

**Gestion del Riesgo**

ANSOLIDATA

**Análisis de Riesgos Informáticos**

Tema:

Gestión del Riesgo en una Organización



**Desarrollado por:**

**Fermín Javier Durón Sánchez**

**Isaías Gamaliel Rojoc Sac**

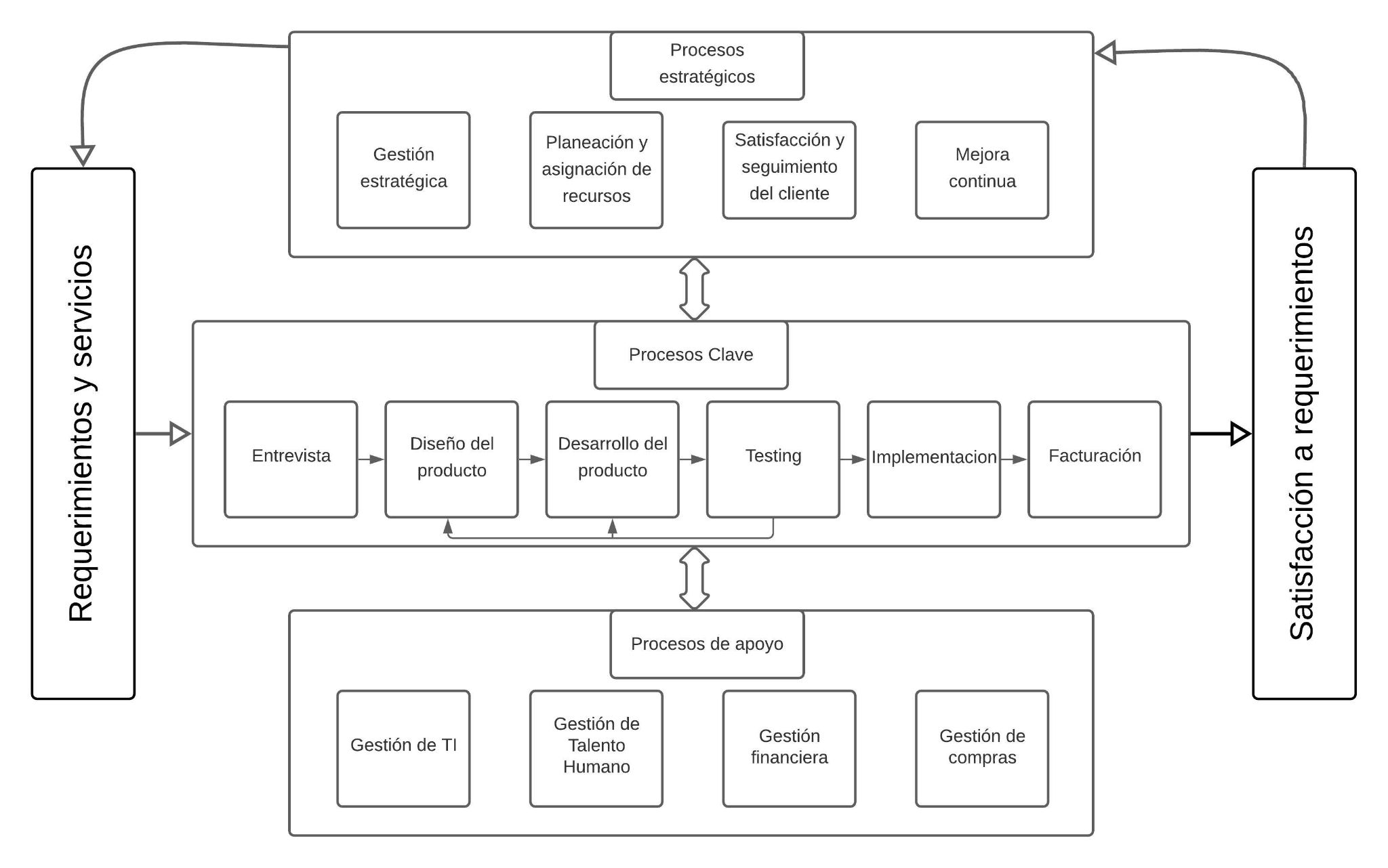
**Angel Ramón Paz López**

**1. INTRODUCCIÓN A LA ARQUITECTURA**

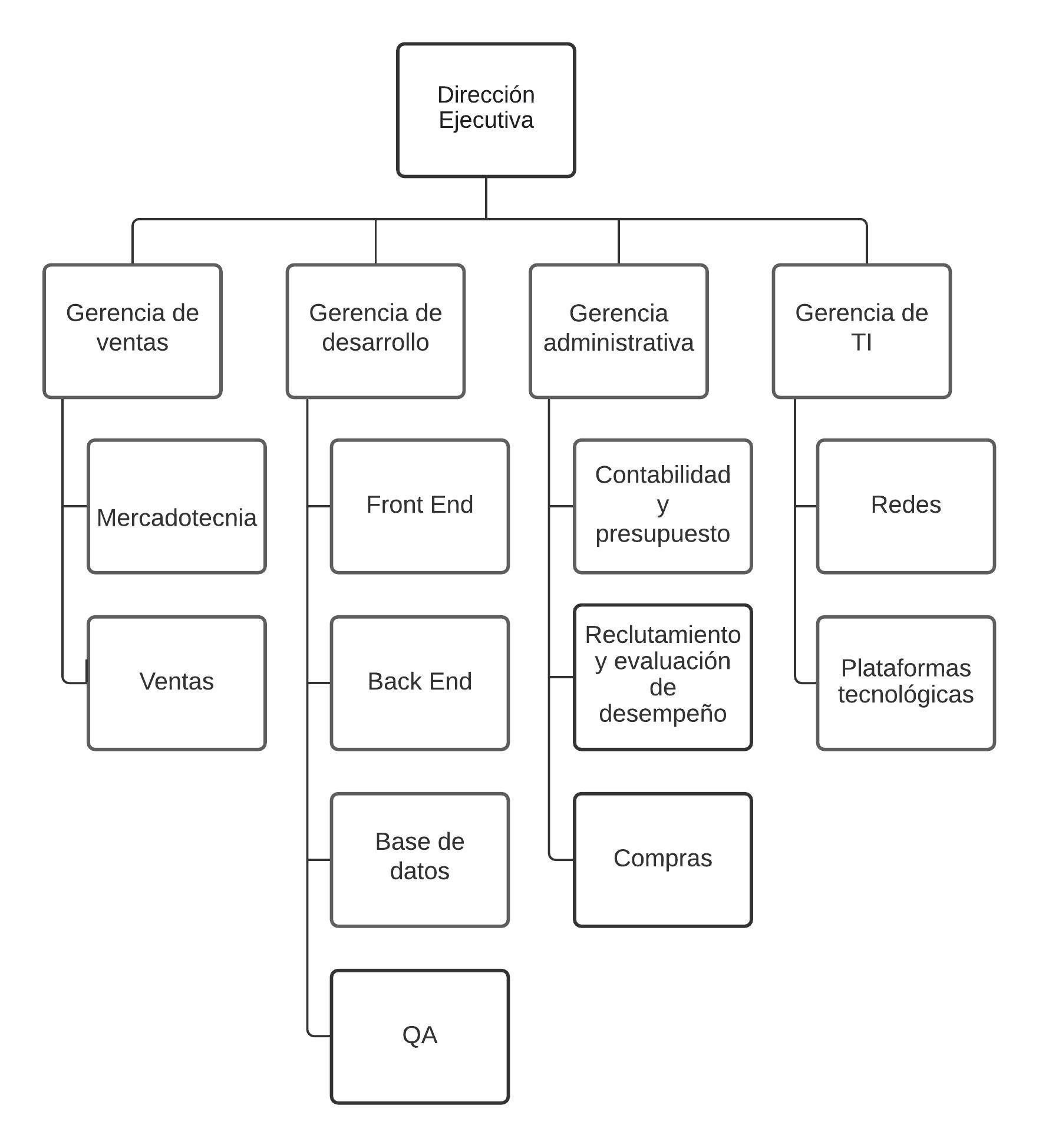
La estructura organizacional forma parte fundamental para el logro de los objetivos de ANSOLIDATA, esta se basa en en un modelo funcional, en el cual cada uno de los puestos es ocupado por personas especializadas en cada una de las áreas lo cual garantiza un buen desempeño en todas sus áreas.

