Especificaciones técnicas del sistema MERO

ESPECIFICACIONES TÉCNICAS DEL SISTEMA MERO

Control de versiones

Versión	Fecha	Elaborado por	Revisado y aprobado por	Descripción de cambios
1.0	10/08/2022	Claudia Muñoz y Carlos Velásquez	Carlos Velásquez	Versión inicial
2.0	12/09/2022	Claudia Muñoz	Carlos Velásquez	Se actualiza sección de ethical hacking y se actualiza diagrama de arquitectura.
3.0	07/03/2023	Claudia Muñoz	Carlos Velásquez	• Se retiran los ANS del documento para pasarlos a los términos de producto. • Se actualiza la sección de certificaciones, para indicar que ya obtuvimos el certificado de ISO27001. • Se agrega subsección de SOC en la sección de Seguridad de la información.

Generalidades del sistema

Introducción

MERO es un *Software as a Service* (SaaS) que permite la gestión de la información de sostenibilidad o ESG (Environmental, social and governance, por sus siglas en inglés) de las compañías. Esta información normalmente se encuentra distribuida a través de las áreas de una organización y carece de procesos de sistematización, lo cual hace su análisis y divulgación un proceso complejo y en la mayoría de los casos manual y sujeto a errores.

Con la implementación de MERO, las compañías tienen la posibilidad de estructurar bien sus procesos de gestión, análisis y divulgación de su información ESG, sin necesidad de realizar grandes inversiones, embarcarse en procesos complejos de desarrollo ni administrar infraestructuras tecnológicas de procesos transversales que no son el *core* de sus negocios.

¿Para qué un Sistema de Información de Sostenibilidad?

- **El panorama más claro para actuar de forma acertada:** Encontrar siempre una vista completa de la compañía para tener mayor certeza al avanzar.
- **Diálogos más constructivos con tus grupos de interés:** Consolidar una visión integral, con diferentes dimensiones que trascienden el lenguaje financiero.
- **Equipos empoderados y con pensamiento estratégico:** Entregar herramientas que reducen la operatividad y facilitar modelos analíticos para transformar los datos en información.
- **El proceso de *disclosure* llevado al siguiente nivel:** Articular y sistematizar la información de las áreas, entregando herramientas que facilitan la divulgación a diferentes iniciativas y estándares globales.

Funcionalidades del sistema

MERO ofrece un set de funcionalidades que son la garantía de estas promesas y permiten a los usuarios obtener valor en su proceso.

Organiza los datos en un solo lugar

Cuestionarios 100% personalizados basados en diferentes estándares e iniciativas

Información con frecuencia mensual, trimestral y anual

Datos históricos con posibilidad de anexos y links como soporte

Almacenamiento seguro y exclusivo en la nube

Gestiona mejor tu información

Posibilidad de integración con sistemas internos y externos

Flujos de información con diferentes roles y permisos

Posibilidad de autenticación por medio del directorio activo corporativo (Azure Active Directory)

Centro de notificaciones para mejor control del proceso

Comparte información y toma decisiones con ella

Centro de exportación y descargas.
*Descargas en formato Excel y word

Tableros analíticos personalizados
*Integración con MS Power BI

Simplifica tu trabajo

Módulo de administrador para controlar el proceso

Traducción automática español-inglés

Módulo de auditor

Módulo de planes de acción para hacer seguimiento a tareas

Clasificación de la información gestionada en MERO

La información gestionada por MERO es considerada confidencial. No obstante, el sistema no está diseñado para gestionar información clasificada como sensible, pues no se permite el manejo de datos personales de los usuarios, diferentes a los requeridos para el proceso de autenticación en el sistema (Contraseña de ingreso). Estos últimos se encuentran almacenados de forma encriptada.

Dicho esto, los niveles de seguridad de la información se han definido siguiendo las buenas prácticas necesarias para su adecuada gestión y posterior divulgación. La información gestionada en MERO puede ser:

- Información de dominio público
- Información generalmente conocida en la industria previamente a que ésta haya sido revelada por la parte.
- Información que haya sido revelada públicamente por un tercero que contaba con el pleno derecho de hacerlo sin infringir un acuerdo de confidencialidad con cualquiera de las partes.
- La información que se compone de datos agregados y resumidos referentes al uso de los productos del cliente que no contiene información desglosada o identificable como proveniente de ningún tercero en particular.
- La información que haya sido o va a ser revelada públicamente por el cliente haciendo uso de las funcionalidades de la plataforma.

