SE APRUEBA PARA EL INSTITUTO DE PREVISIÓN SOCIAL, EL INSTRUCTIVO INSTITUCIONAL DENOMINADO "PROCEDIMIENTO DE SEGURIDAD DESARROLLO DE APLICACIONES INFORMÁTICAS", EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN.

RESOLUCIÓN EXENTA Nº 400

SANTIAGO, 23 AGO 2016

V I S T O S:

1.- La Ley N° 20.255, de Reforma Previsional, que establece la nueva Institucionalidad Pública para el Sistema de Previsión Social y crea entre sus órganos, el Instituto de Previsión Social determinando sus funciones y atribuciones; y el D.F.L. N° 4, de 2009, del Ministerio del Trabajo y Previsión Social que fija la Planta de Personal y fecha de iniciación de actividades de este Instituto.

2.- El D.F.L.N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado, de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

3.- La Ley N° 19.880, de Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.

4.- El D.F.L. N° 278, de 1960, del Ministerio de Hacienda; el D.L. Nº 49, de 1973; el D.F.L. N° 17, de 1989, del Ministerio del Trabajo y Previsión Social; la Resolución N° 1600, de 2008, de la Contraloría General de la República, que fijó las normas sobre exención del trámite de toma de razón; y las facultades que me concede el artículo 57º, de la Ley Nº 20.255.

C O N S I D E R A N D O:

1.- Que, resulta necesario garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información de la División de Informática del Institución de Previsión Social (IPS), para lo cual se analizan las vulnerabilidades en forma automatizada a través de una herramienta de software especializada, administrada por el Departamento de Seguridad de la Información dependiente de la citada División, que permite buscar y eliminar vulnerabilidades de seguridad de las aplicaciones, instaladas en los equipos, y en la configuración de un sistema.

2.- Que, en el contexto citado precedentemente, el Departamento Desarrollo y Mantención dependiente de la División Informática del Instituto de Previsión Social, ha elaborado el "Procedimiento de Seguridad Desarrollo de Aplicaciones Informáticas", cuyo texto ha sido revisado por la Encargada de Seguridad de la Información.

3.- Que, por Oficio Ordinario N° 45514/3261-16, de 03 de agosto de 2016, la División Jurídica de este Instituto, emite informe sobre la aprobación legal del instructivo de la especie, estableciendo la procedencia de dictar la correspondiente resolución aprobatoria por el Departamento de Transparencia y Documentación, la que de conformidad con las disposiciones contenidas en la Resolución N°1600, de la Contraloría General de la República, de 2008, que fija normas sobre exención del trámite de Toma de Razón, se encuentra exenta del mencionado trámite.

R E S U E L V O:

1.- **Apruébase** para el Instituto de Previsión Social, el Instructivo denominado "Procedimiento de Seguridad Desarrollo de Aplicaciones Informáticas", que consta de treinta (30) páginas, que se adjunta como parte integrante de la presente Resolución Exenta, con aprobación legal de fecha 03 de agosto de 2016, cuyo objetivo es garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información de la División de Informática del Institución de Previsión Social (IPS).

2.- Publíquese el Procedimiento, que se aprueba por el presente acto administrativo, en el ambiente "Instructivos Institucionales", de la Intranet del IPS.

3.- Cúmplase con lo dispuesto en el artículo 48, de la Ley Nº 19.880, citada en Vistos Nº 4 y en el Instructivo Presidencial Gab. Pres. Nº 008, de 04 de diciembre de 2006, complementado por Circular Conjunta Nº 3, de 05 de enero de 2007, del Ministerio del Interior y Ministerio de Hacienda, en orden a publicar un extracto del presente acto administrativo en el Diario Oficial y texto completo del mismo en el Banner "Gobierno Transparente".

Notifíquese, regístrese y distribúyase por Departamento de Transparencia y Documentación, a las Jefaturas de las unidades incluidas en la Distribución de la presente Resolución.

