Adecuación de un modelo de madurez de ciberseguridad

Manual de Usuario

Versión: 1.0

Fecha: 28/09/2020

1 SISTEMA

Esta solución permitirá a las empresas principalmente evaluar el nivel actual que se encuentran y puedan determinar que mejoras deben implementar para poder aumentar sus niveles de seguridad.

Como alternativa se determinó realizar una aplicación web, que sea de fácil operación y pueda reflejar los avances dentro de su implementación, logrando visualizar los puntos débiles y capacidades dentro de su organización.

1.1 Objetivo

Presente documento tiene como objetivo establecer una guía descriptiva y práctica del uso de la aplicación web, entregando una ayuda al usuario para que pueda acceder y operar sin problemas.

Como también, lograr entender la metodología que se usará para medir el nivel de ciberseguridad dentro de la organización, detallando el modelo a implementar y los controles que se adecuaron para la aplicación.

1.2 Alcance

Lograr que el usuario entienda e interactúe de forma eficaz con la aplicación.

1.3 Funcionalidad

Este proyecto presenta su mayor funcionalidad a través de la interacción con el usuario, ya que es este el que a través de diferentes módulos podrá ir configurando un perfil personal respecto a la ciberseguridad de la empresa donde se desempeña.

1.4 Requisitos del Sistema

- Conexión a internet
- Navegador de internet recomendado (Chrome, Microsoft Edge, Mozilla)

2 Conceptos y metodología

2.1 Modelos de madurez

Un modelo de madurez se caracteriza por otorgar indicadores o patrones que permiten medir la progresión dentro de una disciplina en particular.

El contenido del modelo típicamente ejemplifica las mejores prácticas y puede incorporar normas u otros códigos de práctica de la disciplina.

Por lo tanto, un modelo proporciona un punto de referencia con el que una organización puede evaluar el nivel actual de capacidad de sus prácticas, procesos y métodos, estableciendo objetivos y prioridades para la mejora.

Para esta aplicación el modelo de madurez de referencia será el establecido por **NIST Framework**, el cual ayuda a las empresas de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos.

NIST Framework le brinda a su empresa una reseña de las mejores prácticas para ayudarlos a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad.

2.2 Funciones

El framework está organizado en cinco funciones principales, donde cada función es esencial para una postura de seguridad operativa y una gestión exitosa del riesgo de ciberseguridad.

- **Identifición**
- **Protección**
- **Detección**
- **Respuesta**
- **Recuperación**

2.2.1 Identificación

Haga una lista de todos los equipos, programas software y datos que use, incluyendo computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.

2.2.2 Protección

- Controle quiénes acceden a su red y usan sus computadoras y otros dispositivos.
- Use programas de seguridad para proteger los datos.
- Codifique los datos delicados, tanto cuando estén almacenados o en tránsito.
- Haga copias de seguridad de los datos con regularidad.
- Actualice los programas de seguridad con regularidad, en lo posible, automatice estas actualizaciones.
- Implemente políticas formales para la eliminación segura de archivos electrónicos y dispositivos en desuso.
- Capacite sobre ciberseguridad a todas las personas que usen sus computadoras, dispositivos y redes. Usted puede ayudar a los empleados a comprender su riesgo personal además de la función crucial que cumplen en el lugar de trabajo.

2.2.3 Detección

- Monitoree sus computadores para controlar si detecta acceso de personal no autorizado a sus computadores, dispositivos (soportes de almacenamiento de datos de tipo USB) y software.
- Revise su red para controlar si detecta usuarios o conexiones no autorizados.
- Investigue cualquier actividad inusual en su red o por parte de su personal.

2.2.4 Respuesta

Implemente un plan para:

- Notificar a los clientes, empleados y otros cuyos datos pudieran estar en riesgo.
- Mantener en funcionamiento las operaciones del negocio.
- Reportar el ataque a los encargados del cumplimiento de la ley y otras autoridades.
- Investigar y contener un ataque.
- Actualizar su política y plan de ciberseguridad con las lecciones aprendidas.
- Prepararse para eventos inadvertidos (como emergencias climáticas) que puedan poner en riesgo los datos.

2.2.5 Recuperación

Después de un ataque:

- Repare y restaure los equipos y las partes de su red que resultaron afectados.
- Mantenga informados a sus empleados y clientes de sus actividades de respuesta y recuperación.

2.3 Niveles de implementación

Los niveles de NIST representan qué tan bien una organización ve el riesgo de ciberseguridad y los procesos implementados para mitigar los riesgos. Esto ayuda a proporcionar a las organizaciones un punto de referencia sobre cómo funcionan sus operaciones actuales.

- **Nivel 1 – (Parcial):** El riesgo de ciberseguridad organizacional no está formalizado ni gestionado de manera ad hoc y a veces reactiva. También existe una conciencia limitada sobre la gestión de riesgos de ciberseguridad.
- **Nivel 2 – (Riesgo informado):** Puede que no exista una política para toda la organización para la gestión de riesgos de seguridad. La gerencia maneja la gestión de riesgos de ciberseguridad basándose en los riesgos a medida que ocurren.
- **Nivel 3 – (Repetible):** Un proceso formal de gestión de riesgos organizativos va seguido de una política de seguridad definida.
- **Nivel 4 – (Adaptable):** Una organización en esta etapa adaptará sus políticas de ciberseguridad en función de las lecciones aprendidas y basadas en análisis para proporcionar conocimientos y mejores prácticas. La organización está aprendiendo constantemente de los eventos de seguridad que ocurren en la organización y compartirá esa información con una red más grande.