A continuación se presenta el mapa de procesos y el organigrama dentro de ANSOLIDATA, la toma de decisiones está a cargo de la Dirección General quienes dictan las políticas y estrategias a seguir por la compañía, siguiendo el flujo del organigrama se cuenta con cuatro gerencias en las cuales se fundamenta la compañía, la primera es la Gerencia Comercial o Gerencia de Ventas, la cual tiene como responsabilidad atraer y buscar clientes para brindar servicios en los cual ANSOLIDATA se especializa, en cuanto a la Gerencia de Desarrollo en base a las necesidades de los clientes desarrolla soluciones web de alta calidad y orientada a la seguridad, la Gerencia Administrativa se responsabiliza de la atracción de talento, los aspectos legales y económicos de la compañía así como suplir la demandas internas para la operación, por último la Gerencia de TI es la base tecnológica sobre la cual opera ANSOLIDATA, ella provee soporte y servicios tecnológicos a los usuarios internos y a los requerimientos de clientes en base al diseño de los proyectos por parte del área de desarrollo.

Figura 1. Mapa de procesos



Fuente: ANSOLIDATA

Figura 2. Organigrama de ANSOLIDATA****

Fuente: ANSOLIDATA

A continuación, se describen las principales atribuciones de cada una de las áreas de la organización.

|  |
| --- |
| Director ejecutivo |
| Jefe inmediato: Ninguno |
| Responsabilidad principal: planear y supervisar todas las actividades administrativas, tecnológicas y financieras de la organización |
| Responsabilidades generales |
| Velar por el correcto cumplimiento de las decisiones tomadas por la Junta Directiva |
| Analizar los requerimientos realizados por cada área velando por el mejor desempeño en un balance económico-efectividad |
| Estudio de mercado y análisis de la competencia |
| Presentación de informes para la junta directiva en base a la periodicidad establecida |
| Representación de la organización de forma interna y externa como representante legal de la misma |

|  |
| --- |
| Director de comercialización |
| Jefe inmediato: Director Ejecutivo |
| Responsabilidad principal: Responsable de contar y ejecutar un plan comercial de la compañía y asegurar la sustentabilidad económica de la compañía |
| Responsabilidades generales |
| instruir, supervisar, brindar seguimiento y asesoramiento al personal de ventas |
| Calcular y proyectar los objetivos comerciales de la organización |
| Generar planes estratégicos de atracción de clientes y mantenerlos fieles a la organización |

|  |
| --- |
| Director de desarrollo |
| Jefe inmediato: Director Ejecutivo |
| Responsabilidad principal: Velar por la estandarización de procesos y mejoras prácticas en el desarrollo de software con el propósito de cumplir los requerimientos de los clientes con altos niveles de satisfacción |
| Responsabilidades generales |
| Establece un plan estratégico para el análisis, diseño, desarrollo e implementación de cada sistema a desarrollar |
| Garantiza la seguridad informática en los sistemas desarrollados |
| Proporcionar capacitaciones relacionadas al área a los miembros de su equipo de trabajo con el fin de mejorar el desempeño |
| Proporcionar canales de comunicación efectivos con los clientes en pro de la satisfacción del mismo |
| Vela por el éxito de cada uno de los proyectos del área |

|  |
| --- |
| Director de administrativo |
| Jefe inmediato: Director Ejecutivo |
| Responsabilidad principal: Velar por el adecuado uso y administración de los recursos de la organización |
| Responsabilidades generales |
| Realizar los contratos requeridos por la organización |
| verificar y aprobar las órdenes de compra requeridas por las distintas áreas en beneficio de la organización |
| Garantizar que el personal contratado sea el idóneo para los puestos disponibles, así como realizar las contrataciones en el menor tiempo posible |
| Garantizar un ambiente adecuado para la realización de las tareas de cada uno de los colaboradores |
| Garantizar la eficiencia operativa en base a los aspectos económicos y legales |

|  |
| --- |
| Director de TI |
| Jefe inmediato: Director Ejecutivo |
| Responsabilidad principal: Garantizar la disponibilidad y correcto funcionamiento de los equipos que componen la infraestructura tecnológica de la organización |
| Responsabilidades generales |
| Mantener la disponibilidad de cada uno de los servicios interno en base la infraestructura de TI |
| Mantener un correcto QoS priorizando el tráfico crítico para la organización |
| Coordinación, análisis, diseño e implementación de proyectos relacionados al área de TI dentro de la organización |
| Administración del área de TI, siendo el responsable del desempeño, disponibilidad crecimiento y operación de los distintos componentes que componen la infraestructura de TI y sus plataformas, tanto en hardware como software. |

**PLANTEAMIENTO DEL PROBLEMA**

Uno de los problemas que tiene una organización es la falta de recursos para poder eliminar o mitigar los riesgos. Por eso es importante tener un planeamiento de riesgos para poder afrontar las amenazas. Comenzando con la detección y eliminación de vulnerabilidades y amenazas, tener un plan de contingencia para poder disminuir o mitigar el riesgo.

**OBJETIVOS**

Definir las actividades y objetivos que la organización ANSOLIDATA considera para la implementación de la gestión de sus riesgos para así poder lograr sus objetivos de negocio y mejorar todos los procesos de administración de éstos.

Una vez implementada una gestión de riesgos la organización podrá identificar los activos de información, el desarrollo, procesos, documentación e implementación de políticas, estándares, procedimientos y directrices que garanticen confidencialidad, la integridad, y disponibilidad de la información, aumentará la probabilidad de alcanzar sus objetivos, mejorar el gobierno, establecerá bases fiables para la toma de decisiones y la planificación, mejorará la eficacia y eficiencia operacional dentro de la organización, mejorará la prevención de pérdidas y minimización de las mismas. Por lo cual aplicar una gestión de seguridad en la organización ANSOLIDATA es muy importante por lo mencionado anteriormente, usando de manera idónea las herramientas de gestión como clasificación de datos, evaluación y análisis de riesgos para así poder identificar, evaluar y monitorear las amenazas y las vulnerabilidades con que cuenta la organización y a la vez establecer y fortalecer mediante políticas de seguridad necesarias donde se reflejen los objetivos de la organización y las responsabilidades que cada uno de los miembros participantes de la organización realizarán en sus actividades diarias y el compromiso de estos para aplicar la gestión de la seguridad de información.