INSTITUTO DE PREVISION SOCIAL
DIRECTOR NACIONAL

PATRICIO CORONADO ROJO
DIRECTOR NACIONAL
INSTITUTO DE PREVISIÓN SOCIAL

DISTRIBUCION:
- Gabinete Dirección Nacional
- Subdirección de Servicios al Cliente
- Subdirección de Sistema de Información y de Administración
- División Jurídica
- División Contraloría Interna
- División Beneficios
- División Canales de Atención a Clientes
- División Informática
- División Planificación y Desarrollo
- Departamento Personas
- Departamento Finanzas
- Departamento Administración e Inmobiliaria
- Departamento Transparencia y Documentación
- Departamento Cobranza Institucional
- Departamento Comunicaciones
- Departamento Auditoría Interna
- Direcciones Regionales IPS
- Subdepartamento de Tesorería
- Unidad de Apoyo Documental División Jurídica

RLO/AGA/VCG/MVEW/NCR/MEGA/RPY/MRC/mrc
Instructivo "Procedimiento de Seguridad Desarrollo de Aplicaciones Informáticas".
VIII- (Folio DTD 3575-114)

PROCEDIMIENTO DE SEGURIDAD DESARROLLO DE APLICACIONES INFORMÁTICAS

Elaborado por:	Revisado por:	Aprobado por:
Departamento Desarrollo y Mantención División Informática	Encargada de Seguridad de la Información	División Jurídica Dirección Nacional

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

CONTROL DE CAMBIOS

Fecha	Versión	Página	Numeración del contenido	Cambio Efectuado/Nombre del responsable
2016	01			Versión inicial del documento

La presente versión sustituye completamente a todas las precedentes, de manera que este sea el único documento válido de entre todos los de la serie.

NOTA DE ENFOQUE DE GÉNERO

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representan siempre a todos/as, hombre y mujeres, abarcando claramente ambos sexos.

NOTA DE CONFIDENCIALIDAD

La información contenida en este documento es de propiedad del Instituto de Previsión Social y debe ser tratada de acuerdo a su nivel de confidencialidad, sobre la base de las instrucciones establecidas en la política de clasificación y manejo de información. El uso no autorizado de la información contenida en este documento podrá ser sancionado de conformidad con la ley chilena. Si usted ha recibido este documento por error, le pedimos eliminarlo y avisar inmediatamente al Instituto de Previsión Social (IPS).

INDICE

1. OBJETIVO ____ 4
2. ALCANCE ____ 4
3. DOCUMENTOS DE REFERENCIA ____ 4
4. DEFINICIONES ____ 5
5. RESPONSABILIDADES ____ 7
6. DESCRIPCIÓN DEL PROCEDIMIENTO ____ 8
6.1 Descripción de Actividades ____ 8
6.1.2 Tipos de vulnerabilidades escaneadas ____ 8
6.1.4 Tipos de ataques ____ 10
6.1.5 Informe Auditoria Técnica ____ 11
6.1.6 Resumen Informe Análisis Técnico ____ 15
6.1.7 Generar Solución Vulnerabilidades de Seguridad ____ 15
6.1.8 Aceptar Riesgos de Vulnerabilidad de Seguridad ____ 16
6.2 Diagrama de Flujo Proceso de seguridad desarrollo de aplicaciones informáticas ____ 17
6.2.1 Parte 1 Proceso de seguridad desarrollo de aplicaciones informáticas ____ 17
6.2.2 Parte 2 Proceso de seguridad desarrollo de aplicaciones informáticas ____ 18
6.3 Matriz de Proceso ____ 19
7. INDICADORES DE GESTION ____ 24
8. CONTROL DE REGISTRO ____ 25
ANEXOS ____ 26
A.1. Formulario del Proyecto para Análisis de Seguridad ____ 26
A.2. Diagrama de Arquitectura ____ 27
A.3. Informe Auditoria Técnica ____ 28
A.4. Resumen Informe Auditoria Técnica ____ 29
A.5. Formulario Aceptación Riesgo Vulnerabilidades de Seguridad de Información ____ 30

1. OBJETIVO

Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información de la División de Informática del Instituto de Previsión Social (IPS).

