Proveedor: Grupo Horus S.A.

Orden de Trabajo

Nro. de Orden	5
Horas Hombre	442 horas
Fecha de pedido	02/01/2020
Plazo de entrega al MITIC	06/03/2020

Nombre del Producto
Sistema de Controles Críticos de Ciberseguridad - Versión 1

Objetivo
Sistema de Gestión para la evaluación de controles críticos de Ciberseguridad de las OEE.

Referencias
- Memorándum CyPI-20190830 de fecha 30 de agosto de 2019.
- Controles críticos de Ciberseguridad: https://www.cert.gov.py/index.php/controles-criticos-seguridad
- Guía de Controles Críticos de Ciberseguridad https://www.cert.gov.py/index.php/download_file/view_inline/1375

Requerimientos Funcionales
- **Proyecto base**
  - Adaptación del proyecto y arquitectura backend del Sistema de Administración del Portal Paraguay portalpy-administracion-backend.
  - Adaptación del proyecto y arquitectura frontend del Sistema de Administración del Portal Paraguay portal-py-administracion.
  - Modificaciones estructurales al ABM Usuarios (Datos básicos).
  - Aplicar la política de reseteo de contraseña.
    - Reutilizar mecanismos de creación y reseteo de contraseña del sistema.
    - Cambiar texto "Olvidó su contraseña?" por "Crear/Cambiar contraseña". (en este mecanismo el sistema le envía un mail al usuario con un link al cual dirigirse para crear o registrar su nueva contraseña).
    - Será en la página que llega como link en el email. https://localhost /#/generarClave.
- **Gestión de usuarios, sesiones y privilegios:**
  - El software debe permitir una gestión de usuarios con niveles de privilegios de acuerdo a los roles indicados en la sección de requerimientos funcionales (administrador, operador, visualizador, etc.), basados en el principio de mínima necesidad de conocimiento.

    Aclaración con relación al diseño de solución: Adaptar la estructura y operatoria de administración de roles y permisos del sistema con creación de los roles **definidos en la sección "Roles y Permisos"**.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

GRUPO HORUS
GRUPO HORUS S.A.

- Debe ser posible establecer una fecha de expiración para las cuentas de usuarios, a partir de la cual la cuenta deberá entrar a un estado "desactivado" o similar, hasta tanto se apruebe la continuidad de la misma. El parámetro de fecha de expiración deberá ser configurable por el MITIC (desde el perfil del administrador)

- El software debe contemplar la expiración de sesiones de acuerdo a parámetros temporales. Estos parámetros pueden ser configurables por el MITIC (desde el perfil del administrador).
  - Las configuraciones se encuentra en BD Postgresql. ABM de la tabla configuración para el rol "administrador"

- **Autenticación y gestión de credenciales:**
  - Los nuevos módulos y funcionalidades especificados en esta OT deben tener implementado mecanismos de protección a los servicios disponibilizados por el Backend (REST).

    Aclaración con relación al diseño de solución: El mecanismo de protección deberá utilizar la misma solución ya implementada en el sistema, utilizando los usuarios por roles y permisos.

  - El software debe permitir establecer políticas de contraseña, que incluyan, como mínimo, la posibilidad de establecer los siguientes parámetros:
    - longitud mínima de la contraseña
    - complejidad de contraseña (mayúsculas, minúsculas, números y caracteres especiales.)
    - Estos parámetros deberán ser configurables por parte del administrador del MITIC.
  - Para el almacenamiento de las contraseñas se debe utilizar algoritmos como: bcrypt, Argon2, PBKDF2 ó scrypt.

- **Gestión de registros de auditoría:**
  - El software debe ser capaz de generar registros de auditoría en Base de Datos de todos los eventos relevantes, con los detalles suficientes para permitir una trazabilidad adecuada, que abarque como mínimo los siguientes eventos:
    - inicios de sesión de usuarios (exitosos y fallidos)

      Aclaración con relación al diseño de solución: Implementación de un mecanismo nuevo para registrar auditorías de login reutilizando arquitectura actual.