2.4 Implementación de niveles

Dentro de la propuesta, se adaptará el NIST Framework a un escenario fácil de implementar, donde se utilizará parte de este modelo de madurez, principalmente aquella definición asociada a los niveles de madurez logrados y fijados por las organizaciones, complementados además con la herramienta de los ***20 controles críticos de la información de CIS***, principalmente porque estos se adaptan de mejor manera a empresas pequeñas y pueden entregar una guía ágil para las empresas en temas de ciberseguridad, siendo estos un recurso referencial que apoya de buena manera a la implementación del modelo NIST.

Para este efecto, se confeccionará un cuestionario donde el usuario podrá evaluar como se encuentran implementados los controles dentro de su organización.

El método para el cálculo del nivel de madurez generado por la organización dentro de la plataforma, estará guiado por funciones porcentuales de acuerdo al avance logrado respecto a las respuestas entregadas.

De acuerdo al punto anterior, los niveles de madurez estarán configurados conforme a los siguientes porcentajes promedios logrados:

- **NIVEL 1: Porcentaje total promedio evaluado entre 0 % y 25 %**
- **NIVEL 2: Porcentaje total promedio evaluado entre 26 % y 50 %**
- **NIVEL 3: Porcentaje total promedio evaluado entre 51 % y 75 %**
- **NIVEL 4: Porcentaje total promedio evaluado entre 76 % y 100 %**

2.5 Cálculo de progreso dentro de cada control

El método para el cálculo del avance generado por la organización dentro de la plataforma a través de los controles, estará guiado por funciones porcentuales de acuerdo al avance logrado respecto a las respuestas entregadas.
De acuerdo al punto anterior, los niveles de avance dentro de cada control estarán configurados conforme a los siguientes porcentajes promedios logrados:

- **CRÍTICOS**: Porcentaje total promedio evaluado entre 0 % y 39 %
- **ADVERTENCIA**: Porcentaje total promedio evaluado entre 40 % y 69 %
- **SATISFACTORIO:** Porcentaje total promedio evaluado entre 70 % y 100 %

3 MÓDULOS DEL SISTEMA

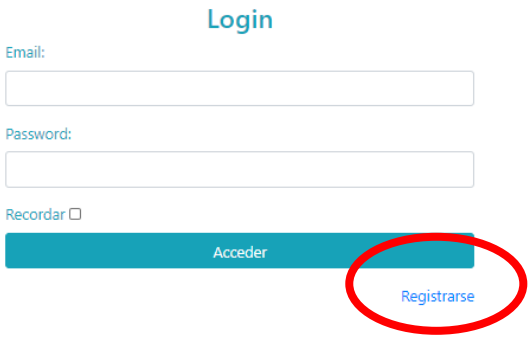
El presente manual está organizado de acuerdo a secuencia de ingreso a las pantallas del sistema de la siguiente manera:

1. Registro de usuario
2. Login de ingreso
3. Interfaz
4. Controles
5. Gráficos controles
6. Gráficos subcontroles
7. Subir evidencia
8. Módulo auditor

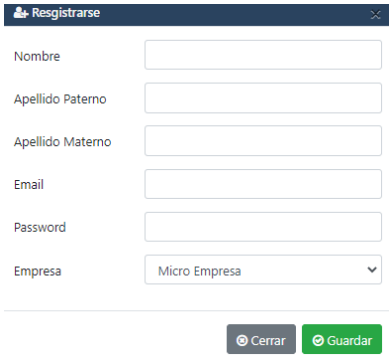
3.1 Módulo de registro de usuario

En esta pantalla se le permite al usuario realizar el registro de los datos, para posterior, ingresar con sus credenciales si problemas a la aplicación.

Para acceder al módulo de registro debe dirigirse al campo “Registrarse”, localizado en la parte inferior derecha.



Al momento de seleccionar el campo “Registrarse”, se desplegará una nueva ventana donde el usuario completará su información personal



Los campos desplegados se detallan a continuación:

- Nombre : Nombre de usuario a registrar
- Apellido Paterno : Apellido paterno de usuario a registrar
- Apellido Materno : Apellido materno de usuario a registrar
- Email : Cuenta de correo electrónico de usuario a registrar (de preferencia uso personal)
- Password : Clave personal de usuario a registrar

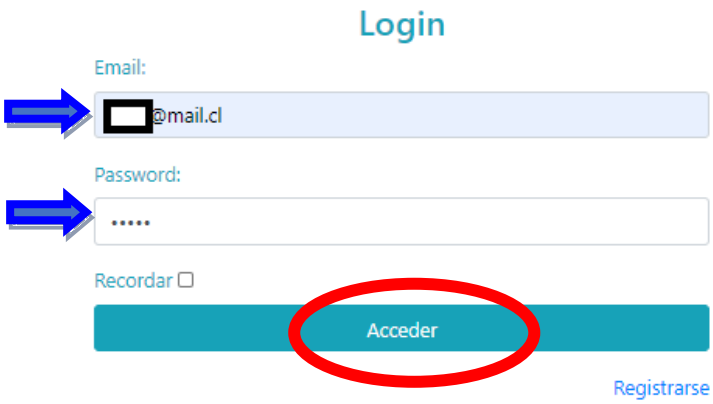
La ventana contiene siguientes botones de acciones:

- Botón cerrar : Al accionar se cierra la ventana
- Botón guardar : Al accionar los datos se guardarán en la base de datos

3.2 Módulo de Login de ingreso

En esta pantalla se le permite al usuario ingresar a la aplicación después de haberse registrado.