**JUSTIFICACIÓN**

Es importante explicarle a la gerencia la importancia de los riesgos que puede sufrir la organización si no se toman medidas para eliminar o mitigar las amenazas antes de que sucedan. Realizando un análisis de riesgos para detectar las causas de las amenazas en la pandemia, se han encontrado varias vulnerabilidades tanto de código como de los servidores y vemos que hay bastante riesgo si no se llegan a eliminar o mitigar las vulnerabilidades y amenazas. Los estudios indican que se han incrementado los ataques cibernéticos a raíz de la pandemia por lo tanto hay que tomar más precauciones en la organización.

**2. ACTIVOS EN SEGURIDAD DE LA INFORMACIÓN**

**2.1 ACTIVOS**

* Computadoras
* UPS’s
* Modems
* Monitores
* Mesas de trabajo
* Televisores
* Discos duros
* Memorias USB
* Firewall de navegación A
* Firewall de navegación B
* Internet para navegación A
* Internet para navegación B
* Firewall socios B
* Firewall socios A
* Internet socios A ISP A
* Internet socios A ISP B
* Internet socios B ISP A
* Internet socios B ISP A
* Router publicaciones A
* Router publicaciones B
* Internet de publicaciones A ISP A
* Internet de publicaciones A ISP B
* internet de publicaciones B ISP A
* Internet de publicaciones B ISP B
* GTM A
* GTM B
* IPS A
* IPS B
* WAF A
* WAF B
* Nexus 7K A
* Nexus 7K B
* Switch perimetrales A
* Switch perimetrales B
* FO A - SP 1
* FO B - SP 2
* Switch acceso A
* Switch acceso B
* Switch acceso C

**2.2 AMENAZAS**

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Como, por ejemplo:

* Malware
  + Troyanos, Virus, Gusanos, Ransomware, Keyloggers, entre otros
* Ataques DDoS
* Infección SQL
* Ataques XSS
* Siniestro
* Intrusos
* Catástrofes naturales causadas por terremotos, inundaciones e incendios.
* Autenticación fraudulenta
* Acceso a la red por personal no autorizado
* Acceso a sistemas por personal no autorizado
* Fuga y daños a la información por razones humanas
* Infección por spyware
* Robo de credenciales
* Software obsoleto o sin licencia
* Mala administración de equipos
* Divulgación de información privada
* Fallo en servicios de comunicación
* Perdida de energía eléctrica comercial
* Mal funcionamiento en equipos
* Mal uso de software
* Uso no autorizado de software
* Fallo en equipos de red
* Fallo en equipos de cómputo
* Falta de personal apto para cada área de la organización
* Infracciones legales por incumplimiento a contratos
* Incumplimientos contractuales por parte de los clientes
* Daños causados por pruebas de penetración
* Seguridad física
* Empleados sin formación
* Ataque por Ransomware

**2.3 VULNERABILIDADES**

Las siguientes listas son las vulnerabilidades que puede llegar a tener la organización:

* Desactualizaciones del sistema
  + PHP, Windows Server, Apache, Nginx, entre otros
* Vulnerabilidades en los atributos de las Cookies
* Vulnerabilidades XSS
* Vulnerabilidades CSRF
* Configuraciones activas que deben de estar desactivadas
  + HTTP TRACE / TRACK Methods Enabled
  + Expose\_php Set to On
* Archivos Javascript sin atributo de Integridad
* Archivos que muestren información activos
  + PHPinfo()
* Errores en la gestión de Recursos
* Errores que permitan acceso a directorios
* Errores en la gestión y asignación de permisos
* Contraseñas fáciles de predecir
* Mantenimientos inadecuados
* Mala administración de la red
* Respaldos inapropiados
* Susceptibilidad de equipos a cambio de temperatura, humedad y variación de voltajes
* Registro de cambios físicos deficientes
* Falta de concientización sobre los riesgos que implica una mala seguridad de la información
* Mal análisis de calidad de software desarrollado
* Falta de documentación sobre procesos, roles y atribuciones del personal
* Falta de política de acceso de mínimo privilegio
* Deficiencia en procesos onboarding y offboarding
* Falta de sistema de respaldo de energía ante cortes eléctricos de la energía comercial
* Descargas no controladas de internet
* Políticas de navegación web libres
* Desmotivación de empleados
* Falta de auditorías internas
* Falta de documentación sobre cada uno de los roles y atribuciones

**3. ANÁLISIS DE IMPACTO DEL NEGOCIO**

**3.1 IMPACTO**

* Robo de información a los usuarios
* Información comprometida de los servidores
* Divulgación de archivos confidenciales
* Los ataques Cross-Site Script entre sitios pueden robar cookies, lo que podría provocar la suplantación de identidad del usuario o comprometer la cuenta de la aplicación
* La explotación exitosa permite a un atacante remoto no autenticado obtener información confidencial o bloquear la aplicación resultando en una condición de denegación de servicio
* Los atacantes pueden aprovechar este problema para ejecutar comandos arbitrarios dentro del contexto del usuario que ejecuta la aplicación afectada
* La explotación exitosa permite que un atacante remoto no autenticado divulgue archivos locales en los hosts
* La explotación exitosa permite al atacante comprometer el sistema
* Un atacante puede aprovechar este problema para ejecutar un código de secuencia de comandos arbitrario en el navegador de un usuario desprevenido en el contexto del sitio afectado
* Un atacante remoto podría aprovechar esta vulnerabilidad para leer un byte más allá del final de un búfer, lo que podría afectar la integridad de la confidencialidad y la disponibilidad de los datos en el sistema de destino
* La explotación exitosa permite a los atacantes remotos eludir la autenticación y acceder a información confidencial

**3.2 PROBABILIDAD**

La probabilidad es la posibilidad de que ocurra un riesgo, tomando en cuenta los controles actuales y su efectividad. En el siguiente cuadro mostraremos algunos ejemplos de las amenazas y su impacto, probabilidad y el riesgo en la organización.

