Propuesta Assesment Centro Medico Integral Fitz Roy

Nullcode Corporate
www.nullcode.com.ar
Mayo 2014

Índice

1 Aviso de Confidencialidad y/o Derechos.

NULLCODE desarrolla la siguiente propuesta integral de Seguridad Informática para Centro Medico Integral CENTRO MEDICO INTEGRAL FITZ ROY. Esta propuesta es confidencial entre ambas partes.

Las expresiones, conceptos y asesoramientos propuestos en este documento son propiedad de NULLCODE para con **Centro Medico Integral Fitz Roy**.

Todas las expresiones, conceptos y asesoramientos incluidos en la presente propuesta son para ser utilizados por NULLCODE, y no podrán ser utilizados bajo ninguna razón sin el expreso consentimiento y/o autorización por escrito.

Todo el material incluido en dicho documento es solamente para la revisión de CENTRO MEDICO INTEGRAL FITZ ROY y sus autoridades y no podrán ser compartidos con cualquier otra persona fuera del equipo de toma de decisión y/o de Centro Medico Integral Fitz Roy.

2 Resumen Ejecutivo

Las organizaciones se exponen a determinados riesgos al utilizar las comunicaciones y sistemas para compartir la información interna y externamente. Estos riesgos no son estáticos, sino rápidamente cambiantes, dinámicos. Debido a un número de factores a saber: descubrimiento constante de debilidades o vulnerabilidades en los sistemas actuales, adquisición de nuevos sistemas con posibles vulnerabilidades, incremento en la sofisticación de los atacantes y amenazas, como así también el aumento de la velocidad de las amenazas.

Por todas estas razones, las organizaciones necesitan determinar su riesgo sobre la base de una frecuencia que dependa de la naturaleza del negocio, en aspectos culturales de la organización (concientización del personal en la manipulación de la información o gestión del conocimiento), como así también del nivel de exposición (factores externos).

Esta es una propuesta de proceso de seguridad que facilita el relevamiento y mejora continua por reducción de riesgos en los activos y/o procesos que abarcan tecnologías informáticas. Para lograr esto la propuesta está estructurada como una secuencia de pasos (o módulos). Cabe recalcar que si el cliente desea instrumentar uno o varios de estos módulos esto se puede realizar ya que estos son independientes, pero se recomienda en lo posible considerar la solución completa presentada y manejarla como proceso completo y/o plan de seguridad informática, o parte del Gobierno de la Seguridad Informática, cada módulo opera individualmente para cubrir todos los aspectos necesarios para cumplir con el apoyo al Gobierno de IT.

- ⇒ **Auditoría Externa** (desde el Internet) incluyendo pruebas de penetración y consultoría especifica adecuada a las necesidades del cliente como puede ser la revisión de la seguridad de un sistema de carga de artículos, encuestas, información específica del periódico.

- ⇒ **Auditoría Interna** (dentro de la organización) la cual también se adecua a las necesidades puntuales de la organización, sistemas de misión crítica, tratamiento de la información interna, arquitectura, equipos de redes, servidores, estaciones de trabajo, equipos con direccionamiento IP. ISO 27001/27002 COBIT

- ⇒ **Remediación & Mitigación** (sobre cada activo) luego de cada testeo, pruebas de seguridad es lógico hallar vulnerabilidades, codificaciones débiles, errores de programación, código inseguro, malas prácticas en general, en las cuales debemos remediar en todo sentido.

- ⇒ **Review Last Check** es una revisión que se lleva a cabo, tiempo después de la ETAPA remediación de la auditoría interna y/o externa inicial.(revisar lo corregido o hallar nuevas brechas de seguridad, a lo y antes visto)

- ⇒ **Risk Assessment** consiste brevemente en la clasificación de activos, análisis de amenazas, impacto, riesgo, probabilidad de ocurrencia, controles, alineación estratégica al negocio etc. Se trabaja con matrices de riesgos exclusiva para Centro Medico Integral Fitz Roy

