cuarto de servidores, debido a que esta gente no tiene conocimiento de como administrarlo, debido a esto ejecuta algo mal en la maquina del servidor y se lo puede tirar.
  + Ingreso de alimentos o bebidas al cuarto de servidores, dado a que si llega a ocurrir un accidente eso puede comprometer la seguridad virtual y fisica del servidor, ademas los alimentos pueden ensuciar los dispositivos lo cual tambien danaria su estructura.
    - **Accion preventiva:** La solucion ante este tipo de problemas son solamente asignar un acceso autorizado al cuarto donde se encuentra el servidor, prohibir rotundamente el acceso de alimentos a esta sala, tambien tener un registro de quienes estan entrando y saliendo debido a que si se llega a generar un robo de algun dispositivo la persona se tiene que hacer responsable de eso.

## Riesgos en nivel logico y virtual

En este enunciado se denominan la mayoria de los ataques que van relacionados con las maquinas que operan en nuestra empresa, se van a nombrar los mas comunes actualmente y a los cuales podriamos ser expuestos, porque como bien se menciona anteriormente nada esta seguro, a cada uno de los riesgos aparte de explicarse que es, tambien se le dara una clasificacion junto con su respectiva recomendación para evitar lo mas posible que este incidente ocurra. Tambien se va a aplicar el mismo plan de contingencia que se menciono en el capitulo anterior, el cual explica las copias de seguridad y demas, la unica diferencia que tiene del enciso anterior, seria en un caso de malware llamado “Wannacry” el cual para el se aplicaran los siguientes pasos:

* El software malicioso o malware llamado “Wannacry” Como su nombre sugiere, el ransomware es un software malicioso que cifra sus archivos y exige un pago (un rescate) para poder descifrarlos. WannaCry sigue siendo una de las cepas de ransomware más conocidas que hay. [12] Este malware tiene una calificacion de CVE de 10.0 la cual es la mas alta, debido a que esto compromete con toda la integridad del sistema[11](Esta informacion es sacada de la base de datos de CVE que es una de las mas especializadas en enumerar y dictaminar la gravedad de las vulnerabilidades y ataques)
* Despues de explicado esto, si el malware llega a atacar un servidor, se cuentan con varias copias de seguridad dentro de las cuales no solo estan dentro de las maquinas virtuales, la del host y en maquinas aparte, si no que tambien se tendran dos copias de seguridad en nube con parte del servicio de OneDrive que maneja Daniel Esteban Valdivieso Diaz y MEGA que maneja Nicolas Elias Bossio Rincon.
* Lo primero que se hace es apagar la maquina totalmente, apagar los servidores, poner a correr el sistema de manera sin conexión, mientras se le hace una revision al sistema para ver que tan infectado esta, hacer un formateo completo y montar las copias de seguridad despues sobre el sistema arrancado.
* Se haran revisiones periodicas y se buscaran a traves de auditorias las vulnerabilidades, para revisar cual puedo ser la falla, la desconexion de corriente electrica que se hace es porque si se le quita la corriente por donde se encuentra infectado hara que el sistema pare y se cierrre inmediatamente debido a que no tendra con que funcionar, de esta forma inhabilitando el paso del o de los atacantes.

Ya mencionado todo esta excepcion o caso particular, se empezaran aclarando uno por uno los riesgos, la forma en como atacan, su clasificacion CVE y aparte de esos sus respectivas acciones preventivas. Cabe aclarar que para darle la clasificacion, se revisa la base de datos, se busca un caso especifico y en base a ese se sacan conclusiones del tipo de ataque para asi darle su puntuacion siendo 0 la mas baja y 10 la mas alta.