    - modificación de parámetros del sistema
      Aclaración con relación al diseño de solución: Reutilizar mecanimos de auditoría implementadas en OT3.

    - gestión de usuarios (cambio de contraseña, creación/modificación de usuarios)
      Aclaración con relación al diseño de solución: Reutilizar mecanimos de auditoría implementadas en OT3.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

GRUPO HORUS
GRUPO HORUS S.A.

- acciones críticas llevadas a cabo por usuarios en el marco del proceso de negocio del sistema. Las siguientes acciones deben ser consideradas: modificación de valores de un diagnóstico en curso, inicio de un nuevo diagnóstico, término de un diagnóstico, eliminación de un diagnóstico en curso.

- El sistema debe tener su propio archivo de log e imprimir los eventos auditables utilizando librerías de log de Java.

- **Acciones del Rol "Administrador Ciberseguridad"**
  - Módulo de Controles y valores posibles
    - Datos básicos de las planillas, informes y documentos del CERT-PY.
    - Tipo de Control: Básico, Fundacional, Organizacional
    - Ver: https://www.cert.gov.py/index.php/controles-criticos-seguridad
    - El proceso de ABM se realizará por medio de la importación/exportación de un template Excel. El flujo a utilizar será el siguiente:
      - Usuario **Administrador de Ciberseguridad** exporta una plantilla Excel "template" del sistema.
      - Usuario **Administrador de Ciberseguridad** realiza los cambios/ajustes en la plantilla Excel
      - Usuario **Administrador de Ciberseguridad** Importa la plantilla Excel.
      - A partir de la plantilla importada, el sistema creará una nueva versión de los controles críticos. Durante el proceso de importación, el sistema debe emitir notificaciones de error que indiquen las celdas o campos incorrectos.
    - En el caso de que se genere una nueva versión de los controles, los diagnósticos en procesos que aún no fueron finalizados estarán vinculados a la versión anterior del control.

  - Módulo de Subcontroles y valores posibles
    - Ver: https://www.cert.gov.py/index.php/controles-criticos-seguridad
    - El proceso de ABM se realizará por medio de la importación/exportación de un template Excel. El flujo a utilizar será el siguiente:
      - Usuario **Administrador de Ciberseguridad** exporta una plantilla Excel "template"del sistema.
      - Usuario **Administrador de Ciberseguridad** realiza los cambios/ajustes en la plantilla Excel
      - Usuario **Administrador de Ciberseguridad** Importa la plantilla Excel.
      - A partir de la plantilla importada, el sistema creará una nueva versión de los controles críticos. Durante el proceso de importación, el sistema debe emitir notificaciones de error que indiquen las celdas o campos incorrectos.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

GRUPO HORUS
GRUPO HORUS S.A.

- En el caso de que se genere una nueva versión de los controles, los diagnósticos en procesos que aún no fueron finalizados estarán vinculados a la versión anterior del control.

- Carga completa de los controles, subcontroles y datos asociados segun planilla https://www.cert.gov.py/index.php/download_file/view/1387/1259