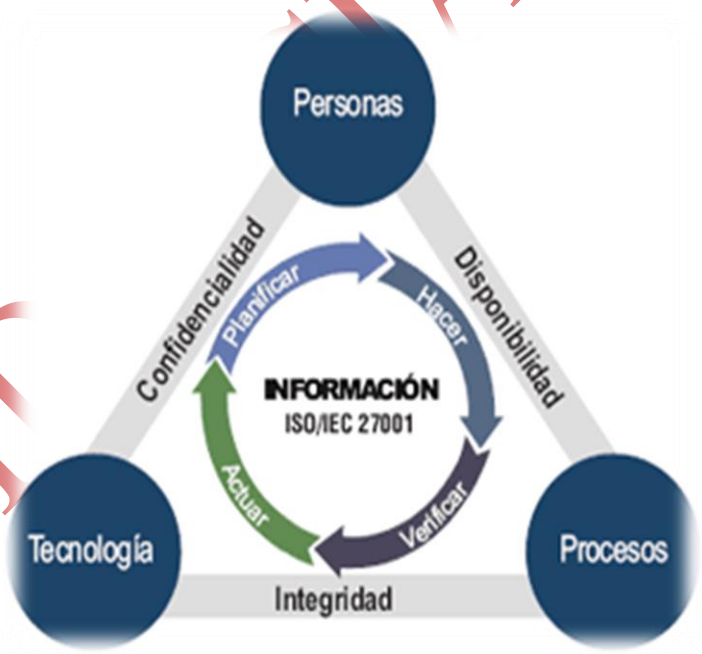
- ⇒ **Consultoría Gobierno S.I.** consiste en una consultoría a nivel global dentro del Gobierno de IT, tales como:
  SOX/PCI/Auditorias/Concientizaciones/BCP/DRP/Programación Segura/Charlas etc.

Este proceso se debe alinear con el "negocio" del cliente para brindar el mantenimiento de la seguridad de la información de la organización, tal como se recomienda en la ISO 27001/27002/COBIT

NULLCODE agradece la posibilidad de presentar esta propuesta a CENTRO MEDICO INTEGRAL FITZ ROY la cual le permitirá incorporar un plan de seguridad informática global en la compañía como así también evaluar el nivel de exposición ante amenazas internas o externas y las posibles vulnerabilidades (basadas en el alcance de la propuesta) de un modo proactivo, es decir, posibilitará encontrar las brechas de seguridad antes de que un atacante o amenaza los aproveche. Consideramos que Centro Medico Integral Fitz Roy puede a partir de este ejercicio copiar el modelo de acciones llevadas a cabo e implementarlas como un plan de seguridad informática que acompaña al negocio en forma permanente.

1) Trabajar con matrices de riesgos, amenaza, impacto, clasificaciones de activos, ejercicios directos de testeos, buenas prácticas, bajo un plan de seguridad aprobado, garantiza el buen tratamiento del riesgo.

NULLCODE propone asistir y colaborar en el proceso de reducir los riesgos (o mitigar aquellos potenciales) del negocio mientras protege sus activos de información. Por tales motivos se presentan todas las herramientas necesarias para llevar a cabo el ejercicio.



La metodología de trabajo, la cual está alineada a estándares internacionales, consiste en tratar de reproducir la manera en que un "hacker"* trataría de introducirse en la organización tanto desde Internet como internamente (dependiendo del módulo pautado), utilizando habilidades, métodos y tecnologías consideradas como mejores prácticas para el desarrollo de dichas tareas.

NULLCODE complementa la metodología con métodos propietarios tales que proveen matrices ya pre armadas y automáticas para la gestión del riesgo.

Esta matrices y/o ejercicios pueden ser utilizables para visualizar el mejoramiento (o no) de la seguridad de la organización, justificable por las medidas de remediación y de negocios aplicadas en el tiempo.

Los entregables del proyecto, como así también las matrices de riesgos incluyen informes que pretenden informar del nivel de riesgo existente detallando resultados y recomendaciones para reducir el riesgo, presentando a nivel ejecutivo (gerencia) como así también a nivel técnico, la métrica de seguridad (RV o Risk-Value) y la consultoría de remediación. Recuerde que cada servicio en sí mismo es parte del próximo servicio y debe ser visto todo bajo un solo contexto, Gobierno de la Seguridad Informática alineado al negocio.

3 Perfil de la Compañía.

NULLCODE fue fundada en sus inicios por el equipo de trabajo Nullcode Services año 2001 quien es considerado como uno de los pioneros en servicios de pruebas de penetración, testing y auditorias de códigos en materia seguridad en Sur América, años después se forma la división 0 Days Vulnerability en las cuales se dio Servicios a compañías tales como Oracle, Microsoft, IBM, SUN etc., auditando códigos, aplicaciones y reportando problemas de seguridad en forma pública y privada

El inminente crecimiento y potencial de ambos grupos de trabajo, dio lugar a la **división Corporativa Nullcode**, quien engloba los servicios generales en materia Gobierno de la Seguridad Informática.