Se deja constancia que, debido a la naturaleza de la aplicación o software, cuya funcionalidad puede ser utilizada de manera interna o bien de manera pública, será decisión del cliente establecer los niveles de privacidad para los reportes generados.

Control de accesos (Perfiles y roles de usuarios)

El acceso a MERO está controlado por perfiles y roles. El perfil es el acceso general que tiene el usuario y el rol es el tipo de participación que tiene un(a) usuario(a) dentro de un flujo de información. Los perfiles y roles asignados pueden ser:

- **Parametrizador:** este perfil permite realizar el SetUp de la instancia cliente y normalmente se otorga solo al equipo de MERO asignado al cliente.
- **Administrador de proceso:** este perfil permite administrar la instancia, ver todos los formularios que se encuentren asociados y diligenciar, revisar o aprobar. En este perfil se debe seleccionar entre dos opciones:

- **Administrador general:** tiene todas las acciones disponibles en todos los formularios de un evento.
- **Administrador por subtema:** tiene todas las acciones disponibles solo en los formularios que se le definan al crear el usuario.

- **Usuario general:** este perfil permite al usuario, navegar y actuar en los formularios del sistema según el rol que le sea asignado (diligenciar, revisar o aprobar).
  - **Diligenciador:** Puede ser responsable de un formulario o de apoyo. Es quién ingresa la información por primera vez a un formulario. Cuando la información de un formulario se encuentra totalmente diligenciada, puede enviar el formulario a su revisión.
  - **Revisor**: Puede ser responsable de un formulario o de apoyo. Es quién revisa la información una vez el diligenciador ha enviado un formulario. Tiene la posibilidad de marcar cada pregunta como revisada, si ve que la información está bien, puede corregirla el mismo, o incluso puede devolver el formulario a su diligenciador, si requiere correcciones por parte de este. Cuando la información de un formulario se encuentra totalmente revisada, puede enviar el formulario a su aprobación.
  - **Aprobador:** Puede ser responsable de un formulario o de apoyo. Es quien aprueba la información una vez el revisor ha enviado un formulario. Tiene la posibilidad de marcar cada pregunta como aprobada, si ve que la información está bien, puede corregirla el mismo, o incluso puede devolver el formulario a su revisor, si requiere correcciones por parte de este. Cuando la información de un formulario se encuentra totalmente aprobada, es quien da por terminado el proceso del formulario.

- **Vista:** este perfil permite ver todos los formularios de la instancia sin posibilidad de editarlos o de actuar en ellos.
- **Traductor:** este perfil permite ver formularios aprobados, ejecutar el proceso de traducción automática y ajustar los textos para una mejor comprensión.
- **Auditor:** este perfil permite participar en los formularios según el permiso que se acuerde con el administrador del proceso. Este permiso puede ir desde solo consultar la información aprobada, hasta tener visual total y acción directa para comentar en los formularios durante todos los estados del flujo de información.
- **Consultor:** este perfil permite participar en los formularios según el permiso que se acuerde con el administrador del proceso. Este permiso puede ir desde solo consultar la información aprobada, hasta tener visual total y acción directa para comentar en los formularios durante todos los estados del flujo de información.

Adicionalmente, los tableros de analítica que se publican en MERO se asignan a nivel de usuarios específicos y no de perfiles, para tener un mejor control del acceso a dicha información.

Arquitectura de la solución

Arquitectura

MERO es un *Software as a Service*, desarrollado con arquitectura monolítica, orientada para ser desplegada en máquinas virtuales. Fue diseñado con arquitectura multi instancia, la cual brinda a cada cliente su base de datos exclusiva, evitando que sus datos se mezclen con los de otro cliente y permitiendo un crecimiento vertical según sus propias necesidades.

Las aplicaciones FrontEnd y BackEnd corren sobre IIS y fueron construidas en (.Net 6), y Angular 11.2.14, respectivamente.