Para poder ingresar, el usuario debe escribir los datos solicitados y apretar el botón “Acceder”



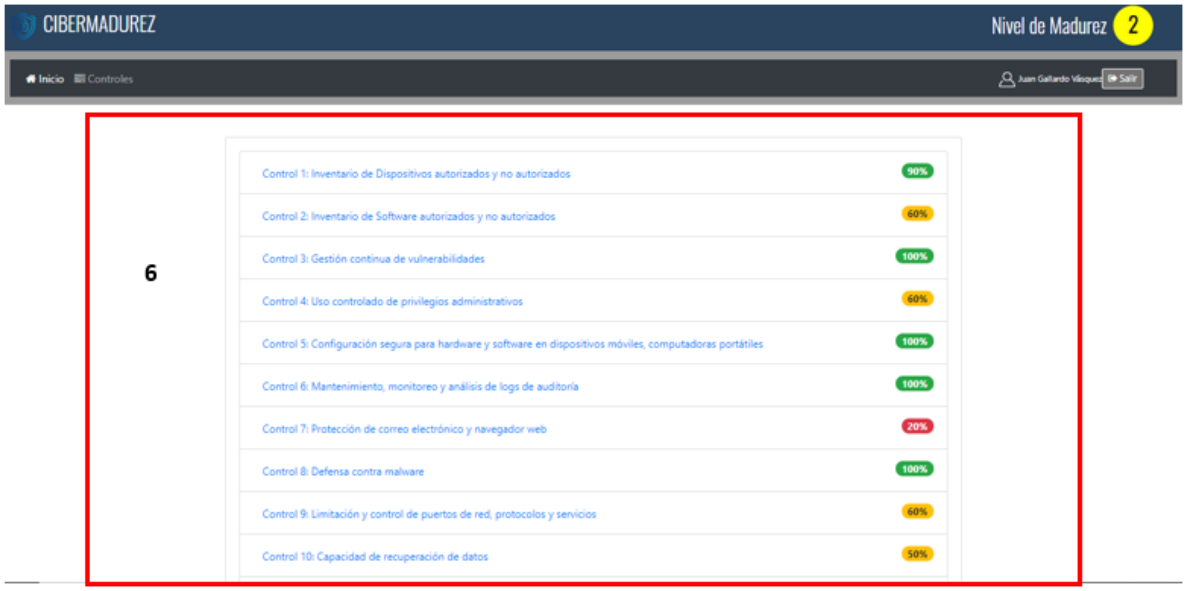
3.3 *Interfaz de la aplicación*

Una vez el usuario ingrese a la aplicación, podrá entrar a visualizar su avance de evolución respecto al cumplimiento de los controles de seguridad logrados.

Dentro de la interfaz, se podrá visualizar diferentes campos, los cuales se detallan a continuación:

Interfaz inicial:

Interfaz de los controles críticos



Dentro de las interfaces podemos señalar los principales campos:

1. Nombre de la aplicación
2. Menú de navegación
3. Nivel de madurez logrado por la organización
4. Nombre de usuario registrado
5. Interfaz de gráficos
6. Interfaz de los controles críticos que la empresa debe evaluar

3.4 Módulo de controles

Esta pantalla presenta los 20 controles críticos de ciberseguridad que la organización debe ir verificando su cumplimiento para ir progresando su nivel de cibermadurez.

Cabe mencionar que los controles críticos de ciberseguridad, son un conjunto de acciones priorizadas, ampliamente analizadas y de efectividad probada que pueden ser tomadas por las organizaciones para mejorar su nivel de ciberseguridad.

Dentro de cada control existen subcontroles, los cuales se adaptan de acuerdo al nivel de la organización, para esta etapa solo se presentan los correspondientes a la "microempresa".

Ejecución del control:

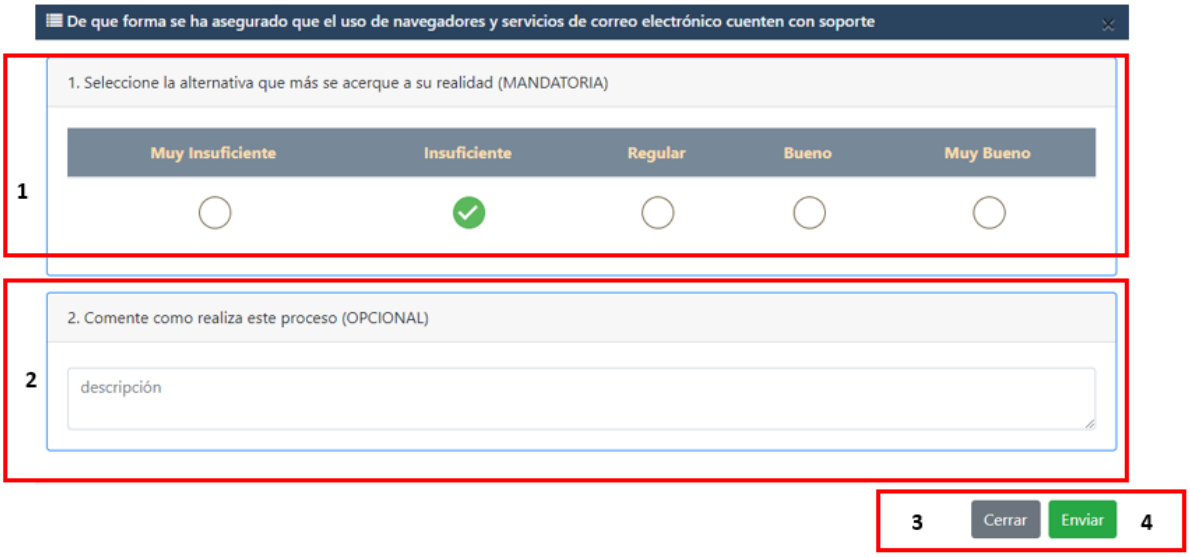
Para esto, el usuario debe seleccionar un control posicionándose sobre el que necesita evaluar, después de seleccionar, se desplegará una ventana donde encontrará los subcontroles que debe cumplir.