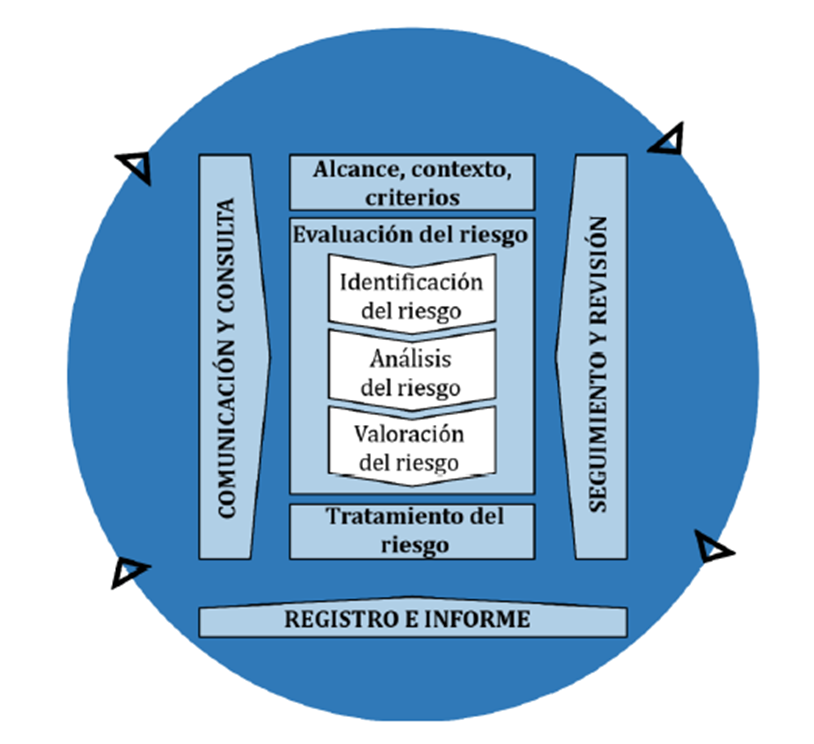
|  |  |  |  |
| --- | --- | --- | --- |
| **Amenaza** | **Impacto** | **Probabilidad** | **Riesgo** |
| **Ataque por Ransomware** | Catastrófico | Posible | Alto |
| **Robo de Credenciales** | Mayores | Posible | Alto |
| **Infección por Spyware** | Mayores | Muy Probable | Alto |
| **Pérdida de suministro eléctrico** | Moderado | Posible | Medio |
| **Inyección SQL** | Mayores | Posible | Alto |
| **Malware** | Moderado | Muy Probable | Medio |
| **Ataques DDoS** | Mayores | Posible | Alto |
| **Ataques XSS** | Mayores | Probable | Alto |
| **Siniestros** | Mayores | Poco Probable | Alto |
| **Intrusos** | Mayores | Posible | Medio |
| **Software obsoleto o sin licencia** | Moderado | Probable | Medio |
| **Acceso a la red por personal no autorizado** | Mayores | Posible | Alto |
| **Catástrofes naturales causadas por terremotos, inundaciones e incendios** | Catastrófico | Poco Probable | Alto |
| **Acceso a sistemas por personal no autorizado** | Mayores | Posible | Alto |

**4. DEFINIR CONTEXTO, ALCANCE Y CRITERIOS DE LA GESTIÓN DEL RIESGO**

**4.1 PROCESO DE GESTIÓN DE RIESGOS**

Entre las diferentes metodologías para la realización del presente trabajo tenemos:

La metodología usada en el proceso de gestión de riesgos en este informe se fundamenta en la norma ISO 31000:2018, la cual tiene un enfoque de proceso por lo que hay que seguir varios pasos para que la implementación de una gestión de riesgos sea eficaz y cumpla los objetivos trazados.



Norma ISO 3100:2018

**CONTEXTO**

Se deberá recopilar toda la información del ambiente, identificando los aspectos internos y externos de la organización en donde será implementado y ejecutado el Análisis de Riesgo. En este punto se debe tener claro los objetivos, propósitos y las actividades que se tienen que realizar para llevar a cabo la Gestión de Riesgos.

**4.2 PROPÓSITOS**

* Soporte al Sistema de Gestión de la Seguridad de la Información
* Cumplimiento Legal
* Plan de Continuidad de negocios
* Plan de respuesta a incidentes

La organización optó por implementar un Sistema de Gestión de Seguridad de la Información para llevar a cabo una gestión del riesgo de la seguridad de la información, ya que la Alta dirección de la organización está consciente de lo valioso que es la protección de sus activos y para ellos es necesario una planificación donde lleve a cabo las actividades necesarias como ser en primer lugar el conocimiento de los riesgos y vulnerabilidades que existen tanto en lo interno y externos, las cuales pueden afectar los objetivos de las mismas, para así con ellos tener un Plan de respuesta e incidentes para poder prevenir eventos no deseados o mitigar el impacto .

**4.3 ALCANCE**

Orientada a los jefes de los organización, a la alta dirección de la organización, jefe de operaciones, y a todos los líderes de cada área quienes son los que estarán vinculados directamente con la implementación de la gestión de riesgo en la organización con el objetivo de brindar seguridad al ciclo de vida de la información de la organización, gestionar los riesgos, optimizar la gestión de riesgos en base a los resultados de evaluaciones del análisis de riesgos para ir mejorando los procesos, todo esto con el propósito de alcanzar la misión de la organización.

**4.4 DEFINICIÓN DE OBJETIVOS**

El propósito del establecimiento del alcance, contexto y criterios es poder adaptar el proceso de la gestión del riesgo, para así permitir una evaluación del riesgo de manera eficaz y un tratamiento apropiado del riesgo con el fin de poder identificar las posibles amenazas o vulnerabilidades de cualquier proceso que pueda poner en riesgo los activos de la organización. El alcance, el contexto y los criterios implican definir el alcance del proceso, y comprender los contextos tanto interno como externo.

La Dirección de alto nivel de la organización debe ser la encargada de la difusión de los objetivos para así todos los niveles, procesos de las mismas se comprometan del modo deseado. También es importante definir un presupuesto para los recursos que se van a utilizar para la materialización de los planes de riesgos**.**

**4.5 NOMBRAMIENTO DE RESPONSABLES**

La dirección debe delegar responsabilidades de las labores de la Gestión de Riesgos en uno o más empleados. **Este punto dependerá del tamaño de la organización**

Los grupos de trabajo no deben superar los 10 miembros. Si la organización es pequeña el límite debería ser hasta 5 miembros.

Si el personal es interno, tienen la ventaja de que conocen el área donde se realizarán las evaluaciones la cual esto es una garantía para la dirección. Se puede recurrir a aquellos cargos que tengan una visión parcial o total de los procesos.

Cuando la organización es demasiado pequeña o no tiene la capacidad para realizar este tipo de tareas, la organización puede apoyarse con un ente externo indicado para que le brinde servicio de consultoría.