Ventajas del sistema multi instancia:

- Los clientes no se ven afectados por lo que sucede en otras instancias de MERO
- La información de los clientes está mucho más segura, completamente separada de otros
- Las funciones avanzadas como integración con otros sistemas pueden soportarse sin problema

Servidores:

El sistema se ejecuta en dos servidores AWS EC2, uno de aplicación y otro de base de datos; con Windows Server 2019 y actualizaciones al día. Un ejemplo de configuración de servidores es:

- Instancias de AppServer: r6a.xlarge (4 vCPU y 32GB de RAM)
- Instancias de DBServer: m6a.xlarge (4 vCPU y 16GB de RAM)

Estos servidores se van escalando a medida que las instancias van necesitando recursos. Se usan servidores de buen tamaño, y al configurar, se asigna a cada instancia un consumo máximo permitido de recursos, por ejemplo, cantidad de RAM y afinidad con ciertas CPUs; de esta manera, una instancia puede tener acceso a buena cantidad de recursos en periodos pico, pero en ningún momento podrá consumirse todos y afectar las otras instancias.

Regiones de la nube AWS:

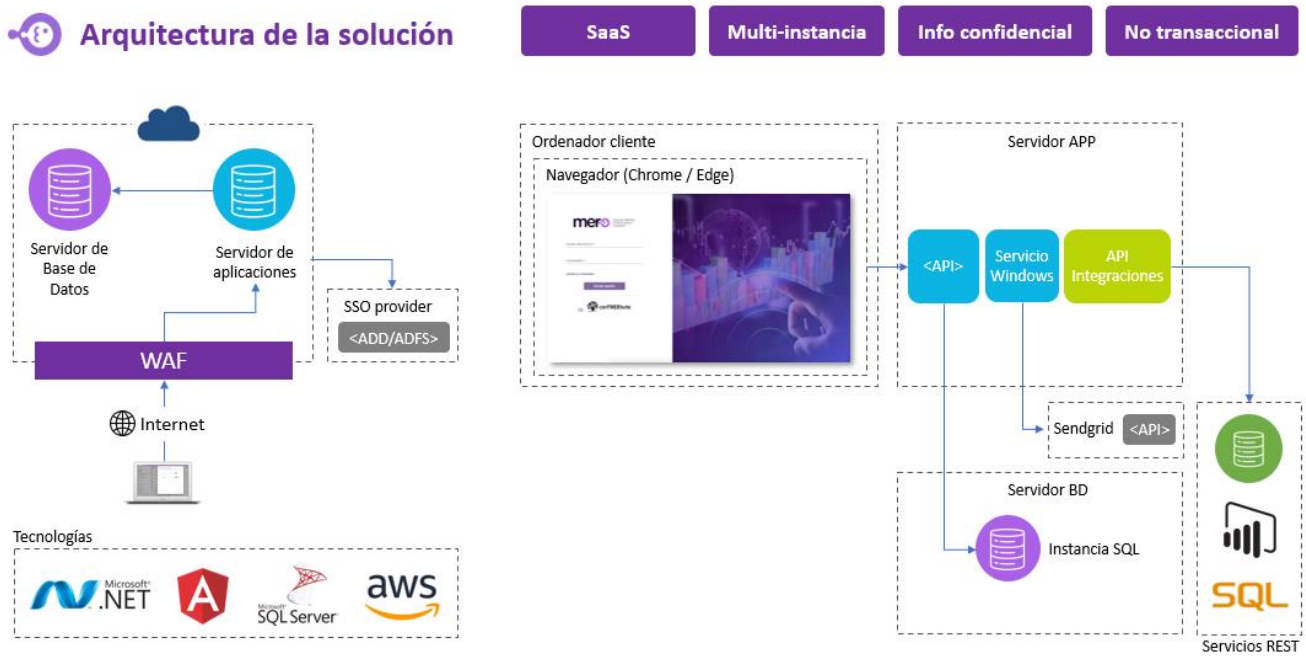
Los servidores de aplicación de MERO se encuentran en la región Ohio (us-east-2) y el servidor FTPS de backups se encuentra en N. Virginia (us-east1). Para mayor detalle ver sección de Backups.