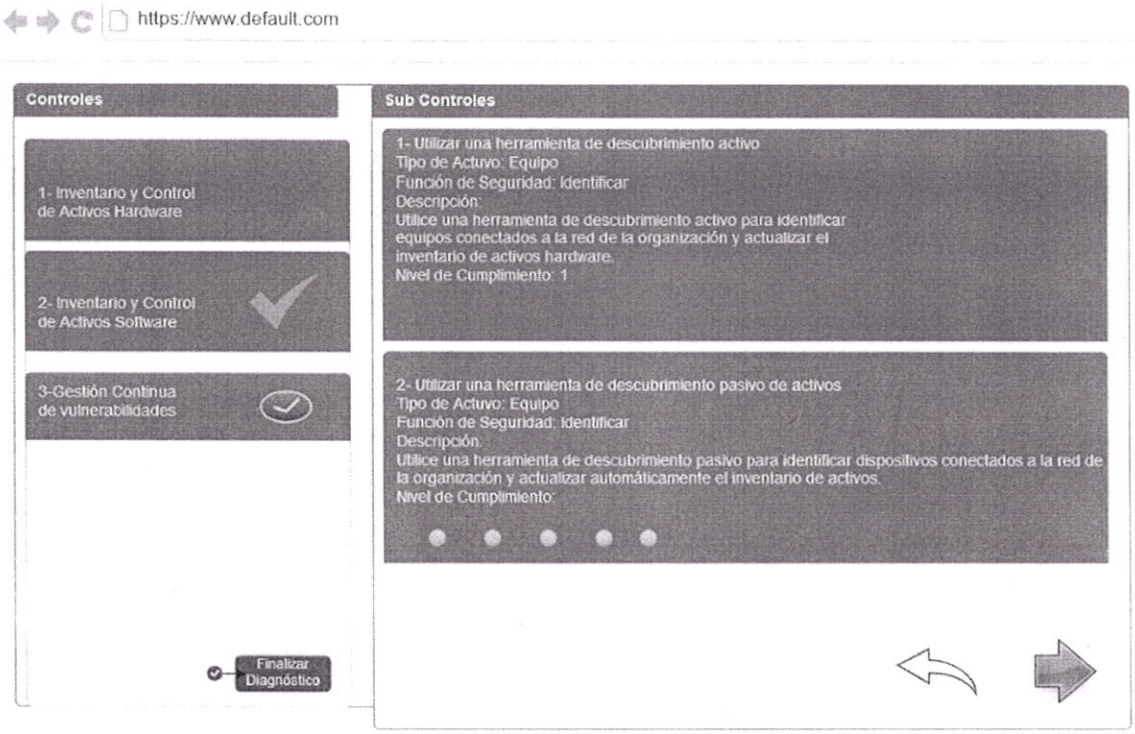
  Para ABM de controles , subcontroles, y valores posibles, para mejor experiencia de usuario, se procederá con un procedimiento de importación y exportación de los controles a partir de una plantilla en formato Excel.

  Durante el proceso de importación, el sistema debe emitir notificaciones de error que indiquen las celdas o campos incorrectos.

- **Acciones del Rol "Operador de Ciberseguridad de la OEE"**
  - Visor de resumen de los controles (solo lectura)
    Lista de Tipos de Controles, Controles, y Subcontroles agrupados.

  - Diagnóstico
    Es la Pantalla de Evaluación.
    - Datos cabecera del diagnóstico (#diagnostico)
    - Datos de la institución
    - Datos del responsable de Seguridad de la Información (SI)
    - Datos de Controles criticos
    - Datos de SubControles críticos
    - Instructivo de como el usuario debe llenar: https://www.cert.gov.py/application/files/5415/3667/3284/Instructivo.pdf

  - Evaluación
    - Análisis de la fórmula utilizada por el CERT-PY https://www.cert.gov.py/index.php/download_file/view/1387/1259
    - Proceso de Cierre y evaluación, según diagrama de pantalla:



- Impresión del diagnóstico cerrado en PDF/XLS
- Resumen Gerencial

Parámetros (rango de fecha de evaluación) Salida(Diagnóstico, Tipo de Control, Sumatoria de Puntaje Logrado, Sumatoria de Puntaje Ideal, Porcentaje).

- Visor e "Histórico de Diagnósticos" de la Institución con su correspondiente evaluación.
  Parámetros(rango de fecha de evaluación) Salida(Evaluación, Puntaje de la Evaluación).

- Reportes
  - Porcentaje de cumplimiento total, con su mensaje
    Es el mensaje que se estira de la configuración de mensajes por puntajes totales (parámetros periodos de fechas de evaluación) (salida con columnas Evaluación (terminada), puntaje, mensaje).