Las diferentes interfaces asociadas a este módulo se detallan a continuación:

Dentro de la interfaz de los “controles”, se podrán visualizar diferentes campos, los cuales se detallan a continuación:

1. Campo asociado a los 20 controles a completar
2. Porcentaje logrado después de la evaluación
3. Campo de subcontroles asociados al control respectivo
4. Subcontrol con su respectiva recomendación
5. Campo de evaluación con su respectivo indicador de realizado

Luego de ingresar el control, el usuario debe seleccionar el botón “evaluar”, donde se desplegará una nueva ventana, a través de esta, el usuario deberá completar el campo que más se adecua a su situación (**Muy Insuficiente, Suficiente, Regular, Bueno, Muy Bueno**).



Dentro de la interfaz de la evaluación, se podrá visualizar diferentes campos, los cuales se detallan a continuación:

1. Campo donde el usuario debe seleccionar la alternativa que más se asemeja a su realidad.
2. Campo opcional donde el usuario puede detallar algún comentario de acuerdo al subcontrol.

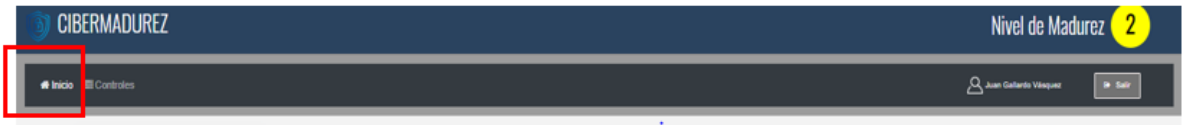
La ventana contiene siguientes botones de acciones:

3. Botón cerrar : Al accionar se cierra la ventana
4. Botón guardar: Al accionar los datos se guardarán en la base de datos

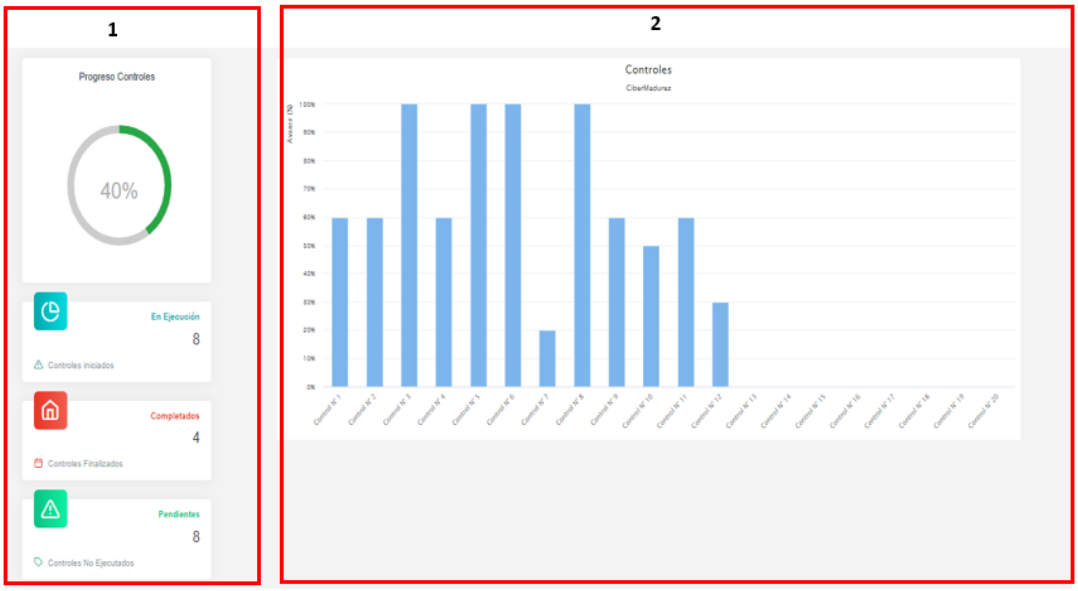
3.5 Módulo de gráficos Controles

El propósito de este módulo es de generar un impacto respecto al nivel actual en ciberseguridad de la organización, el cual le permitirá al usuario identificar los controles que se encuentran con menos cumplimiento y avance facilitando una planificación de sus objetivos y prioridades.

Para acceder a este módulo el usuario debe hacer clic en el botón “inicio” en la barra de navegación.