Motor de BD:

Base de datos en SQL Server 2016 con el SP y Cumulative Update más reciente. Para la base de datos se elige SQL server, ya que en años recientes se ha puesto a la par de los grandes de la industria, como son Oracle y DB2, con un excelente desempeño, seguridad superior, características avanzadas, lo suficientemente robusta para realizar las operaciones proyectadas con MERO y gran capacidad de escalabilidad, además de ser natural en el stack de tecnologías con Microsoft .Net

El servidor de DB no tiene puertos expuestos a internet. Se siguen las buenas prácticas recomendadas por AWS para segmentación de redes y enrutamiento según *AWS well architected framework* .

Diagrama de arquitectura



Ambientes

Tenemos los siguientes ambientes para asegurar el adecuado despliegue de las funcionalidades del sistema:

- **Ambiente de desarrollo**:
  Ambiente para trabajar todas las nuevas funcionalidades y realizar las pruebas de integración y unitarios. En este ambiente no se utilizan datos de producción de los clientes.

- **Ambiente de pruebas**:
  Ambiente para realizar el proceso de testing y validar nuevas funcionalidades integradas al sistema. En este ambiente no se utilizan datos de producción de los clientes.

- **Ambiente de pruebas de pruebas de seguridad:**
  Ambiente para realizar el proceso de hacking continuo. En este ambiente no se utilizan datos de producción de los clientes.

- **Ambiente de producción**
  Ambiente de acceso de los usuarios finales. En este ambiente es donde se gestionan los datos reales (de producción) de los clientes.

Control de cambios y versiones del sistema

Una nueva versión se MERO puede darse por la liberación de una nueva o nuevas funcionalidades y/o por la corrección de bugs.

En la etapa de requerimientos se realiza un análisis de impacto para evaluar qué otras funcionalidades se verán afectadas por los cambios o adiciones a realizar, de este modo garantizamos que se cubren los escenarios necesarios tanto para el desarrollo como para las pruebas.

En el ambiente de desarrollo y pruebas se garantiza que la nueva versión funciona perfectamente y se corrigen los bugs en el caso que se encuentren nuevos. Una vez la nueva versión está lista, se eligen de dos a tres clientes que no estén en un punto del proceso crítico, como por ejemplo a días previos para completar el flujo de información de formularios para un proceso de divulgación. Esto se realiza con ayuda de los líderes de proyecto de set up de MERO.

Se realiza el despliegue de la nueva versión en horario no laboral en las instancias seleccionadas. Se lleva un control de versiones donde se indica la versión del sistema, la fecha de liberación, el desarrollador líder, la versión de frontend, backend, WorkerServer y/o API, según los elementos que se vean actualizados en la nueva versión y se indica las funcionalidades y/o bugs que incluye la nueva versión de cara al cliente y separadamente de cara al equipo técnico. Además, se lleva control por instancia de la versión actual, la fecha en que se publicaron las últimas 5 versiones y la persona en que realizó el despliegue. Igualmente, en cada instancia se llevan los backups de los archivos de cada publicación realizada. Se monitorea durante 2 a 5 días en las instancias actualizadas, según el impacto de la nueva versión, cuando se comprueba que la versión funciona según lo esperado y no se presentan bugs, se realiza el despliegue en las demás instancias, en caso contrario se corrigen los bugs presentados y se estabiliza nuevamente la versión antes de publicar en otras instancias.

Protocolo de Internet

MERO usa la cuarta versión del Protocolo de Internet (IPv4). Se tiene estimado una actualización para soportar también el protocolo IPv6 (*dual stack*) a mediados del 2023.

Autenticación y autorización

Gestión de accesos

- La autorización se realiza con base en perfiles y su mapeo a recursos a los que deba tener acceso.
- A excepción del login y la opción de Restablecer contraseña, los métodos de la API requieren autenticación.
- En el logIn y la opción de reestablecer contraseña (en caso de usuarios registrados en el Authentication Provider integrado en MERO), se gestionan los intentos fallidos de autenticación para prevenir ataques que intenten adivinar credenciales de acceso.
- En caso de usuarios registrados en el Authentication Provider integrado en MERO, se valida que la contraseña tenga al menos 8 caracteres, contenga al menos un número, una letra mayúscula y una minúscula.

Integración con AAD (Azure Active Directory)

- La autenticación se realiza con OpenID Connect.
- Puede soportar un proveedor de autenticación de propiedad del cliente y/o un proveedor implementado directamente en MERO.