2. ALCANCE

Se aplica a los sistemas de información, en el alcance definido del Sistema de Gestión de la Seguridad de la Información (SGSI), del Instituto de Previsión Social que se encuentren en ambiente de desarrollo, con el fin de proteger y garantizar la confidencialidad, integridad y disponibilidad de la información desplegada internamente en la División de Informática del IPS.

3. DOCUMENTOS DE REFERENCIA

- Resolución Exenta N°56, 15/02/2016; Política Organizacional de la Seguridad de la Información del IPS.
- Resolución Exenta N ° 320, 19/07/2012; Establece Estructura Orgánica del Instituto de Previsión Social.
- Resolución Exenta N° 657,03/12/2015; Define la Política General de Seguridad de la Información del IPS.
- Resolución Exenta N° 231, 24/02/2014; Fija la Estructura Orgánica Interna de la División Informática
- Norma NCh-ISO 27000: 2013.
- Norma NCh-ISO 27002:2013:
  - A.14.2.7 Desarrollo Externalizado
  - A.14.2.8 Pruebas de seguridad del sistema
  - A.14.2.9 Pruebas de aceptación del sistema

4. DEFINICIONES

a) **Aseguramiento de calidad (QA):** Es el conjunto de actividades planificadas y sistemáticas aplicadas en un Sistema de Calidad, para que los requisitos en cuanto a la calidad de un producto o servicio sean cumplan con lo requerido.

b) **Ajax:** Es una técnica de desarrollo web para crear aplicaciones interactivas.

c) **Arquitectura de Sistema:** Es un modelo conceptual que define la estructura, comportamiento y la visión de un sistema.

d) **Caché de Navegación:** Es un lugar de almacenamiento temporal que se encuentra en la computadora y que guarda archivos que han sido descargados por el navegador para mostrar sitios desde la red. Dentro de estos archivos se encuentran aquellos documentos necesarios para la visualización de un sitio, tales como archivos HTML, hojas de estilo de CSS, scripts de JavaScript, gráficos, imágenes y contenido multimedia en general.

e) **CAPTCHA:** Es una prueba controlada por una máquina. Corresponde a las siglas de "Completely Automated Public Turing test to tell Computers and Humans Apart" (prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos).

f) **Cross-site scripting (XSS):** Es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera persona inyectar en determinadas páginas web, código JavaScript o en otro lenguaje similar (ejemplo: VBScript), evitando medidas de control implementadas al efecto. Este tipo de vulnerabilidad se conoce en español con el nombre de "secuencias de órdenes en sitios cruzados".

g) **Desarrollo Integro:** Capacidad de mantener con exactitud la información tal cual fue generada durante el desarrollo, sin ser manipulada o alterada por personas o procesos no autorizados ajenos al proyecto.

h) **Diagrama de Arquitectura:** Es un trazado donde se plasma de forma gráfica las interconexiones de infraestructura y arquitectura del sistema.

i) **Fuerza Bruta:** Es un tipo de ataque de hacking que se programa de manera automática. Consiste en probar durante un período y en determinados lugares, distintas palabras hasta "adivinar" la contraseña.

j) **HyperText Markup Language (HTML):** Es un estándar que sirve de referencia al software que conecta con la elaboración de páginas web en sus diferentes versiones, definiendo una estructura básica y un código (denominado HTML) para la definición de contenido de una página web, como texto, imágenes, videos, juegos, entre otros.

k) **Infraestructura de seguridad perimetral:** Es el conjunto de hardware y software sobre el que se integran elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y disuasión de intrusos en recintos especialmente sensibles.

l) **Pruebas de diccionario:** Es un método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario. Las pruebas de diccionario tienen pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes con letras en mayúsculas y minúsculas mezcladas con números (alfanuméricos) y con cualquier otro tipo de símbolos. Sin embargo, para la mayoría de los usuarios recordar contraseñas tan complejas resulta complicado. Existen variantes que comprueban también algunas de las típicas sustituciones (determinadas letras por números, intercambio de dos letras, abreviaciones), así como distintas combinaciones de mayúsculas y minúsculas.