* **Phishing:** es un delito cibernético en el que un objetivo u objetivos son contactados por correo electrónico, teléfono o mensaje de texto por alguien que se hace pasar por una institución legítima para atraer a las personas a proporcionar datos confidenciales, como información de identificación personal, detalles bancarios y de tarjetas de crédito, y contraseñas.[13] Estos son muy comunes en empresas donde se tienen secciones de atencion al cliente debido a que es la persona que casi no conocen de seguridad inormatica, y por lo tanto se pueden hacer campanas de ingenieria social a traves de correos, redes sociales, paginas web y demas, por lo cual son mas vulnerables y de ahi ingresaria el virus al sistema de la empresa. La clasificacion CVE de este ataque es de 7.3[14]
  + **Accion preventiva:** Lo primero que hay que hacer con esto es sensibilizar a todos los empleados de la empresa sobre conceptos basicos de seguridad para usuarios, en los cuales se toman algunas discreciones para evitar este tipo de ataques, tambien tener un servicio de correo privado es una muy buena solucion dado que da mas controles a los que se reciben, dado que es la forma mas comun cuando hacen phishing.
* **Ramsomware:** Ransomware es un tipo de malware o software malicioso, que bloquea los datos de la víctima o el dispositivo informático y amenaza con mantenerlo bloqueado — o peor — a menos que la víctima le pague al atacante un rescate.[15] Estos se suelen inyectar de muchas maneras al sistema pero las mas comunes que casi siempre se utilizan son el phishing y ataques via redes de conexión de datos que se veran mas adelante, la clasificacion de esta vulnerabilidad es de un 4.6 debido a que si un sistema esta bien configurado, es mas dificil que entre debido a que si no usa la tecnica de phishing va a ser mas complicado acceder a la informacion del sistema.[16]
  + **Accion preventiva:** Una de las acciones preventivas para este tipo de ransomware, es tener una buena configuracion del sistema, mantener redes de conexión privadas, aparte tener un firewall, el cual es un cortafuegos que bloquea conexiones del servidor hacia ciertos sistios y hacia ciertas direcciones, porque esto comprometeria que alguna pagina no registrada infecte el servidor cuando se le de acceso a esta.
* **SQL injection:** es un ataque en el que se inserta código malicioso en cadenas que luego se pasan a una instancia de SQL Server para analizar y ejecutar. Cualquier procedimiento que construya declaraciones SQL debe revisarse para detectar vulnerabilidades de inyección porque SQL Server ejecutará todas las consultas sintácticamente válidas que reciba.[17] Estos ataques se deben en su mayoria a las bases de datos comprometidas, en el caso de la de nosotros es asi, por lo tanto se menciona debido a que sus ataques se deben en su mayoria a puertos abiertos de la base de datos junto con malas configuraciones de firewall de red, si clasificacion CVE se le da de 0 lo cual indica que es la mas baja, pero si se deja escalar podria tener grandes repercusiones, dado que esto tumbaria nuestro servidor.[18]
  + **Accion preventiva:** Para este tipo de ataques lo que se utiliza regularmente es que se hace una configuracion segura y exhaustiva en cuanto a la base de datos, dado a que esta es a la que atacan directamente, ejecutando consultas a tope lo cual puede colgar y comprometer el servidor, lo que se suele prever es una revision de puertos, que se cierren despues de cierto tiempo de inactividad no mayor a 5s, ademas la configuracion de cierre de sesiones de los dispositivos, debido a que si estos no se cierran pueden acceder a ese computador y comprometer la base de datos.
* **Ataque DdoS:** es un intento malicioso de interrumpir el tráfico normal de un servidor objetivo, servicio o red al abrumar al objetivo o su infraestructura circundante con una avalancha de tráfico de Internet.[19] Este ataque es uno de los mas peligrosos debido a que este compromete el sistema del servidor y aparte de eso de la red, con un nivel medio de gravedad y una clasificacion CVE de 5.0[20]
  + **Accion preventiva:** Como casi todas las acciones que se han mencionado anteriormente, casi siempre dependen de las configuraciones, pero en este tipo de ataques que comprometen la red y el servidor, son un poco mas complejos, debido a que se tiene que prever bastante, el tema de las configuraciones de las Ips de los dispostivos las cuales deben ser dinamicas para de esta forma, esten actualizandose cada cierto tiempo, tambien tener en cuenta que acceso a que direcciones se tienen configurada en el firewall, dado que este ataque ataca directamente con la integridad del servidor.
* **Ataque DNS:** Un ataque DNS es cualquier ataque dirigido a la disponibilidad o estabilidad del servicio DNS de una red. Los ataques que aprovechan el DNS como su mecanismo como parte de su estrategia general de ataque, como el envenenamiento de caché, también se consideran ataques de DNS.[21] Estos ataque se hacen directamente al servidor lo cual imposibilita que los dispositivos puedan acceder a dominios de red de la plataforma y a algunos recursos. Esta es una falta de tipo grave y que cuenta con un CVE de 5.5 lo cual indica un nivel alto de compromiso con nuestro sistema.[22]
  + **Accion preventiva:** Este es uno de los ataques al cual se le pueden prestar mas atencion dado que este tipo de ataques bloquea la mayoria de protocolos de red los cuales son el TCP, UDP, ICMP, todos los servicios de red y demas, por lo tanto, se debe contar uno con personal especializado en este tema de conexiones de redes y en seguridad para evitar este tipo de cosas, ademas la configuracion de lo que se ha mencionado anteriormente, de manera segura y especifica, dado que al hacerla de esta forma generara mas tiempo para acceder a los recursos.