Ver el detalle: *A1. Manual de configuración SSO V2*

Transporte de datos

- El FrontEnd y el BackEnd están configurados para acceder por canal seguro TLS por defecto.
- El FrontEnd y el BackEnd tiene la funcionalidad de redireccionar a puerto 443 en caso de ser accedidos por puerto 80.

Auditoría y log de errores

Los errores que se producen en el sistema son almacenados en una tabla de Log. Se lleva traza de los cambios que realizan los usuarios en la información, en una tabla de Auditoría. Para los formularios existe una tabla especial que almacena los cambios realizados en los diferentes estados del flujo de información.

La información que se almacena en la tabla de auditoría de MERO es:

- **IdAuditoria:** que es el Identificador único del registro de auditoria
- **IdUsuario:** identifica inequívocamente el usuario que realiza la acción
- **IdRecurso:** donde se realiza la acción
- **IdAuditoriaAccion:** que indica la acción realizada: Crear, Modificar, Eliminar, login
- **Fecha:** fecha y hora en que el usuario realizó la acción
- **IdRegistro1 y IdRegistro2:** son ids de tablas transaccionales que dan más detalle del recurso cuando es necesario, como por ejemplo el idFormularioEvento
- **DescripcionCambios:** donde se indica el valor actual y valor anterior de los campos actualizados. Acá se registran los registros exitosos, los fallidos quedan en tabla de Log.

La información de que se almacena en la tabla de log de errores es:

- **IdLog:** Identificador único del registro
- **IdRecurso:** donde se presentó el error
- **IdUsuario:** que estaba realizando la acción donde se generó el error, el usuario también puede ser el servicio de Windows cuando estaba ejecutando alguna tarea.
- **IdLogAccion** que derivó el error entre: Crear, Modificar, Eliminar, Consultar, Listar, Error general
- **Fecha:** fecha y hora en que se presentó el error
- **Descripcion:** descripción del error
- **MensajeTecnico:** tipo de error
- **Pila:** error técnico detallado
- **InformacionAdicional:** es la traza de la sección de código donde sucedió el error

Estas tablas de log y auditoría no se tienen disponibles para consulta desde la interfaz, pero se puede solicitar información en caso de que se necesite para algún evento específico. La información de ambas tablas se retiene por 6 meses. De requerir información de periodos anteriores se podrá buscar en los *BackUps* de base de datos anteriores.

Integración con sistemas

Integración hacia MERO

En algunos casos, para dar respuesta a cierto número de preguntas, el cliente puede tener actualmente la información en algún sistema, por lo cual Mero ofrece la posibilidad de cargar automáticamente datos, para esto:

- Se provee una API REST, con autenticación Basic.
- Se cargan las respuestas a nivel de pregunta, no de formulario.

Ver el detalle: *A2. Manual integración hacia MERO V1*

Integración desde MERO

MERO cuenta con una ***API REST*** con ***basic authentication*** a través de la cual el cliente puede consumir información almacenada en MERO. Esta API está incluida en las licencias con un alcance general que se compone

de unos ***queries*** específicos que permiten realizar consumos que se puedan necesitar. Los *queries* disponibles son:

- **Query Descriptivas y de selección:** contiene toda la información de los indicadores para las preguntas de tipo descriptivas y de selección con su respuesta. Esta información se entrega filtrada por dimensión y/o evento si tiene más de 300.000 registros
- **Query numéricas anuales e históricas:** contiene toda la información de los indicadores para las preguntas de tipo numéricas anuales e históricas y con su respectiva respuesta. Esta información se entrega filtrada por dimensión y/o evento si tiene más de 300.000 registros
- **Query numéricas mensuales:** contiene toda la información de los indicadores para las preguntas de tipo numéricas mensual y con su respectiva respuesta. Esta información se entrega filtrada por dimensión y/o evento si tiene más de 300.000 registros
- **Usuarios:** contiene la lista de usuarios activos del sistema, con su perfil y correo

Ver detalle: *A3. Manual consumo API desde MERO V1*

Seguridad de la Información

Confidencialidad

Uso general de SSL/TLS.