Vista general de la interfaz:



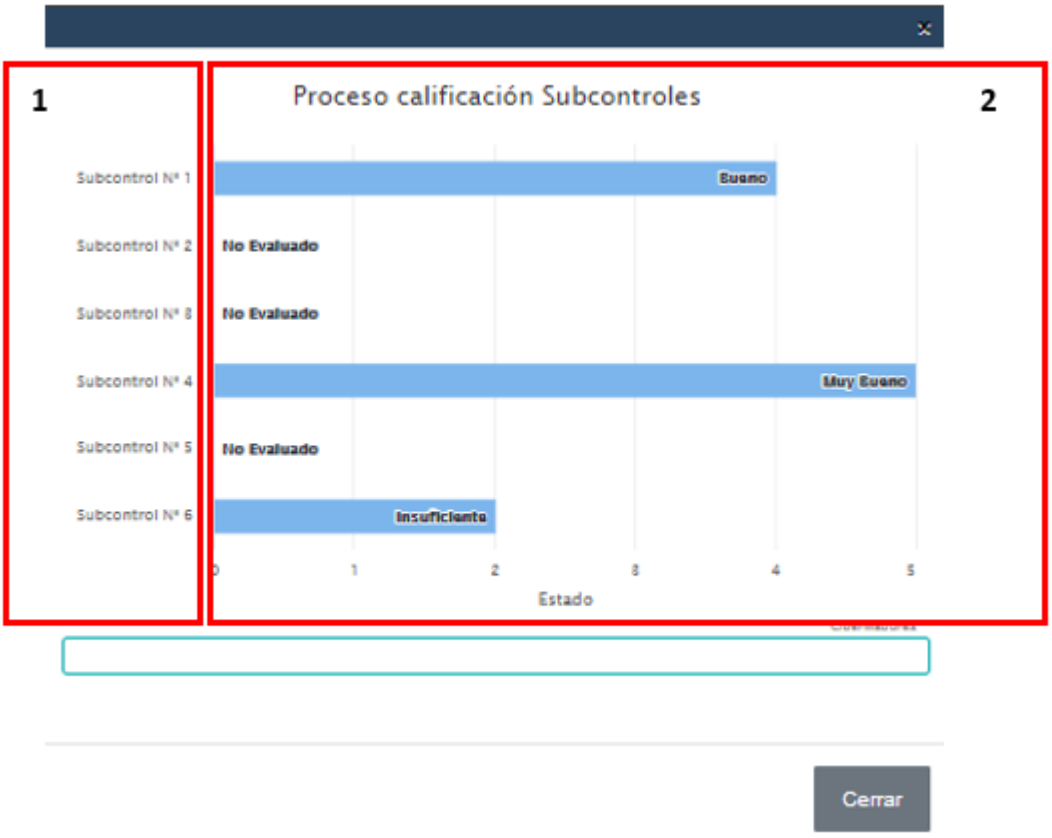
Dentro de la interfaz de gráficos de controles, se podrá visualizar diferentes campos, los cuales se detallan a continuación:

1. Interfaz que permite identificar el avance de los controles identificando cuales se encuentran en proceso, pendientes y completados
2. Interfaz que permite identificar de forma gráfica el avance de los controles.

3.6 Módulo de gráficos Subcontroles

El propósito de este módulo es que el usuario pueda visualizar como han sido evaluados los subcontroles dentro de cada control, de acuerdo al criterio de cumplimiento dentro de su organización.

Para acceder a este módulo el usuario debe hacer clic sobre la gráfica del control y se le desplegará una nueva ventana donde podrá visualizar su cumplimiento dependiendo de la evaluación, en el caso de no estar evaluado el subcontrol, aparecerá una leyenda “No evaluado”.



Dentro de la interfaz de gráficos de los subcontroles, se podrá visualizar diferentes campos, los cuales se detallan a continuación:

1. Interfaz que permite identificar el número del subcontrol.
2. Interfaz que permite identificar de forma gráfica el avance de los subcontroles con su respectiva evaluación.

La ventana contiene siguiente botone de acción:

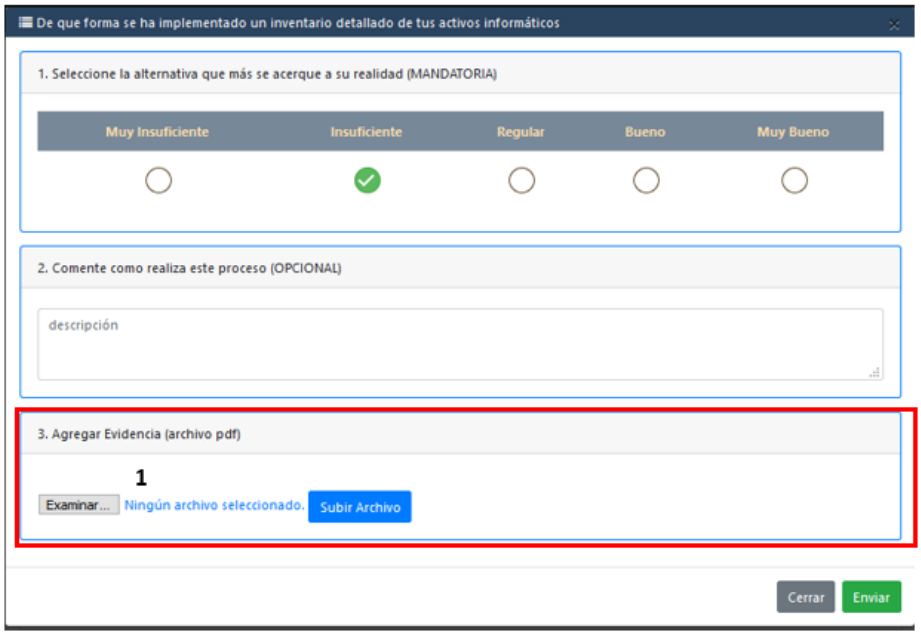
1. Botón cerrar : Al accionar se cierra la ventana

3.7 Módulo de subir evidencia

El propósito de este módulo es que el usuario pueda subir evidencia de como está realizando el trabajo, ya sea alguna instrucción al personal o manejos de sistemas, donde a través de este documento valide su progreso.