m) **Pruebas del sistema de permisos y autorización:** Son pruebas que permiten entender cómo funciona la autorización de acceso, los permisos asociados y cómo saltarse el mecanismo de autorización sin el conocimiento de las claves de ingreso.

n) **Pruebas de los mecanismos de autenticación:** Son pruebas que permiten evaluar la vulnerabilidad del sistema frente a accesos o manipulaciones no autorizadas.

o) **Pruebas de los mecanismos de sesión:** Son pruebas que permiten evaluar el funcionamiento correcto de los controles de seguridad del sistema para asegurar la integridad y confidencialidad de los datos.

p) **SQL injection:** Es un método de infiltración de código intruso, que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

5. RESPONSABILIDADES

a) **Jefe Departamento Desarrollo y Mantención (D y M)**: Responsable de gestionar y controlar el adecuado desarrollo de las aplicaciones informáticas, basado en metodologías estándar para la correcta programación y documentación de los sistemas; desarrollar los diseños lógicos y físicos según los requerimientos definidos y solucionar las brechas de seguridad detectadas en los desarrollos internos y externos reportados por los jefes de proyectos.

b) **Jefe Departamento de Seguridad de Información (DSI):** Responsable de coordinar, controlar y ejecutar la implementación de los controles, de desarrollar el análisis de vulnerabilidad de seguridad del sistema de la información (SGSI) sobre los sistemas o servicios desarrollados internamente y de realizar la protección de los activos de información del IPS.

c) **Jefe Departamento de Tecnología:** Debe gestionar y controlar la continuidad operativa, del modelo de gestión tecnológica y de telecomunicaciones del IPS, según los estándares definidos y solucionar las brechas de seguridad reportadas en los desarrollos internos y externos reportados por los jefes de proyectos.

d) **Funcionario del IPS:** Responsable de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral. Tiene la obligación de alertar de manera oportuna y adecuada, por los canales y procedimientos formales establecidos al efecto , de cualquier situación que pueda poner en riesgo la seguridad de la información.

e) **Jefe de Proyecto (JP):** Responsable total del planeamiento y la ejecución acertada de un proyecto determinado o determinable. Es el interlocutor válido, por parte del equipo de desarrollo, para comunicarse con el Jefe Departamento de Seguridad de Información y ser responsable de controlar todas las etapas del proyecto, para asegurar tanto los recursos materiales necesarios como el desarrollo íntegro del sistema.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

6.1 Descripción de Actividades

El análisis de vulnerabilidades se realiza en forma automatizada a través de una herramienta de software especializada, administrada por el Departamento de Seguridad de la Información, que permite buscar y eliminar vulnerabilidades de seguridad de las aplicaciones, instaladas en los equipos, y en la configuración de un sistema.

Los requisitos previos para iniciar el proceso de seguridad en el desarrollo de aplicaciones informáticas son:

- Aplicación o sistema a analizar disponible en un ambiente QA.
- Documentación solicitada completa, que incluye:
  - Formulario del Proyecto para Análisis de Seguridad (Ver Anexo A.1.).
  - Diagrama Arquitectura Proyecto (Ver Anexo A.2.).

Con la documentación correcta y validada por el Departamento de Seguridad de Información, se da inicio al proceso de análisis de vulnerabilidades de seguridad, cuyo plazo estimado para finalizar el proceso es de 5 días hábiles (plazo que puede variar según el proyecto).

6.1.2 Tipos de vulnerabilidades escaneadas

Actualmente existen diferentes tipos de análisis, para determinar vulnerabilidades, entre los que se encuentra el escaneo que se realiza en los sistemas, para a qué sistema se puede acceder desde Internet o desde otra red próxima.