**4.6 RESPONSABLES DE LOS ACTIVOS**

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Descripción general | Tipo de activo | Responsable del activo |
|
| Firewall de navegación A | dispositivo en clúster activo-pasivo con firewall de navegación B, el objetivo es proporcionar conectividad hacia internet a la organización y su red de agencias | Infraestructura | Dirección de TI |
| Firewall de navegación B | dispositivo en clúster activo-pasivo con firewall de navegación A, el objetivo es proporcionar conectividad hacia internet a la organización y su red de agencias | Infraestructura | Dirección de TI |
| Internet para navegación A | Servicio con protocolo de alta disponibilidad, este se utiliza para proporcionar navegación web a toda la corporación | Infraestructura | Tigo |
| Internet para navegación B | Servicio con protocolo de alta disponibilidad, este se utiliza para proporcionar navegación web a toda la corporación | Infraestructura | Claro |
| Firewall socios B | dispositivo en clúster activo-pasivo con firewall socios A, la función del clúster es brindar conectividad con empresas socias de negocio | Infraestructura | Dirección de TI |
| Firewall socios A | dispositivo en clúster activo-pasivo con firewall socios B, la función del clúster es brindar conectividad con empresas socias | Infraestructura | Dirección de TI |
| Internet socios A ISP A | Servicio con protocolo de alta disponibilidad, este se utiliza para la comunicación con socios comerciales para cada uno de las distintas transacciones | Infraestructura | Tigo |
| Internet socios A ISP B | Servicio con protocolo de alta disponibilidad, este se utiliza para la comunicación con socios comerciales para cada uno de las distintas transacciones | Infraestructura | Claro |
| Internet socios B ISP A | Servicio con protocolo de alta disponibilidad, este se utiliza para la comunicación con socios comerciales para cada uno de las distintas transacciones | Infraestructura | Tigo |
| Internet socios B ISP A | Servicio con protocolo de alta disponibilidad, este se utiliza para la comunicación con socios comerciales para cada uno de las distintas transacciones | Infraestructura | Claro |
| Router publicaciones A | Router en con protocolo de alta disponibilidad con Router de Publicaciones B, este es es un punto de convergencia para el tráfico de servicios públicos que ingresa a la institución | Infraestructura | Dirección de TI |
| Router publicaciones B | Router en con protocolo de alta disponibilidad con Router de Publicaciones B, este es un punto de convergencia para el tráfico de servicios públicos que ingresa a la institución | Infraestructura | Dirección de TI |
| Internet de publicaciones A ISP A | Servicio en HA con servicio B del mismo ISP, con el fin de brindar alta disponibilidad ante posible caída de uno de los dos servicios, también se brinda alta disponibilidad a nivel de proveedor ante una caída general de uno de los dos ISP | Infraestructura | Tigo |
| Internet de publicaciones A ISP B | Servicio en HA con servicio B del mismo ISP, con el fin de brindar alta disponibilidad ante posible caída de uno de los dos servicios, también se brinda alta disponibilidad a nivel de proveedor ante una caída general de uno de los dos ISP | Infraestructura | Claro |
| internet de publicaciones B ISP A | Servicio en HA con servicio A del mismo ISP, con el fin de brindar alta disponibilidad ante posible caída de uno de los dos servicios, también se brinda alta disponibilidad a nivel de proveedor ante una caída general de uno de los dos ISP | Infraestructura | Tigo |
| Internet de publicaciones B ISP B | Servicio en HA con servicio A del mismo ISP, con el fin de brindar alta disponibilidad ante posible caída de uno de los dos servicios, también se brinda alta disponibilidad a nivel de proveedor ante una caída general de uno de los dos ISP | Infraestructura | Claro |
| GTM A | Equipo en clúster activo-pasivo con en datacenter A, el objetivo es realizar el balanceo de cargas del tráfico entrante para cada uno de los servicios de acceso público que brinda la institución | Infraestructura | Dirección de TI |
| GTM B | Equipo en clúster activo-pasivo con en datacenter B, el objetivo es realizar el balanceo de cargas del tráfico entrante para cada uno de los servicios de acceso público que brinda la institución | Infraestructura | Dirección de TI |
| IPS A | Equipo en clúster con IPS B, brinda un filtrado de paquetes el cual proporciona mayor seguridad ante ataques remotos sobre diferentes tipos de protocolos usando diversos métodos de análisis | Infraestructura | Dirección de TI |
| IPS B | Equipo en clúster con IPS B, brinda un filtrado de paquetes el cual proporciona mayor seguridad ante ataques remotos sobre diferentes tipos de protocolos usando diversos métodos de análisis | Infraestructura | Dirección de TI |
| WAF A | Firewall de aplicaciones web en clúster con WAF B, éste realiza un análisis sobre el tráfico web con el fin de evitar conexiones maliciosas o respuestas con datos sensibles, una vez que el waf detecta un ataque bloquea este tráfico | Infraestructura | Dirección de TI |
| WAF B | Firewall de aplicaciones web en clúster con WAF A, este realiza un análisis sobre el tráfico web con el fin de evitar conexiones maliciosas o respuestas con datos sensibles, una vez que el waf detecta un ataque bloquea este tráfico | Infraestructura | Dirección de TI |
| Nexus 7K A | Switch de capa 3 en el cual se interconectan, todos los firewalls de: navegación, socios, servicios y base de datos, además de todo el tráfico de la red | Infraestructura | Dirección de TI |
| Nexus 7K B | Switch de capa 3 en el cual se interconectan, todos los firewalls de: navegación, socios, servicios y base de datos, además de todo el tráfico de la red | Infraestructura | Dirección de TI |
| Switch perimetrales A | Equipos de interconexión de proveedores de telecomunicaciones | Infraestructura | Dirección de TI |
| Switch perimetrales B | Equipos de interconexión de proveedores de telecomunicaciones | Infraestructura | Dirección de TI |
| F.O. A - SP 1 | Fibra Oscura que interconecta los centros de datos, sumamente importante para mantener la alta disponibilidad entre equipos internos en clúster | Infraestructura | GreenNet |
| F.O. B - SP 2 | Fibra Oscura que interconecta los centros de datos, sumamente importante para mantener la alta disponibilidad entre equipos internos en clúster | Infraestructura | GreenNet |
| Switch acceso A | Switch de 48 puertos en spanning tree con los switches B y C | Infraestructura | Dirección de TI |
| Switch acceso B | Switch de 48 puertos en spanning tree con los switches A y C | Infraestructura | Dirección de TI |
| Switch acceso C | Switch de 48 puertos en spanning tree con los switches A y B | Infraestructura | Dirección de TI |
| PC Gerente General | equipo de cómputo destinado al gerente | Cómputo | Dirección de TI |
| PC 1 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 2 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 3 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 4 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 5 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 6 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 7 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 8 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 9 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 10 desarrollo | Equipo de cómputo destinado al desarrollo | Cómputo | Dirección de TI |
| PC 1 finanzas | Equipo de cómputo destinado a finanzas | Cómputo | Dirección de TI |
| PC 1 diseño | Equipo de cómputo destinado a diseño | Cómputo | Dirección de TI |
| PC 2 diseño | Equipo de cómputo destinado a diseño | Cómputo | Dirección de TI |
| PC 3 diseño | Equipo de cómputo destinado a diseño | Cómputo | Dirección de TI |
| PC 1 marketing | Equipo de cómputo destinado a marketing | Cómputo | Dirección de TI |
| PC 1 finanzas | Equipo de cómputo destinado a finanzas | Cómputo | Dirección de TI |
| PC 1 RRHH | Equipo de cómputo destinado a RRHH | Cómputo | Dirección de TI |
| PC 1 administración | Equipo de cómputo destinado a tareas administrativas | Cómputo | Dirección de TI |
| PC 1 Infraestructura y operaciones tecnológicas | Equipo de cómputo para personal de IT | Cómputo | Dirección de TI |
| PC 2 Infraestructura y operaciones tecnológicas | Equipo de cómputo para personal de IT | Cómputo | Dirección de TI |
| Servidores Atenas | Servidor controlador de dominio para toda la organización | Infraestructura | Dirección de TI |
| Servidor París | Servidor Windows IIS para publicación de sitios web | Infraestructura | Dirección de TI |
| Servidor Londres | Servidor Windows IIS para publicación de sitios web | Infraestructura | Dirección de TI |
| Servidor Praga | Servidor de base de datos para almacenamiento de información en producción | Infraestructura | Dirección de TI |
| Servidor Berlín | Servidor de base de datos para almacenamiento de información de la organización | Infraestructura | Dirección de TI |

**5. EVALUACIÓN DEL RIESGO**

**5.1 POLÍTICAS DE GESTIÓN DE RIESGOS**

La organización ha decidido implementar una política que permita reconocer de forma sistemática los eventos internos o externos a ella que pueden representar riesgos para el logro de los objetivos del negocio.

Lo anterior requiere la implementación de herramientas para evaluarlos de manera consistente, determinar sus consecuencias y poder desarrollar acciones de mitigación que permitan mantenerlos en un nivel aceptable.