- El FrontEnd y el BackEnd están configurados para acceder por canal seguro TLS por defecto.
- El FrontEnd y el BackEnd tiene la funcionalidad de redireccionar a puerto 443 en caso de ser accedidos por puerto 80.

Integridad

Se delega en la encriptación de datos en transporte (TLS). Dada la clasificación de la información en MERO y su nivel de seguridad requerido, no es necesario implementar procesos de Hash.

Disponibilidad

Se logra mediante varias estrategias:

- Infraestructura de primera calidad, como son los servicios AWS.
- Procesos estandarizados y optimizados para despliegue de actualizaciones.
- Procesos estandarizados para mantenimiento de plataforma.
- Backups y plan de continuidad de negocio.

Análisis de riesgos

El análisis y control de riesgos de MERO se realiza periódicamente siguiendo las directrices de la norma ISO 27001.

Cifrado de la información

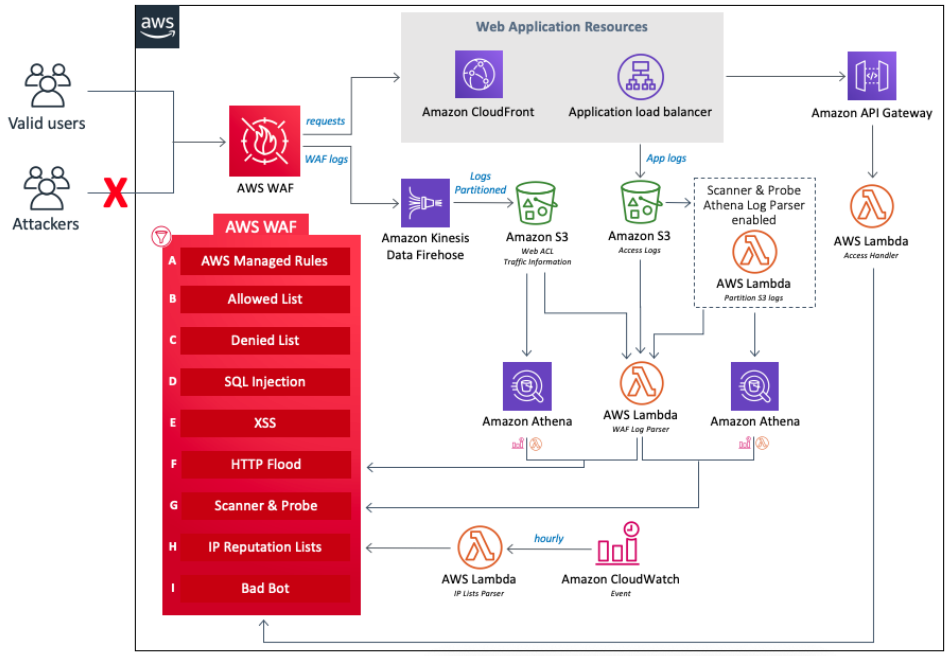
La información sensible que maneja el sistema es la contraseña del usuario. En caso de ser usuarios que no estén integrados con authentication provider (SSO), esta se encuentra cifrada en reposo y transporte. El cifrado de contraseñas se realiza con Advanced Encryption Standard (AES) 192 bits.

El resto de los datos que se gestionan en MERO no están catalogados como información sensible y se requiere que no estén cifrados para su uso en todo el proceso de gestión de información y analítico. Además, la BD no se

encuentra expuesta a internet. Todos los transportes de información se realizan con certificado de seguridad (HTTPS).

Gestión de incidentes de ciberseguridad

Con el AWS WAF protegemos MERO web y todas nuestras API contra ataques web y bots comunes que pueden afectar la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos. AWS WAF brinda control sobre cómo el tráfico llega a MERO, lo que nos permite crear reglas de seguridad que controlan el tráfico de bots bloquean los patrones de ataque comunes, como la inyección de SQL o el scripting entre sitios. También nos permite personalizar las reglas que filtran patrones de tráfico específicos. Para este servicio utilizamos las reglas administradas de AWS WAF, un conjunto preconfigurado de reglas administrado por AWS para abordar problemas como los 10 riesgos de seguridad principales de OWASP y los bots que consumen recursos en exceso, distorsionan las métricas o pueden causar tiempo de inactividad. Estas reglas se actualizan periódicamente a medida que surgen nuevos problemas.