## **Ejecucion del plan de contingencia**

Despues de mencionar todos los posibles riesgos a los cuales se nos puede exponer nuestro sistema y de como pueden generar compromisos serios en cuanto a la disponibilidad, integridad y seguridad de la informacion, se ejecuto un plan de contingencia con las caracteristicas que se han mencionado a lo largo del documento, contando la excepcion mencionada en el capitulo anterior, por lo tanto en caso de alguna falla o de algun riesgo se tienen en cuenta los siguientes encisos:

1. Los encargados de la ejecucion del plan de contingencia en este caso son las personas encargadas de la infraestructura tecnologica del proyecto, los cuales son Daniel Esteban Valdivieso Diaz y Nicolas Elias Bossio Rincon.
2. Se tiene la disponibilidad de copias de seguridad replegadas en cada una de las maquinas virtuales, dentro de las maquinas del host que aloja cada maquina virtual, una copia de seguridad remota distribuida en cada computador con la informacion del resto de las maquinas y con una copia de seguridad en la nube que se manejaran a traves del OneDrive y MEGA.
3. Hay dos servidores extras anadidos, los cuales haran de tipo servidor espejo, en el cual habra un principal manejando las copias de seguridad y un servidor “hijo” como le hemos denominado que tendra el registro tambien de estas maquinas virtuales con una copia de seguridad extra.
4. En el caso de que algun incidente de estos ocurra lo que se ejecutara es que principalmente se le quitara la conexión al servidor, y se trabajara de manera local mientras, se desconecta el servidor que se encuentre infectado y se pondra a correr el servicio con algunas copias de seguridad que se encuentren en las otras maquinas
5. Dado el caso de que se comprometa el sistema completo, se hara un formateo de las maquinas completas y se recuperara con las copias de seguridad que se encuentren en la nube, se escogieron estas porque, la integridad y disponibilidad que ofrecen son mayores a las locales, debido a que estas se encuentran aseguradas por las empresas que prestan estos servicios, ademas estas copias son revisadas constantemente por los de infraestructura y ademas, la disponibilidad da la ventaja de acceder a ella desde cualquier sitio de manera remota a cualquier hora.

### Referencias

[1] "¿Qué es una amenaza informática? ¿Cómo contenerla?" Blog HostDime Latinoamérica, servidores dedicados. <https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/> (accessed Mar. 16, 2023).

[2] "Contingencia - Concepto, tipos, ejemplos y plan de contingencia." Concepto. <https://concepto.de/contingencia/> (accessed Mar. 16, 2023).

[3] "Tipos de Vulnerabilidades y Amenazas informáticas." AMBIT - BST. <https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-informáticas> (accessed Mar. 16, 2023).

[4] "Análisis de riesgos informáticos y ciberseguridad." AMBIT - BST. <https://www.ambit-bst.com/blog/análisis-de-riesgos-informáticos-y-ciberseguridad> (accessed Mar. 16, 2023).

[5] Inicio - Uninavarra. <https://uninavarra.edu.co/wp-content/uploads/2016/12/GT-PL-02-PLAN-DE-CONTIGENCIA-INFORMATICO-1-1.pdf> (accessed Mar. 16, 2023).