Es política de la organización:

* Establecer y poner en práctica una metodología para la gestión de riesgos
* Definir y establecer el nivel aceptable de los riesgos
* Realizar evaluaciones periódicas de los procedimientos
* Mantener informado a los involucrados sobre el estadio y los riesgos de la organización

**PRINCIPIOS**

Los riesgos en la organización surgen tanto de la amenaza de que algo no deseado ocurra, como de que algo bueno no ocurra. La organización debe de estar preparada y eliminar todos los riesgos posibles, debe de ser adecuadamente administrado y gestionado, siendo por ello es necesario analizar y considerar la existencia de condiciones, situaciones o eventos que pueden desencadenarse y resultar en consecuencias negativas para la organización.

La organización debe contar con políticas de riesgo y con un sistema de gestión y control integral de ellos. Para estos efectos, deben establecer los objetivos estratégicos de negocios, el análisis de alto nivel de los riesgos estratégicos que pueden afectarlos y la asignación de recursos para una adecuada ejecución de las acciones de mitigación según la naturaleza, complejidad, volumen de negocios, las operaciones y las actividades de la organización.

La alta gerencia tiene la responsabilidad de aplicar políticas necesarias para una adecuada gestión de riesgos.

**ESTABLECIMIENTO DE OBJETIVOS**

* Integrar la gestión de riesgos en el proceso de planificación de la organización

**IDENTIFICACIÓN, EVALUACIÓN, RESPUESTA Y ACTIVIDADES DEL CONTROL DE RIESGOS**

* Identificar, evaluar, generar respuestas y actividades de control de los riesgos a nivel de entidad, sistemas, centros de operaciones y procesos.
* Mitigar los riesgos relacionados con las operaciones de la organización hasta el nivel más bajo prácticamente posible o que se pueda alcanzar.
* Asegurar que las actividades de control estén incorporadas en todos los procesos de la organización, orientadas a la eficacia y efectividad en el desarrollo de sus actividades, y de una seguridad confiabilidad de la información.

**SUPERVISIÓN**

* Implementar los mecanismos apropiados para la adecuada operatividad del Proceso de Gestión Integral de Riesgos.
* Supervisar en forma permanente y oportuna las actividades de gestión de riesgos para determinar su vigencia, consistencia, calidad, así como efectuar las modificaciones pertinentes

**6. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS**

Se debe llevar a cabo de manera sistemática, iterativa y colaborativa basándose en el conocimiento y los puntos de vista de las partes interesadas las cuales están divididas en tres partes: Identificación de Riesgos, Análisis de Riesgos y Valoración de Riesgos.

**6.1 IDENTIFICACIÓN DE RIESGOS**

* Evaluar todas las situaciones que puedan poner en riesgo el cumplimiento de los objetivos de la organización, se debe tener en cuenta los riesgos de origen tanto internos de la organización como los externos, en esta etapa se requiere identificar las vulnerabilidades, amenazas, consecuencias y factores de riesgo.
* A través de una reunión entre los responsables, la organización deberá tener identificados sus objetivos y lo más importante definir los factores que influyen en los procesos y priorizarlos estos factores en función del impacto que tengan, ya que no todos los factores o acciones tienen el mismo nivel de importancia.
* Se debe identificar las fuentes de incertidumbre y poder predecir sus efectos
* Analizar eventos no deseados sucedido en el pasado y cómo puede relacionarse en el futuro
* Analizar las interacciones y las dependencias
* **Identificación de Amenazas**
* Podemos definir una Amenaza como cualquier evento que explota las vulnerabilidades de un sistema, con el impacto de causar eventos no deseados, que podrían resultar en consecuencias graves para un sistema u organización como ser la pérdida de la información.
* Podemos identificar las amenazas realizando las acciones necesarias:
* Entrada: las entradas de información del historial y sus incidentes pasados, de las observaciones de los responsables y usuarios de los activos, y aún de catálogos externos de amenazas.
* Acción: identificar las amenazas y las posibles fuentes que lo originan.
* Salida: listar las amenazas ya identificadas por el tipo y por la fuente.
* Identificación de las posibles fuentes de las amenazas
  + La amenaza puede afectar de manera negativa y comprometer los activos de las organizaciones por lo cual es muy importante que puedan ser identificadas.
  + El agente de la amenaza es una entidad con potencial para crear una amenaza, explotando o evidenciando las vulnerabilidades de los mecanismos de seguridad de las organizaciones.
  + El ser humano es uno de los principales y más peligrosos agentes de amenaza.
  + Las amenazas pueden ser deliberadas, accidentales o de origen natural y ambiental.
  + Realizar Entrevistas, visitar las áreas donde hay entrada de información, realizar listas de verificación ayudan en las acciones de identificación de amenazas.
* Las amenazas pueden ser que afecten a más de un activo ya sea de forma parcial o total.
* Si se presenta en estos casos, el equipo de analistas debe tener en cuenta que tanto los riesgos y amenazas pueden afectar a los activos de manera diferente,
* Es esencial e importante priorizar siempre el cuidado debido con lo que son las entradas de la información que son los datos y la información que la organización recibe, pues se trata de datos confidenciales de los clientes los cuales son muy sensibles para la organización por lo cual deben ser tratados de la mejor manera.
* **Identificación de Consecuencias**

Para la evaluación de las consecuencias se debe seleccionar entre:

* Las Pérdidas financieras
* Las Pérdidas legales
* Las Pérdidas reputacionales

**6.2 ANÁLISIS DE RIESGOS**

* El objetivo en primer lugar es realizar una valoración de los riesgos para así priorizar y clasificarlos, lo cual sería una fuente de información para la toma de decisiones.
* El análisis de los riesgos dependerá de la información disponible y de su origen
* Las Metodologías a usar serán cualitativas o cuantitativas porque es necesario diseñar escalas para un mejor análisis de riesgos
* Se debe considerar la probabilidad y las consecuencias de los eventos.
* Considerar la eficacia de los controles de seguridad existentes.

Probabilidad: Se define como una posibilidad de que un evento suceda.

|  |  |
| --- | --- |
| VALOR | PROBABILIDAD DE OCURRENCIA |
| **RARO** | Rara Vez o esporádico, puede suceder 1 vez en una década |
| **POCO PROBABLE** | Ocasional, puede suceder 1 vez en al año |
| **POSIBLE** | Posible, puede suceder 1 vez en al mes |
| **MUY PROBABLE** | Frecuente, puede suceder 1 vez a la semana |
| **CASI SEGURO** | Muy Frecuente, puede suceder 1 vez a diario |

Consecuencias: Se define como el resultado de un evento no deseado la cual puede tener un efecto negativo en el cumplimiento de los objetivos del proceso de la gestión del riesgo.

|  |  |
| --- | --- |
| VALOR | PROBABILIDAD DE OCURRENCIA |
| **DESPRECIABLE** | Insignificantes, no afectan a los objetivos |
| **MENORES** | Bajo, puede haber una afectación baja en los objetivos |
| **MODERADAS** | Moderado, puede haber una afectación significativa en los objetivos |
| **MAYORES** | Crítico, puede haber afectación grave a los objetivos |
| **CATASTRÓFICAS** | Catastrófico, puede haber afectación desastrosa a los objetivos |

**ESQUEMA DE PRIORIZACIÓN DE RIESGOS // NIVELES DE RIESGO**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **PROBABILIDAD** | | | | |
|  |  | **RARO** | **POCO PROBABLE** | **POSIBLE** | **MUY PROBABLE** | **CASI SEGURO** |
| **I**  **M**  **P**  **A**  **C**  **T**  **O** | **DESPRECIABLE** | Bajo | Bajo | Bajo | Medio | Medio |
| **MENORES** | Bajo | Bajo | Medio | Medio | Medio |
| **MODERADAS** | Medio | Medio | Medio | Alto | Alto |
| **MAYORES** | Medio | Medio | Alto | Alto | Muy Alto |
| **CATASTRÓFICAS** | Medio | Alto | Alto | Muy Alto | Muy Alto |

**6.3 VALORACIÓN DE LOS RIESGOS**

A continuación, se describe la escala de valoración de los riesgos en la organización, cada uno de ellos fue valorado teniendo en cuenta, el impacto que produciría que se tendría cada uno de ellos en la organización tomando en cuenta el peor de los casos y los controles existentes para cada uno de ellos.