NULLCODE ofrece soluciones consultativas a sus clientes basadas en las mejores herramientas e inteligencia que proveen de soluciones completas y administradas, en respuesta a desafíos de negocios en materia de riesgo de seguridad informática.

"La misión de NULLCODE es ser el socio preferido de seguridad informática para organizaciones, ofreciendo servicios alineados a la realidad, entendiendo sus necesidades y posibilidades-costos"

NULLCODE está en el negocio de ayudar a sus clientes a reducir el riesgo inherente en la utilización de tecnología de la información. Esto se logra mediante primero de la identificación del riesgo a través de servicios de auditoría de ciclo de vida y proporcionando las medidas ("countermeasures") COSO/COBIT, necesarios para que las organizaciones puedan reducir el riesgo de una manera constante en el tiempo y adecuada a sus negocios. Esta metodología de gestión de riesgos se mantiene en el núcleo de negocios y proporciona una forma racional para trabajar con sus clientes, teniendo en cuenta el impacto en el negocio y el riesgo asociado a los costos de las medidas para reducirlo. Esto se realiza mediante el uso de varias áreas de práctica, creadas para reducir el riesgo en situaciones específicas del negocio. Cada una de estas áreas de práctica son implementadas con el uso de productos de tecnologías de punta y emergentes (a través de compañías conocidas como socios de tecnología de **NULLCODE** y las mejores prácticas por los servicios de profesionales y operativos.

NULLCODE es una compañía privada y respaldada por inversionistas con oficinas en Buenos Aires Argentina; su mercado principal es el de las Américas; los clientes están entre mediana empresa, privadas y gubernamentales.

Entre los clientes **NULLCODE** se incluyen la organización de salud, manufactura, financieras, aseguradoras y Gobierno, entre otros.

4 Alcance y metodología.

4.1 Antecedentes

NULLCODE proporciona asesoramiento en Seguridad Informática a sus clientes siguiendo los lineamientos de la metodología de "RISK MANAGEMENT". Esto implica el establecer los riesgos a los cuales se expone la organización de un cliente identificando los elementos a saber: Vulnerabilidades, Amenazas, Activos, Impacto y Costos. Con estos elementos se puede determinar el riesgo, cuantificarlo y determinar el costo para reducirlo y así proteger los activos de la compañía, y determinar el impacto en la organización que produciría dicho riesgo.

NULLCODE ofrece los servicios basándose en normas, estándares mundiales tales como: COSO-COBIT-OSSTMM-ISO-27001/ISO-27005/SOX/PCI/HIPPA, esto quiere decir que cuando armamos los planes, servicios y remediaciones, siempre estamos alienados a determinaos puntos de controles o forma de accionar de estas buenas prácticas, regulaciones. Por tales motivos nuestros servicios ayudan a los servicios internos de auditoría y cumplimiento como así también a las demás gerencias.

NULLCODE ha organizado sus soluciones en distintos módulos:

Módulo	Descripción
1-Risk Assesment	Consultoría orientada a entender y trabajar en reducir el riesgo a un nivel de estado aceptable para la compañía, llevando a cabo tareas de clasificación de activos, vulnerabilidades, amenazas, controles, mitigación, etc.
1.1-Consultoría Global de Seguridad	**Este es un servicio de global consultoría que es conducido por el equipo de Seguridad de la Información de NULLCODE, es una suma de todos los servicios actuales y ayuda a las necesidades del cliente en cuanto a conducir e introducir en su compañía requerimientos globales de certificación Seguridad de la Información.(ISO 27001/2)**
2-External Security Audit	Exhaustivo chequeo de vulnerabilidades o test de penetración (hacking ético) realizados desde Internet hacia la red de la organización.
3- Internal Security Audit	Exhaustivo chequeo de vulnerabilidades, configuraciones, test de penetración (hacking ético) y mucho más, realizados dentro de la compañía. Es el Testing más completo que una compañía puede llevar a cabo.
4-Review Last Check	Revisión de cambios y chequeo de vulnerabilidades o test de penetración (hacking ético) realizados previamente en servicios internos y/o externos. Chequeo de remediaciones aplicadas y/o nuevas amenazas.

4.2 Alcance específico

El alcance de la presente propuesta, cubre varios servicios que fueron alienados y ajustados al pedido puntual del cliente, con el objetivo de ofrecer un plan completo de Seguridad Informática, como parte del Gobierno de IT alineándonos al Gobierno Corporativo.