Ethical Hacking

Se realizan pruebas integrales de seguridad (SAST, DAST, SCA, IAS) en modalidad Hacking Continuo.

Para estas pruebas nuestro proveedor **Fluid Attacks** usa herramientas automatizadas para el análisis de vulnerabilidades que están homologadas por el CVE (Common Vulnerabilities and Exposures) y adicional cuenta con capital humano que identifica vectores de ataques que una herramienta automatizada no puede encontrar.

Las vulnerabilidades se priorizan por criticidad, donde las primeras serán las que tengan una criticidad mayor a 7. Para la solución, en caso de ser necesario, se acudirá al equipo Azul (Sofistic), quien apoyará en la forma adecuada para cerrar la vulnerabilidad. Una vez cerrada y publicada la corrección, se pedirá re-ataque al equipo de hacking a través de la respectiva plataforma de gestión del proceso, y si efectivamente se cerró

quedará en estado cerrada, sino se reabrirá nuevamente. Las vulnerabilidades con criticidad menor a 7, entran al Backlog de desarrollo para ser remediadas.

En caso de que el cliente lo requiera, podemos entregar certificado de este servicio indicando el estado de remediación actual.

SOC

Sofistic S.A.S, experta en la prestación de servicios y soluciones de ciberseguridad, nos provee los servicios de SOC (Security Operations Center). El servicio de SOC para la monitorización con soporte de hasta 24x7 de las alertas de CrowdStrike, de Cloudflare Web Application Firewall y los registros de auditoría de la base de datos y el servidor principal. Cuenta con Azure Sentinel como herramienta SIEM cloud, lo que permite una visión más completa de cada uno de los eventos de ciberseguridad que aparezcan, en una única solución que permite una gestión de estos de forma más efectiva y rápida.

En caso de que el cliente lo requiera, podemos entregar certificado de este servicio.

Entrega de información y certificado de borrado

En los casos que aplique se garantizará un borrado de la información, eliminando toda la información entregada por el cliente a través de herramientas o mecanismos de borrado seguro. La información del cliente se entregará en un formato que será acordado entre las partes, al momento de resolverse el contrato o a la terminación del servicio de modo que el cliente pueda almacenarla en sus propios sistemas o usarla en un sistema de un nuevo proveedor.

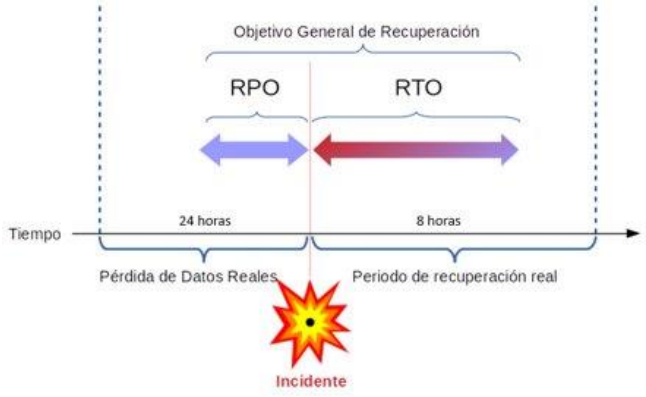
Continuidad del negocio

El proceso de continuidad de negocio de MERO se realiza siguiendo las directrices de la norma ISO 27001.

Plan de recuperación de desastres (RTO, RPO)

Los tiempos que tenemos definidos para MERO ante un desastre son:

Recovery Point Objective (RPO)	Recovery Time Objective (RTO) RTO
24 horas	8 horas
Intervalo de tiempo que puede pasar durante una disrupción antes de que la cantidad de datos perdidos durante ese periodo exceda el límite máximo tolerable.	Duración de tiempo y nivel de servicio dentro de los cuales un proceso de negocio debe ser restaurado después de un desastre para evitar consecuencias inaceptables asociadas con una brecha de continuidad.



Política de Backups

Como esquema de backups principal se usa el servicio AWS Backup para tener imágenes diarias de las máquinas virtuales.
Como segundo nivel, y para poder llevar a cabo la retención de archivos según la política, se tiene otro sistema de backup basado en servidor FTPS (FTP over SSL/TLS) que está en una cuenta diferente de Amazon, y en una región diferente a la de las instancias que respalda. Los archivos se transportan y almacenan comprimidos y encriptados con AES 256 bits. Si la instancia de MERO se encuentra en la región Ohio (us-east-2), el servidor FTPS de backups estará en N. Virginia (us-east1) y viceversa.