Los riesgos serán aceptables únicamente por los responsables de cada área de la organización, cuando estos sean catalogados de nivel bajo, todos los demás riesgos que sean calificados como: medio, alto o muy alto no serán aceptados y será necesario tratar los mismos ya sea, transfiriendo, reduciendo o evitando el riesgo.

|  |  |  |
| --- | --- | --- |
| **EVALUACIÓN DEL RIESGO - NIVEL DEL RIESGO** | | **OPCIONES DE GESTIÓN DEL RIESGO / EN FUNCIÓN DEL NIVEL DEL RIESGO ADMISIBLE** |
|  | BAJO | \* Asumir el riesgo |
|  | MEDIO | \* Reducir el Riesgo |
|  | ALTO | \* Evitar el Riesgo. |
| \* Compartir o transferir el riesgo |
|  | MUY ALTO O CRÍTICO | \* Reducir el Riesgo |
| \* Evitar el Riesgo. |
| \* Compartir o transferir el riesgo |

|  |  |  |  |
| --- | --- | --- | --- |
| **Amenaza** | **Impacto** | **Probabilidad** | **Riesgo** |
| **Ataque por Ransomware** | Catastrófico | Posible | Alto |
| **Robo de Credenciales** | Mayores | Posible | Alto |
| **Infección por Spyware** | Mayores | Muy Probable | Alto |
| **Pérdida de suministro eléctrico** | Moderado | Posible | Medio |
| **Inyección SQL** | Mayores | Posible | Alto |
| **Malware** | Moderado | Muy Probable | Medio |
| **Ataques DDoS** | Mayores | Posible | Alto |
| **Ataques XSS** | Mayores | Probable | Alto |
| **Intrusos** | Mayores | Posible | Medio |
| **Software obsoleto o sin licencia** | Moderado | Probable | Medio |
| **Acceso a la red por personal no autorizado** | Mayores | Posible | Alto |
| **Catástrofes naturales causadas por terremotos, inundaciones e incendios** | Catastrófico | Poco Probable | Bajo |
| **Fuga y daños a la información por razones humana** | Mayores | Posible | Alto |
| **Fallo en servicios de comunicación** | Menor | Poco probable | Bajo |
| **Perdida de energia electrica comercial** | Mayor | Posible | Alto |
| **Fallo en equipos de red** | Menor | Poco probable | Bajo |
| **Incumplimientos contractuales por parte de los clientes** | Menor | Posible | Bajo |
| **Seguridad física** | Moderado | Poco probable | Bajo |
| **Acceso a sistemas por personal no autorizado** | Mayores | Posible | Alto |

Una vez valorado los riesgos en esta etapa tendremos identificados para alta dirección de la organización de los riesgos y amenazas que atentan sus activos y a la vez sus objetivos, con su respectivo nivel para así fundamentar la toma de decisiones de qué tratar el riego o la amenaza (Reducir el Riesgo, Evitar el Riesgo o Compartir el Riesgo).

**6.4 TRATAMIENTO DE LOS RIESGOS**

En esta etapa se definen los planes a implementarse para el tratamiento de los riesgos que no se cuenten con una catalogación aceptable y asumible para cada responsable, los planes de tratamiento pueden basarse en las siguientes opciones:

* Asumir el riesgo:
* Transferir
* Mitigar
* Eliminar

**6.4.1 ASUMIR EL RIESGO**

Es la aceptación del riesgo como tal, es decir correr el riesgo, para esta opción no se implementaría ningún control. Esta debe ser una decisión de la alta dirección por la cual debe estar 100% fundamentada y registrada. Se recomienda que se cree un registro de los riesgos asumidos, sobre las bases de su aceptación y los responsables de la aprobación de esta opción.

**6.4.2 REDUCIR EL RIESGO**

También lo podemos denominar Modificación o Mitigación del riesgo cuyo propósito es implementar controles para reducir el impacto de los riesgos a un nivel aceptable para la organización. La implementación de los controles de seguridad tiene que realizarse en base al alcance y contexto de los criterios de la organización como ser: requisitos legales o jurídicos, requisitos ambientales, culturales, entre otros.

La función que deberían realizar los controles de seguridad para la protección de los activos es:

* **Corrección:** Actividades que puedan corregir cualquier anormalidad que genere riesgos para la organización.
* **Eliminación:** Actividades que puedan excluir posibles fallos en los sistemas de información o fuentes de vulnerabilidades, reduciendo los riesgos que pudieren existir.
* **Prevención:** Implementación de controles para prevenir los riesgos que pudieran amenazar a la organización
* **Mitigar el Impacto:** Implementar controles que reduzcan el daño cuando se produzca algún tipo de incidente no deseado.
* **Detección:** Controles que permiten detectar cualquier fuente de amenaza, vulnerabilidades o cualquier tipo de anomalía que se considere riesgo para la organización.
* **Recuperación:** Actividad que permita volver a la situación normal
* **Monitoreo:** Actividad que permita observar y acompañar los procesos del tratamiento de los riesgos, amenazas y vulnerabilidades.
* **Conciencia:** Actividades de enseñanza de comunicación y concientización a todos los empleados de la organización sobre la seguridad de la información, y por las cuales los usuarios sepan aplicar dichos conocimientos de forma eficaz en sus rutinas diarias.

**6.4.3 EVITAR EL RIESGO**

En esta acción se decide evitar el riesgo mediante la eliminación de la fuente o actividad que lo genere, el equipo de análisis al estudiar de que el nivel de riesgo es muy alto y la implementación de los controles de seguridad es muy caro puede acceder a evitar el riesgo.

**6.4.4 COMPARTIR O EXTERNALIZAR EL RIESGO**

Es compartir o transferir el riesgo con una entidad externa. Por ejemplo, los seguros o el uso de servicio de socios.