  - Porcentaje de cumplimiento por tipo (Controles Básicos, Fundacionales, Organizacionales), con su mensaje.

    Es el mensaje que se estira de la configuración de mensajes por puntajes por controles.(parámetros periodos de fechas de evaluación, Tipo de Control) (salida con columnas Control, Puntaje, mensaje).

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

GRUPO HORUS
GRUPO HORUS S.A.

- Porcentaje de cumplimiento de acuerdo a la escala (0 al 4), esto es cuantos controles nulos, básicos, etc.
  (parámetros: Diagnostico, Nivel de Cumplimiento) (salida: con columnas Evaluación, Sub Control).

- **Módulo de Evaluación global**
  - Ver el resumen gerencial de todas las instituciones y sus historiales de diagnóstico.
    Parámetros(no tiene parámetros) Salida(Evaluación, OEE, Puntaje de la Evaluación) obs: la información mostrada solamente sobre las últimas evaluaciones activas finalizadas.

  - Visor e "Histórico de Diagnósticos" de la Institución con su correspondiente evaluación.
    Parámetros(rango de fechas, OEE) Salida(Evaluación, Controles, Subcontroles,Puntaje de la Evaluación, agrupado por Evaluación, Controles, y Subcontroles).

  - Se deberá procesar la información recibida y generar un gráfico con los porcentajes de cumplimiento, totales individuales y por tipo (Controles Básicos, Fundacionales, Organizacionales), de todas las instituciones.
    Parámetros(no tiene) Salida(Ultima Evaluación de cada OEE en grafico de barra con puntajes totales de evaluación).
    Parámetros(OEE) Salida(Última Evaluación en gráfico de barra con puntajes totales por Tipo de Control).

  - Generación de informe por rangos dinámicos. Por ejemplo instituciones entre XX% y YY%, instituciones por debajo XX%
    Parámetros(Rango de Porcentajes) Salida(Lista de OEEs).

- **Módulo de Generación de Informes Global**
  - Porcentaje de cumplimiento total, e individual por institución.
    Parámetros (OEE(con opción "todos") Salida(Ultima Evaluación de cada OEE, Puntaje).

  - Listado y/o cantidad de instituciones con mayor, menor o igual cumplimiento que X nivel de cumplimiento.
    Parámetros(Nivel, Menor o Mayor,) Salida(Lista de OEEs) con grafico de torta. Obs: incluir observación que la información se basa en OEEs que hicieron evaluación.

  - Evolución temporal de una determinada institución
    Parámetros(OEE) Salida(Evaluación, Fecha de Evaluación, Puntaje de Evaluación) grafico de linea.

  - Evolución temporal global.
    Parámetros(no tiene) Salida(promedio de puntajes de OEEs) gráfico de linea.

  - Porcentaje de cumplimiento por tipo (Controles Básicos, Fundacionales, Organizacionales)

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

GRUPO HORUS
GRUPO HORUS S.A.

Parámetros(no tiene) Salida(Tipo de Control, OEE, Puntaje de última Evaluación) con un promedio final.

- Porcentaje de cumplimiento de acuerdo a la escala (0 al 4).
  Parámetros(OEE) Salida(OEE, Nivel, Porcentaje).

Roles y Permisos

- **Resumen Perfiles y Permisos y de Auditorías**
  - ADMINISTRADOR (Rol 1 - existente)
  - ADMINISTRADOR DE CIBERSEGURIDAD (Rol nuevo creado id = 5 en esta OT)
  - VISUALIZADOR DE CIBERSEGURIDAD (Rol nuevo creado id = 6 en esta OT)
  - AUDITORÍA DE CIBERSEGURIDAD (Rol nuevo creado id = 7 en esta OT)
  - OPERADOR CIBERSEGURIDAD OEE (Rol nuevo creado id = 8 en esta OT)
  - VISUALIZADOR DE CIBERSEGURIDAD OEE (Rol nuevo creado id = 9 en esta OT)

- **Permisos ADMINISTRADOR:**
  - mantener todos los permisos existentes. Se proporcionará la última versión de la BD.
  - configuración de fecha de expiración de contraseñas.
  - configuración de expiración de sesiones.
  - configuración de parámetros de políticas de contraseña.
  - Configuración de mensajes para reportes de evaluación.