Luego de la visita y charla que hemos podido tener juntos, como usted puede apreciar hemos incorporado varios servicios en un servicio global enfocado en las necesidades de ustedes.

El objetivo es conducir un plan integral de seguridad de la información en etapas y ciclos, estimamos que esto va a llevar un trabajo de pasos tras pasos entendiéndose a un año o dos de trabajo en conjunto.

4.2.1 Servicios Cotizados

1.1 - Consultoría Global de Seguridad

Este es un servicio de global consultoría que es conducido por el equipo de Seguridad de la Información de NULLCODE, es una suma de todos los servicios actuales y ayuda a las necesidades del cliente en cuanto a conducir e introducir en su compañía requerimientos globales de certificación Seguridad de la Información.(ISO 27001/2)

4.3 Alcance del Servicio

Basado en el servicio Global, es importante poder definir etapas en donde tengamos un estimado de comienzo y final en un marco de trabajo. (Denominado etapas)

Consultoría Global de Seguridad Incluye todos los servicios

4.3.1 ETAPA 1

(Duración 3 meses)

- Solicitar los documentos formales que actualmente posee el cliente.
- Leerlos, entenderlos y detectar anomalías.
- Proponer modificaciones, mejoras a ser aplicadas.
- Otorgar los nuevos documentos ya modificados.

(Cierra etapa 1)

1. Política de Confidencialidad y protección de datos.
2. Política de Seguridad Informática General.
3. Acuerdo con terceros servicios y/o contrataciones.
4. Campaña de concientización en materia Seguridad de la Información.
5. Un Email para denuncias y/o avisos seguridadinformatica@cmfitzroy.com.ar

- ✓ Ley 26.529 Derechos del Paciente Artículos C-D-13/Historia clínica informatizada
- ✓ Ley 25.326 Protección de los Datos Personales: Artículos 8-9-10
- ✓ Ley 26388 Delitos Informáticos

4.3.2 ETAPA 2

(Duración 4 meses)

Vulnerability Assesment:

Las actividades no van a degradar ningún servicio, ni la red ni los equipos productivos.

1. Charla Grupal y/o Presentación Inicial sobre tareas y objetivos a realizar "Alineación con el Cliente"
2. Testeos de Vulnerabilidades en Servidores Críticos
3. Testeos de Vulnerabilidades en Servidores No Críticos
4. Testeos de Vulnerabilidades en Estaciones de trabajos
5. Testeos de Vulnerabilidades en Equipos de Redes
6. Testeos de Vulnerabilidades en Equipos Impresoras, Centrales etc.
7. Testeos de Vulnerabilidades en Capa Aplicaciones Páginas Webs Internas
8. End Point Security Revisión completa de estaciones de trabajo
9. Software malicioso
10. Software No corporativo
11. Detectar software Licenciado
12. Revisión de Usuarios Administradores
13. Revisión por dentro de las Bases de Datos (MSSQL)
14. Informe ,
15. Plan de Remediación
16. Tablero Control

4.3.3 ETAPA 3

(Duración 3 meses)

1. Clasificaciones de Activos
2. Solución Fuga de Datos (se propone una según requerimientos)
3. Controles en Tablero
4. Concientizaciones
5. Charlas grupales

4.3.4 ETAPA 4

(Duración 4 meses)

Penetration Testing sobre activos críticos / Mensual

1. Penetration Testing Interno todos los activos
2. Penetration Testing Externo Webs , sitios
3. Controles en Tablero
4. Sugerencias de cómo proteger lo hallado
5. Tablero final de 50 controles ISO 27001/2 COBIT

Importante: Todas las etapas pueden ser modificables y ajustadas a necesidades específicas del cliente, pero es importante comprender que en condiciones adecuadas debemos cumplir el plan en 14 meses estipulados.

5 El modo de las Trabajo de NULLCODE

Los Servicios Profesionales de **NULLCODE** son directos y reales, utilizamos técnicas y/o herramientas que ayudan a los clientes a desarrollar una estrategia de seguridad mediante la implementación de un modelo de defensa que incluye Técnicas, organización y control de operaciones.