Estas opciones fueron definidas por el equipo de analistas al momento de valorar los riesgos tomando en cuenta la información que se recopiló en el proceso de Identificación de riesgos y el análisis de los mismo.

teniendo claro el esquema y clasificación de los riesgos el equipo de analistas definió el plan de tratamiento necesario para cada riesgo contando con el respaldo de la alta gerencia, el cual se comparte a continuación

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Amenaza** | **Riesgo** | **Plan de respuesta** | **Acción** | **Responsable** | **Fecha de cumplimiento** | **Costo** |
| **Ataque por Ransomware** | Alto | Eliminar | Implementación de políticas en firewall de navegación el cual utilice inspección de paquetes por UTM, además de antivirus locales en cada PC | Gerencia de TI | Tercer trimestre del 2021 | $3.450,00 |
| **Robo de Credenciales** | Alto | Reducir | Creación de política de contraseñas que involucre a usuarios y el preset de los equipos de plataformas | Gerencia de TI | Tercer trimestre del 2021 | 0 |
| **Infección por Spyware** | Alto | Eliminar | Implementación de políticas en firewall de navegación el cual utilice inspección de paquetes por UTM, además de antivirus locales en cada PC | Gerencia de TI | Tercer trimestre del 2021 | $0,00 |
| **Inyección SQL** | Alto |  | Creación de Pipe, métodos o sentencias preparadas para sanitizar las entradas y salidas del Sistema. | Gerencia de desarrollo | Tercer trimestre del 2021 | $0,00 |
| **Ataques DDoS** | Alto | Mitigar | Aplicar políticas de monitoreo y eliminación de eventos en IPS | Gerencia de TI | Tercer trimestre del 2021 | $0,00 |
| **Ataques XSS** | Alto | Mitigar | Optimización de políticas de actualización de software para prevenir Ataques XSS a nivel de usuario y a nivel de desarrollo políticas de programación seguras como implementar framework seguros y desarrollo de aplicaciones web sensitivas | Gerencia de desarrollo y TI | Tercer trimestre del 2021 | 0 |
| **Acceso a la red por personal no autorizado** | Alto | Eliminar | Desactivar los puertos inactivos de los switch de acceso y habilitación de Port Security en los puertos operativos para evitar el intercambio de terminales | Gerencia de TI | Tercer trimestre del 2021 | $0,00 |
| **Fuga y daños a la información por razones humana** | Alto | Mitigar | Creación de política de concientización de la seguridad de la información a usuarios y documentación necesaria para el uso de las herramientas proporcionadas para sus labores | Gerencia administrativa | Tercer trimestre del 2021 | $0,00 |
| **Perdida de energía eléctrica comercial** | Alto | Mitigar | Reemplazo de sistema de UPS y moto generadores | Gerencia administrativa y de IT | Segundo trimestre del 2022 | $25.000,00 |
| **Acceso a sistemas por personal no autorizado** | Alto | Eliminar | Aplicar políticas de filtrado web para evitar la intrusión de usuarios no autorizados y políticas de usuario para resguardar accesos internos | Reemplazo de sistema de UPS y moto generadores | Gerencia administrativa y de IT | $0,00 |
| **Malware** | Medio |  | Implementación de políticas en firewall de navegación el cual utilice inspección de paquetes por UTM, además de antivirus locales en cada PC | Gerencia de TI | Tercer trimestre del 2021 | $0,00 |
| **Software obsoleto o sin licencia** | Medio | Eliminar | Implementación de política de control de activos de informática para conocer las fechas de caducidad y plan de reemplazo o renovación de licencias | Gerencia de TI | Tercer trimestre del 2021 | $0,00 |
| **Catástrofes naturales causadas por terremotos, inundaciones e incendios** | Bajo | Aceptar | Actualmente se cuenta con dos centros de datos para para prevenir este riesgo | Director ejecutivo, Gerencia administrativa y de TI | N/A | $0,00 |
| **Fallo en servicios de comunicación** | Bajo | Aceptar | Se tiene contratados servicios de comunicación en alta redundancia con distintos proveedores para evitar la indisponibilidad del servicio | Gerencia de IT | N/A | $0,00 |
| **Fallo en equipos de red** | Bajo | Aceptar | Se tiene los equipos de comunicación internos en clúster para evitar ese riesgo | Gerencia de IT | N/A | $0,00 |
| **Incumplimientos contractuales por parte de los clientes** | Bajo | Aceptar | Personal a cargo cuenta con sus procedimientos bien definidos para contar con un respaldo legal ante este riesgo | Gerencia Administrativa | N/A | $0,00 |
| **Seguridad física** | Bajo | Aceptar | Se cuenta con la implementación de controles de acceso físicos, dispositivos de acceso funcionales y personal de seguridad que resguarda el control para proporcionar acceso a personal autorizado a la institución | Gerencia Administrativa | N/A | $0,00 |

**6.5 MONITORIZACIÓN LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

La administración de la organización es la responsable del monitoreo. Se debe de realizar el monitoreo continuo de los riesgos de forma periódica. Adicionalmente la organización debe de auditar revisiones anuales para evaluar los riesgos de la seguridad de la información.

Durante las etapas de este proceso, es necesario el monitoreo periódico en las actividades. Es necesario la permanente comunicación con la alta gerencia y demás departamentos de la organización.

Se debe de informar la evolución y estado de los riesgos, así como los procesos que se han utilizado para eliminar o mitigar los riesgos. Además, se debe de archivar para que quede constancia de cómo se fueron eliminando los riesgos y así poder hacer mejores planificaciones continuas.

**CONCLUSIONES**

Toda organización debe tomar en cuenta lo que es la seguridad de la información y estar consciente en proteger sus activos más valiosos como es la información, lo cual debe dotar de confidencialidad, integridad y disponibilidad de sus activos, lo cual garantizara los objetivos de la organización dando prestigio y confiabilidad para sus clientes, para esto la organización debe implementar controles adecuados de acuerdo al nivel de importancia de sus activos y el impacto que pudiese ocasionar un evento no deseado o una vulnerabilidad de algún sistema de información, para ello las organización deben contar con metodologías, políticas, procedimientos para poder contrarrestar las amenazas que día a día aparecen con el pasar del tiempo con el objetivo de identificar y aprovechar las vulnerabilidades para poder burlar los sistemas de seguridad de una organización y tener acceso a sus activos más valiosos ya sea para revelar, alterar o destruir la información u otros fines que tenga el atacante informático.

Es por ello que los sistemas de gestión de riesgos es una de las soluciones para toda organización para estar preparados contra cualquier evento no deseados ya sea vulnerabilidades, amenazas o desastres naturales que ocasionen efectos negativos a los sistemas de información de la organización, la cual permite a las organizaciones enlistar las amenazas, los riesgos y el impacto que puedan ocasionar cualquier evento no deseado mediante un análisis de riesgos y con los datos recopilados se procede a la evaluación y al monitoreo que nos permite reducir los costos y pérdidas cuando se pudiera materializar una amenaza, ya que con una eficaz implementación de un sistema de gestión de riesgos la organización tendría la capacidad de prevenir y detectar los riesgos antes de su aparición, cabe mencionar también que dentro de un sistema de gestión de riesgos se usan las mejores prácticas y estándares y metodologías como lo es OWASP cuyo objetivo es que se construyan plataformas o aplicaciones de manera segura, basándose en el ciclo de desarrollo del software de aplicaciones. La guía OWASP va dirigida para Desarrolladores de Software, Tester de Software y Especialistas de Seguridad.

|  |  |  |  |
| --- | --- | --- | --- |
| **Hoja de control de actividad grupal**  Fermin Javier Durón Sánchez | | | |
|  | Marcar con una **X** lo que proceda | | |
| **Asistencia a reuniones de equipo** | Asistencia a una sesión o ninguna | Asistencia a dos sesiones | Asistencia a tres sesiones  xxx |
| Isaías Gamaliel Rojoc Sac |  |  | X |
| Angel Ramón Paz López |  |  | X |
| Fermín Javier Durón Sánchez |  |  | X |
| **Tareas o entregas a realizadas** | Ninguna o una tarea | Dos tareas | Tres tareas |
| Isaías Gamaliel Rojoc Sac |  |  | X |
| Angel Ramón Paz López |  |  | X |
| Fermín Javier Durón Sánchez |  |  | X |