[6] "¿Qué es la seguridad informática y cómo puede ayudarme?" VIU. <https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme> (accessed Mar. 16, 2023).

[7] "¿Qué son los datos en informática?" icorp. <https://icorp.com.mx/blog/que-son-los-datos-en-informatica/> (accessed Mar. 16, 2023).

[8] "GestiÃ³n de incidentes informÃ¡ticos." Universidad AutÃ³noma de Chihuahua. <https://ciberseguridad.uach.mx/empresas/gestion-de-incidentes-informaticos/> (accessed Mar. 16, 2023).

[9] P. Castejón. "Activos Informáticos: Las 7 claves que tienes que conocer." Perito Judicial GROUP©. <https://peritojudicial.com/activos-informaticos/> (accessed Mar. 16, 2023).

[10] "Qué es un plan de contingencia y cómo crear uno en 8 pasos • Asana." Asana. <https://asana.com/es/resources/contingency-plan> (accessed Mar. 16, 2023).

[11] "CVE-2002-0013 : Vulnerabilities in the SNMPv1 request handling of a large number of SNMP implementations allow remote attackers to cause." CVE security vulnerability database. Security vulnerabilities, exploits, references and more. <https://www.cvedetails.com/cve/CVE-2002-0013/> (accessed Mar. 16, 2023).

[12] N. Latto. "¿Qué es WannaCry?" ¿Qué es WannaCry? <https://www.avast.com/es-es/c-wannacry> (accessed Mar. 16, 2023).

[13] "Phishing | What Is Phishing?" Phishing | General Phishing Information and Prevention Tips. <https://www.phishing.org/what-is-phishing> (accessed Mar. 16, 2023).

[14] "CVE-2007-1736 : Mozilla Firefox 2.0.0.3 does not check URLs embedded in (1) object or (2) iframe HTML tags against the phishing site bla." CVE security vulnerability database. Security vulnerabilities, exploits, references and more. <https://www.cvedetails.com/cve/CVE-2007-1736/> (accessed Mar. 16, 2023).

[15] "What is Ransomware? | IBM." IBM - Deutschland | IBM. <https://www.ibm.com/topics/ransomware> (accessed Mar. 16, 2023).

[16] "CVE-2020-6023 : Check Point ZoneAlarm before version 15.8.139.18543 allows a local actor to escalate privileges while restoring files in." CVE security vulnerability database. Security vulnerabilities, exploits, references and more. <https://www.cvedetails.com/cve/CVE-2020-6023/> (accessed Mar. 16, 2023).

[17] "SQL Injection - SQL Server." Microsoft Learn: Build skills that open doors in your career. <https://learn.microsoft.com/en-us/sql/relational-databases/security/sql-injection?view=sql-server-ver16> (accessed Mar. 16, 2023).

[18] "CVE security vulnerability database. Security vulnerabilities, exploits, references and more." CVE security vulnerability database. Security vulnerabilities, exploits, references and more. <https://www.cvedetails.com/vulnerability-list/opsqli-1/sql-injection.html> (accessed Mar. 16, 2023).

[19] "What is DDos attack?" Microsoft. https://www.microsoft.com/es-ww/security/business/security-101/what-is-a-ddos-attack. (accedido el 16 de marzo de 2023).

[20] "CVE-2000-0138 : A system has a distributed denial of service (DDOS) attack master, agent, or zombie installed, such as (1) Trinoo, (2) T". CVE security vulnerability database. Security vulnerabilities, exploits, references and more. https://www.cvedetails.com/cve/CVE-2000-0138/ (accedido el 16 de marzo de 2023).

[21] "Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)". CVE security vulnerability database. Security vulnerabilities, exploits, references and more. https://www.cvedetails.com/microsoft-bulletin/ms09-008/ (accedido el 16 de marzo de 2023).

[22] "Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)". CVE security vulnerability database. Security vulnerabilities, exploits, references and more. https://www.cvedetails.com/microsoft-bulletin/ms09-008/ (accedido el 16 de marzo de 2023).