Para acceder a este módulo, el usuario debe ingresar a evaluar un subcontrol y dentro de esta ventana acceder al campo "*3. Agregar Evidencia (archivo pdf)*", desde este campo podrá seleccionar un archivo, el cual dentro de las condiciones es que solo sea en **formato PDF.**

IMPORTANTE: En el caso de subir un archivo que no sea PDF, el sistema arrojará un mensaje de advertencia



Dentro de la interfaz de subir evidencia, se podrán visualizar diferentes campos, los cuales se detallan a continuación:

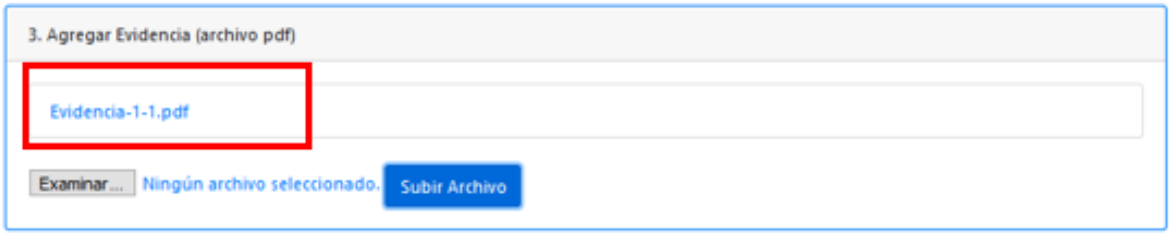
1. Contenedor donde será almacenado el archivo

La ventana contiene siguiente botone de acción:

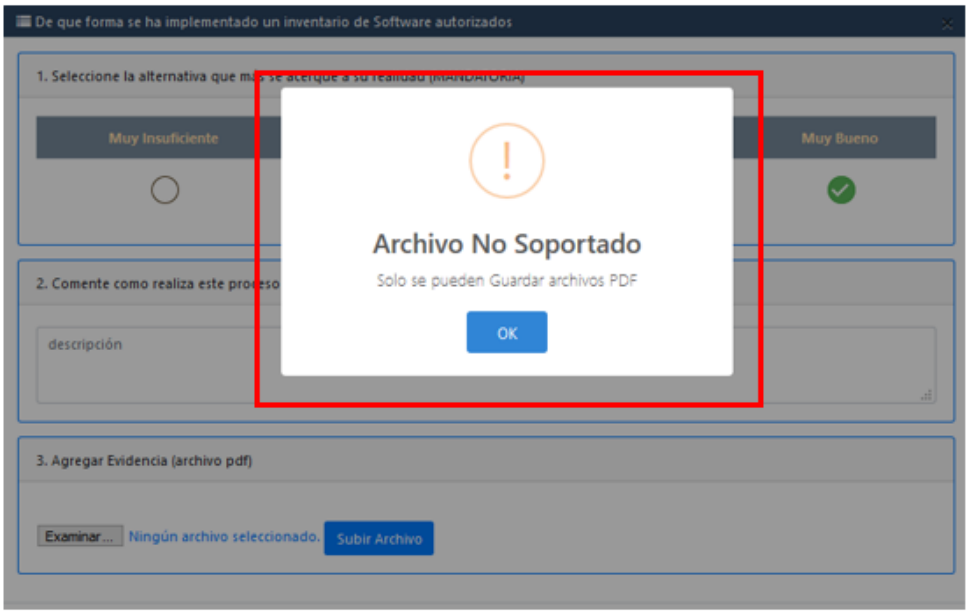
1. Botón examinar : Al accionar permite al usuario seleccionar un archivo PDF.

Botón subir archivo : Al accionar permite subir el archivo al contenedor

Ventana con evidencia alojada en el contedor:



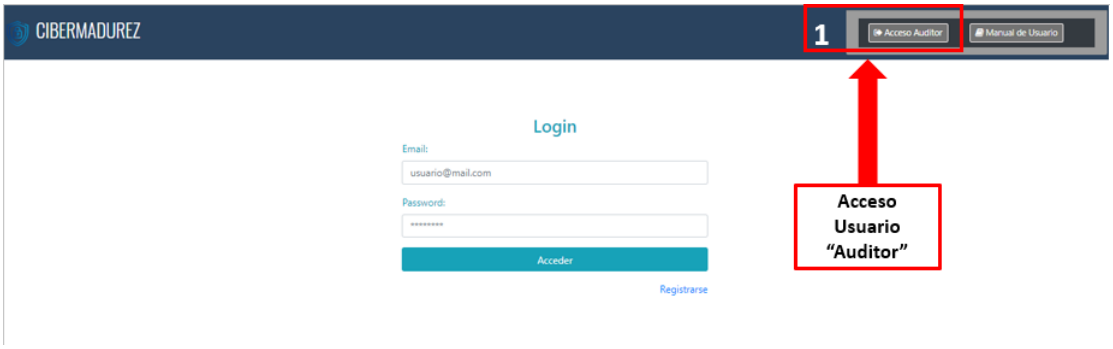
Mensaje de error al subir archivo distinto a PDF:

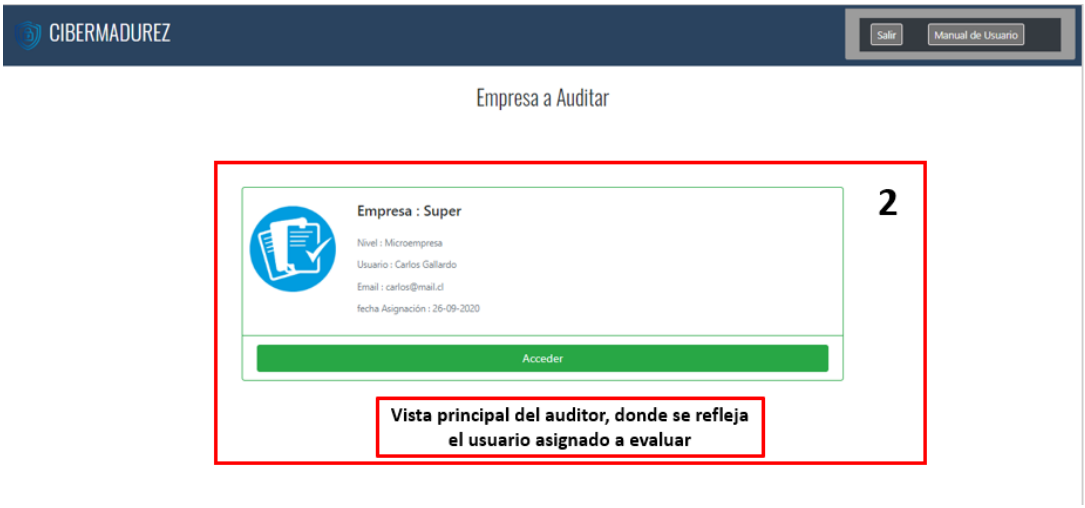


3.8 *Módulo Auditor*

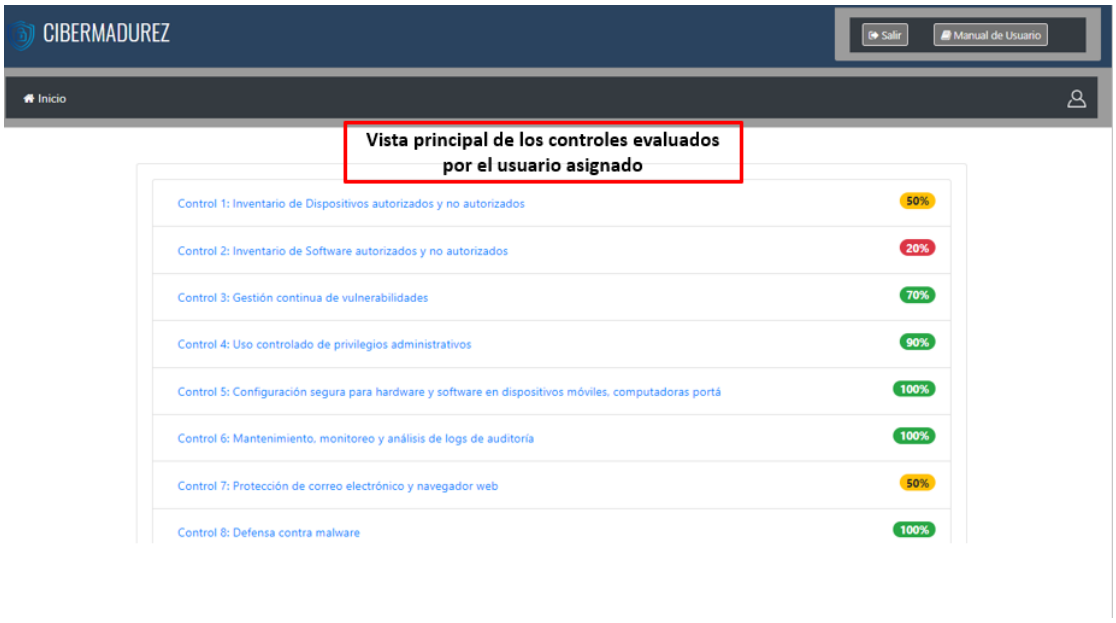
El propósito de este módulo es que el usuario de la categoría de auditor pueda evaluar la evidencia subida por el usuario a la plataforma, donde podrá emitir comentarios sobre el procedimiento a evaluar.

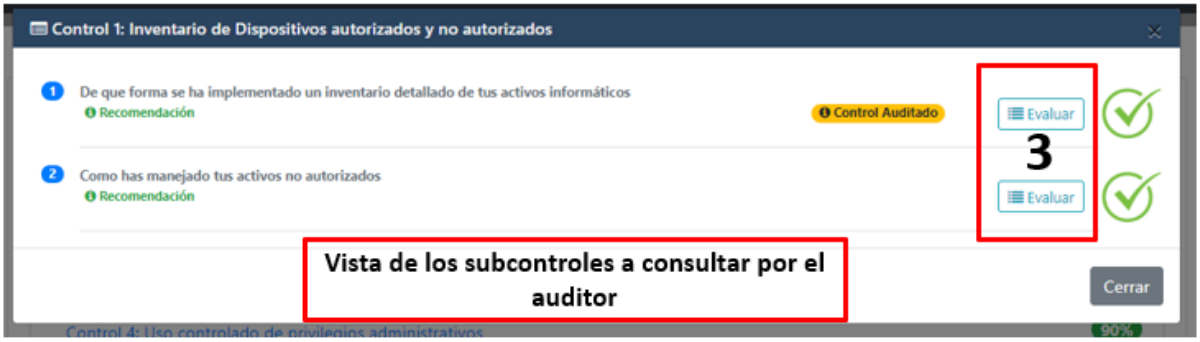
Para acceder a este módulo, el usuario auditor debe ingresar a un módulo de acceso solo para auditores, donde una vez dentro del sistema se le desplegarán unas vistas diferenciadas del usuario.