- **ADMINISTRADOR CIBERSEGURIDAD**
  - ABM Controles y valores posibles
  - ABM Subcontroles y valores posibles
  - Carga completa de los controles, subcontroles y datos asociados según planilla
  - Resumen gerencial de todas las instituciones y sus historiales de diagnóstico.
  - Visor e "Histórico de Diagnósticos" de la Institución con su correspondiente evaluación.
  - Informe gráfico de porcentajes de cumplimiento, totales individuales y por tipo (Controles Básicos, Fundacionales, Organizacionales), de todas las instituciones.
  - Generación de informe por rangos dinámicos.

- **VISUALIZADOR CIBERSEGURIDAD**
  - Ver los reportes del operador institucional de cualquier OEE.
  - Ver los reportes del administrador ciberseguridad.

- **OPERADOR INSTITUCIONAL/OEE DE CIBERSEGURIDAD**
  - Visor de resumen de los controles (solo lectura)

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

GRUPO HORUS
GRUPO HORUS S.A.

- Registro de Diagnósticos (Aquí se incluye datos del responsable de la seguridad de la información).
- Resumen Gerencial
- Visor e "Histórico de Diagnósticos"
- Reportes
  - Porcentaje de cumplimiento total, con su mensaje
  - Porcentaje de cumplimiento por tipo (Controles Básicos, Fundacionales, Organizacionales), con su mensaje.
  - Porcentaje de cumplimiento de acuerdo a la escala (0 al 4), esto es cuantos controles nulos, básicos, etc.

- **VISUALIZADOR INSTITUCIONAL**
  - Ver los reportes que ve el operador institucional

- **AUDITORÍAS DE CIBERSEGURIDAD**
  - de inicios de sesión (fallido/exitoso)
  - de configuración de fecha de expiración de contraseñas.
  - de configuración de expiración de sesiones.
  - de configuración de parámetros de políticas de contraseña.
  - de ABM de usuarios y roles.
  - del proceso de negocio del sistema.

Requerimientos No Funcionales

- Todos los listados deben contar con paginación del lado del servidor, salvo autorización expresa del MITIC.
- Todos los campos obligatorios deben estar identificados con (*) y emitir los mensajes de validación apropiados.
- Para la generación de reportes utilizar la librería Eclipse Birt.
- Cualquier librería adicional deberá ser autorizada por el equipo técnico del MITIC.
- Para todos los casos, los servicios REST deben devolver únicamente aquellos datos a utilizarse.
- Los proyectos Java deben funcionar correctamente en IDE Eclipse Oxygen o posterior.
- Los parámetros de configuración deben estar especificados en el backend de la aplicación.
- Los proyectos frontend deben utilizar invocaciones REST con path relativo, configurando una sola variable /api.
- Para el uso o modificaciones de herramientas de georeferenciamiento deberá estar aprobado por el equipo técnico del MITIC.

Entregables

- Deberá entregarse todo el código fuente en los proyectos (repositorio y ramas) indicados por el equipo técnico del MITIC, modificando y entregando los productos y documentaciones en dichos repositorios.
- A efectos de documentación del sistema, se deberá tener en cuenta la preparación o ajustes de los siguientes documentos:
  - Documento de Arquitectura de Solución

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

GRUPO HORUS
GRUPO HORUS S.A.

- Guia de Instalación
- Manual de Usuario
- Documento Casos de Pruebas
- Documento Descripción de Versión

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

Director General de Gobierno Electrónico
Administrador de contrato

Grupo Horus S.A
Proveedor

GRUPO HORUS
GRUPO HORUS S.A.