Backups de base de datos

- Son de copia completa, pues no aplica la opción incremental.
- Se realizan diariamente, en la noche o en la madrugada, según la programación que le corresponda a la instancia, entre 10pm y 4AM.

Backups de archivos de aplicación y ejecutables de aplicación

- Se realizan diariamente, son incrementales, creando una copia completa cada fin de semana.
- Se realizan en la noche o en la madrugada, según la programación que le corresponda a la instancia, entre 10pm y 4AM.
- Se realizan usando instantáneas de volumen, para prevenir posibles errores al intentar respaldar archivos que están siendo usados.

Retención

Base de datos:
Se mantiene una copia diaria de los últimos 60 días, y a partir de ahí, semanal, de los últimos 6 meses y mensual por 1 año.

Archivos de aplicación y ejecutables de aplicación:
Se mantiene una copia diaria de los últimos 60 días (incremental, según se definió anteriormente), y a partir de ahí, mensual, de los últimos 12 meses.

Certificaciones

ISO 27001

El 20 de enero de 2023 Icontec nos otorga el certificado de ISO27001, a continuación, se puede ver el detalle del alcance y las fechas relevantes:

Informes SOC 1, SOC 2 y SOC 3

Los informes de Control de organizaciones y sistemas (SOC) de AWS son informes de análisis independientes de terceros que demuestran de qué manera AWS logra los controles y objetivos clave de conformidad. La finalidad de estos informes es ayudarle a usted y a sus auditores a entender los controles de AWS que se han establecido como soporte a las operaciones y la conformidad.

SOC 1	**SOC 2:** seguridad, disponibilidad y confidencialidad	**SOC 2:** Privacidad	**SOC 3:** seguridad, disponibilidad y confidencialidad
Descripción del entorno de control de AWS y una auditoría externa de los controles y objetivos definidos por AWS	descripción del entorno de control de AWS y una auditoría externa de los controles de AWS que cumplen los principios y criterios de seguridad, disponibilidad y confidencialidad de servicios de confianza de AICPA	Descripción del entorno de control de AWS y una auditoría externa de los controles que cumplen los principios y criterios de privacidad de servicios de confianza de AICPA	Informe que demuestra que AWS ha cumplido los principios y criterios de seguridad, disponibilidad y confidencialidad de servicios de confianza de AICPA
Frecuencia: 6 meses: 1/10-31/3 y 1/4-30/9	**Frecuencia:** 6 meses: 1/10-31/3 y 1/4-30/9	**Frecuencia:** Momento (según la fecha del informe)	**Frecuencia:** 6 meses: 1/10-31/3 y 1/4-30/9

A continuación, se presentan los informes SOC 1, SOC 2 y SOC 3 para el periodo del 1ero de abril al 30 de septiembre del año 2021.

SOC 1: *A5. Service_Organization_Controls_(SOC)_1_Report_Current.pdf*
SOC 2: *A6. Service_Organization_Controls_(SOC)_2_Report_Current.pdf*
SOC 3: *A7. Service_Organization_Controls_(SOC)_3_Report_Current.pdf*

Contactos y horarios de atención

La atención a soporte y mantenimiento se prestará en de lunes a viernes de 8:00 am a 12:00 y de 2:00 pm a 6:00 pm, exceptuando días festivos en Colombia y con posibilidad de horarios reducidos durante los periodos de vacaciones. Si se requiere disponibilidad por fuera de este horario deberá acordarse entre las partes.

Las respuestas a las solicitudes se proporcionan solo durante el horario hábil. Intentaremos responder a las solicitudes dentro de un día hábil; en la práctica, nuestras respuestas son generalmente aún más rápidas.

No prometemos ni garantizamos ningún tiempo de respuesta específico. Podemos limitar o denegar su acceso al soporte si determinamos, a nuestra discreción razonable, que está actuando, o ha actuado, de una manera que resulta o ha resultado en un mal uso del soporte o abuso de los representantes de MERO.