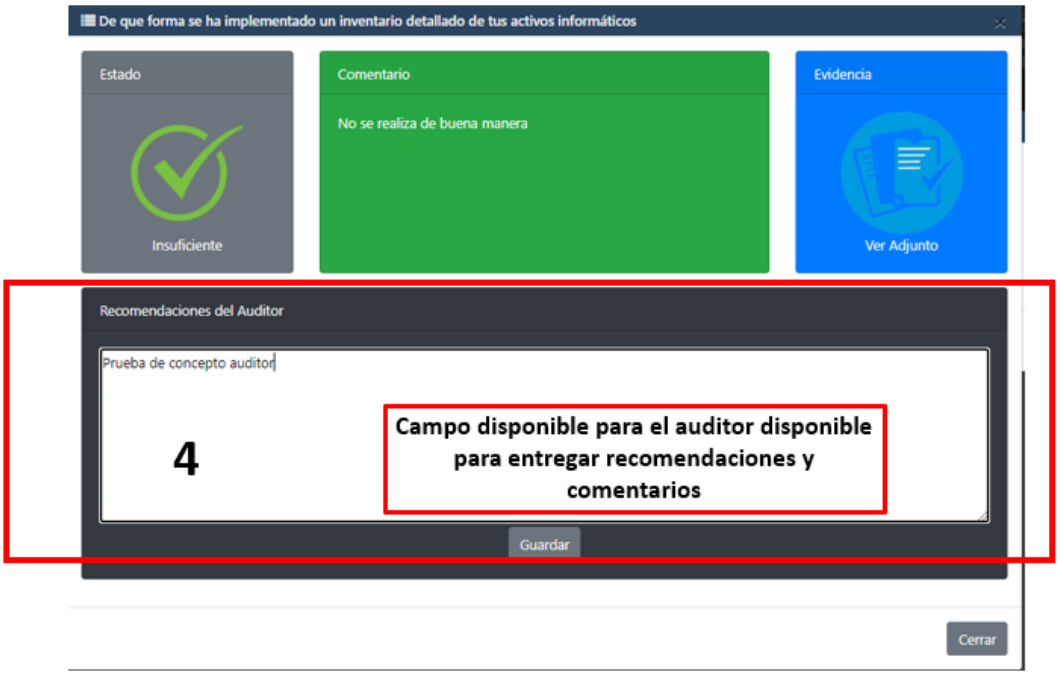


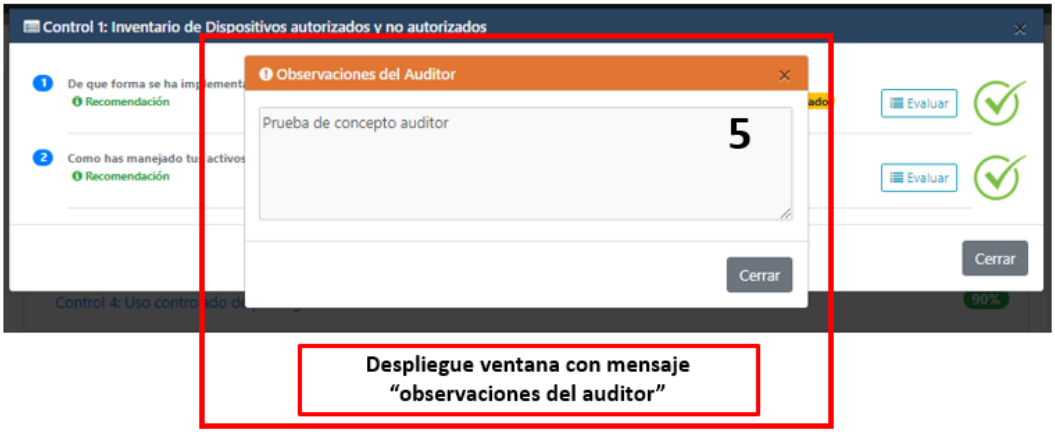


Vista principal de los controles evaluados por el usuario asignado









Dentro de la interfaz de auditor, se podrán visualizar diferentes campos, los cuales se detallan a continuación:

1. Acceso al panel de auditor
2. Vista del auditor con usuario asignado
3. Acceso a evaluar los controles del usuario
4. Vista disponible para el auditor, donde existe campo para entregar recomendaciones
5. Ventana despliegue comentario auditor

4 GLOSARIO

A continuación, se detallan algunos términos asociados a la aplicación:

Término	Descripción
Nivel de madurez	Nivel de madurez en que se encuentra a organización respecto a temas de ciberseguridad, se clasifica de 1 a 4 y se calcula de acuerdo al porcentaje de cumplimiento de los controles
Recomendación	Campo que entrega una recomendación asociada al subcontrol que permite al usuario entender de mejor manera como cumplir lo solicitado
Control	Componente asociado a los 20 controles críticos de ciberseguridad
Subcontrol	Subcontrol dependiente del control, el cual dependerá del nivel de empresa que se evalúa
Auditor	Persona externa que podrá ser parte del proyecto y participará de forma activa en el proceso de evolución de cibermadurez