1. **Factor Hacker**. Desde el punto de vista del atacante, este considera como puede ser atacado el sistema en forma remota. (ETAPA1 y ETAPA2)

2. **Factor Riesgo**. Desde el punto de vista de la compañía, cual es el riesgo de ser atacados, cuáles podrían ser las pérdidas o su potencial impacto. (ETAPA1 y ETAPA2)

3. **Factor Defensa**. Desde el punto de vista de la Compañía, deben considerar como los sistemas pueden ser protegidos.(ETAPA 4, ETAPA FINAL)

5.1 Detalle de los procesos

Los procesos de análisis internos, externos y asesoramiento, apuntan a detectar riesgo, amenaza, impacto, controles, vulnerabilidades en los sistemas. Estos procesos apuntan a detectar debilidades o carencia de controles en los equipos de la red, servidores, servidores de aplicaciones o aplicaciones específicas y/o procesos. Ya sea, descuidos nativos de estos o bien, de carácter humano.

Mientras se desarrolla un Testing/servicio, algunos de los resultados encontrados no siempre permiten el control completo del equipo o una explotación con acceso directo al sistema, pero podría ser uno de los elementos que protege a la organización del exterior, cuando se sacan algunos de estos elementos, la capa de protección al exterior se derrumba. Entonces, encontrar una vulnerabilidad o brecha de seguridad en el sistema de información, puede ser el equivalente a una potencial y exitosa intrusión de terceros no autorizados a futuro.

El Testing externo, interno es básicamente un proceso destinado a demostrar como un riesgo puede materializarse, y poner en riesgos el/los sistemas de la compañía.

Existen dos métodos para realizar el testing, una denominado caja blanca, y la otra caja negra.

Caja Blanca: el atacante dispone de información o datos de la red a ser atacada tipo de firewall, usuario del sistema, sistemas operativos, etc. Esta información puede ser utilizada para realizar tanto un ataque interno como externo a la organización. Un atacante experto con habilidades de ingeniería social podría conseguir resultados sorprendentes.

*Cabe comentar acá que normalmente esto no incluye conocimiento del código fuente. El análisis del código para revisar su seguridad es algo recomendado y que **NULLCODE** tiene experiencia pero se considera fuera del alcance de esta propuesta. Si se desear incluir análisis de código se deberá realizar un relevamiento en cuanto a tamaño del código, numero de archivos, lenguaje de programación etc. para poder determinar el esfuerzo/tiempo/costo.*

5.2 Sobre la protección de la información

NULLCODE considera la información de sus clientes de extrema importancia, por tal motivo se protege la información del cliente y la recolectada, utilizando las tecnologías más avanzadas y las mejores prácticas del Mercado.

Particularmente la información utilizada e intercambiada con el cliente se almacena en los sistemas internos de NULLCODE y se protegen de la siguiente manera:

1. Fuerte autenticación y validación del usuario
2. Cifrado de la información en tránsito
3. Uso de equipo específico para el cliente.
4. Finalizado el servicio, el cliente puede solicitar el borrado total de la información recolectada y analizada.

6 Gerenciamiento del Proyecto

El gerenciamiento de los proyectos será dirigido desde nuestras oficinas en Buenos Aires, Argentina, pero dado el servicio solicitado estaremos trabajando una semana en las instalaciones de Centro Medico Integral Fitz Roy.

Las actividades serán realizadas por un equipo de profesionales, el cual incluye mínimamente un líder de Proyecto y un especialista en seguridad. El líder de proyecto será el responsable de coordinar las actividades y el especialista en seguridad de conducir los diferentes test a realizar y transmitir la información necesaria que permita realizar el correspondiente análisis.

7 Tiempos de pruebas

Los test que se realizan poseen técnicas probadas y no producen inconvenientes en los sistemas de los clientes, pero no obstante, y existiendo posibilidades remotas de que ello ocurriera, es que NULLCODE recomienda tomar las siguientes precauciones antes de comenzar a trabajar:

(a) Coordinación de los trabajos entre Nullcode y Centro Medico Integral Fitz Roy
(b) Avisos diarios ,previos a cada actividad
(c) Horarios según el cliente aconseje/cronograma

8 Resultados

Los entregables contendrán los resultados obtenidos de acuerdo a las actividades desarrolladas, en términos al estado de la seguridad informática detectado en CENTRO MEDICO INTEGRAL FITZ ROY dicha información será presentada de la siguiente manera:

Una presentación, documentos de trabajo, lineamientos que contendrán los siguientes aspectos:

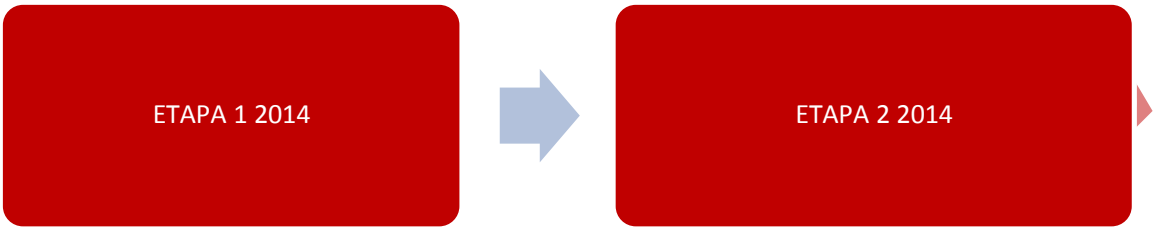
- ✓ Resumen Técnico completo dividido según se acuerde.
- ✓ Resumen y comentarios de los trabajos realizados.
- ✓ Detalles y recomendaciones sobre las vulnerabilidades encontradas.
- ✓ Conclusión final y recomendaciones.

9 Estimación de tiempos

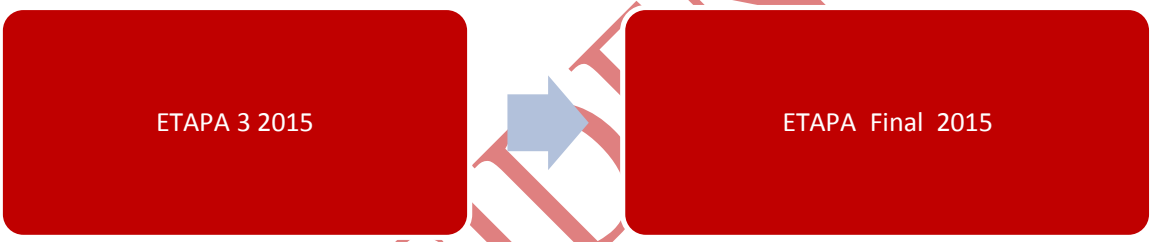
En base al plan y/o servicio solicitado, se propone manejar Etapas.

El diagrama siguiente ayuda a visualizar estas Etapas.

2014



2015



10 Estimación de costos

La siguiente tabla indica los costos a nivel trabajo.
Para esta propuesta se han ofrecidos todos los servicios, personalizados al cliente, tales como matrices, técnicas, herramientas free correspondientes.

10.1 Cotización

Modalidad por etapas:

ETAPA 1.....$ 70.000

ETAPA 2.....$ 80.000

ETAPA 3.....$ 50.000

ETAPA 4.....$ 80.000

Modalidad por contratación externa:

Esta modalidad se refiere a la contratación externa de un recurso experto en seguridad informática el cual llevaría a cabo todas las etapas detalladas y el seguimiento del tablero de control durante el tiempo contratado.

El tiempo de contratación mínima para llevar a cabo las etapas es de **14 meses** por un monto de **$ 20.000 mensual**.

Propuesta válida hasta 31/07/2014

11 Procesos de Aprobación

Si esta propuesta ofrecida a CENTRO MEDICO INTEGRAL FITZ ROY es aceptada, se le enviaran dos documentos a ser firmados llamados:

1) Autorización de servicios
2) Acuerdo de confidencialidad mutua (NDA)

Una vez llevado a cabo esto, se realizará:

1) La pauta del calendario de actividades.
2) Comunicación entre equipos para recolección de datos iniciales
3) Comienzo del Plan ETAPA 1 y luego ETAPA 2
4) Estado final

12 Equipo asignado

El siguiente, será el equipo NULLCODE asignado a este proyecto.
En caso de ser requerido más personal el mismo será notificado con anticipación.

Nombre	Posición	Función
Iván Sánchez	**Audit & Compliance Penetration Tester**	**Penetration tester / Auditor Interno TI /Forense / CISM /ISO 27001-2**

Forma conjunta de Trabajo.

1-Una visita periódica según vamos acordando.

2-Conexión directa VPN de 9 a 17 hs en forma diaria para trabajar con el recurso asignado de Fitz Roy. (En el caso no tengan un recurso exclusivo para seguridad informática, entonces esta vpn/citrix nos va a ser de mucha ayuda diaria)

3-Skype directo.

13 Compromiso de Calidad

Como parte del compromiso de NULLCODE a la calidad de servicio, se le pide al cliente que toda acción que considere a ser mejorada, sea comunicada, para una mejora continua de los procesos de trabajo de NULLCODE: **Clientes@Nullcode.com.ar**