6.1.2.1 Vulnerabilidades de los Sistemas Operativos y Aplicaciones Comerciales.

El objetivo es detectar aquellas vulnerabilidades que puedan existir en los Sistemas Operativos y en las Aplicaciones desarrolladas y mantenidas dentro del ambiente QA y que puedan ser visibles desde Internet.

6.1.2.2 Vulnerabilidades en Aplicaciones Propietarias.

Su objetivo es verificar el nivel de seguridad que posean las aplicaciones desarrolladas internamente en el Instituto de Previsión Social (IPS), comprobando si existen deficiencias en la programación que pudieran ser aprovechadas por un atacante.

6.1.2.3 Vulnerabilidades en la Autenticación y/o Control de Acceso

Su objetivo es verificar el nivel de seguridad de los métodos de ingresos y la posibilidad de accesos no autorizados en los sistemas desarrollados o

mantenidos internamente expuestos a Internet que permitan el acceso de terceros, ya sea mediante autenticación por contraseñas o por medios criptográficos.

6.1.3 Pruebas realizadas

Se llevan a cabo una serie de pruebas de forma externa a los sistemas, simulando, en la medida de lo posible, un ataque real por un hacker, con el objetivo de determinar qué información se podría obtener al realizar un ataque y qué vulnerabilidades se detectan.

El alcance de los trabajos para cada uno de los sistemas analizados incluye las siguientes actividades:

- Análisis de estructura y arquitectura funcional, intentando detectar información visible desde internet de todos los elementos implicados en el servicio: direcciones IP, nombres de dominio, nombre de servidores, etc.
- Test de visibilidad que permita obtener un inventario de los servicios accesibles desde las direcciones IP's públicas, con el fin de determinar cuáles serían las principales puertas de entrada que valoraría un intruso a la hora de intentar un ataque contra los recursos corporativos y dentro del alcance propuesto.
- Identificación de las tecnologías utilizadas: S.O., versiones del software base, nivel de actualización, etc.
- Identificación de las posibles debilidades desde el punto de vista de la seguridad:
    - Pruebas de los mecanismos de autenticación.
    - Pruebas de los mecanismos de sesión.
    - Pruebas del sistema de permisos y autorización.
    - Pruebas de la lógica de negocio.
    - Pruebas de la validación de datos.
    - Pruebas de denegación de servicio.
    - Pruebas sobre los servicios web.
    - Pruebas sobre AJAX.
- Explotación de fallos de programación (SQL injection, XSS, inyección de ficheros, escalado de privilegios, entre otros):
    - Vulnerabilidades en la autenticación
    - Enumeración de usuarios
    - Pruebas de diccionario sobre cuentas de Usuario o cuentas predeterminadas
    - Pruebas de Fuerza Bruta
    - Pruebas para saltarse el sistema de autenticación
    - Pruebas de gestión del Caché de Navegación y de salida de sesión

- Comprobar Sistemas de recordatorio/restauración de contraseñas vulnerables
- Pruebas de CAPTCHA

- Actualizaciones y parches

  El objetivo es conocer el estado de actualización de los sistemas buscando mantenerlas al día. Cada sistema incluido en el alcance definido del SGSI, debe ser analizado para conocer las versiones del software y la correcta aplicación de actualizaciones y parches, así como el tiempo de respuesta en estas situaciones.

- Seguridad en los accesos.

  El objetivo de esta actividad es comprobar la seguridad de los accesos y las posibilidades que tendría un usuario de acceder a operaciones no permitidas y/o datos no autorizados. Para ello, se deben realizar pruebas en las aplicaciones y en las redes que permitan comprobar la posibilidad de vulnerar el esquema de autorizaciones diseñado.

6.1.4 Tipos de ataques

Existen tres tipos de ataques al sistema que son simulados dentro de todas las pruebas para encontrar vulnerabilidades.

- Ataques Pasivos: Recopilando toda la información posible de los sistemas, sin más conocimientos previos de ellos que el que se encuentra en Internet, es decir, de dominio público. Este tipo de ataque permite tener un mejor conocimiento del objetivo para lanzar ataques activos con posterioridad.

- Ataques Activos: Aplicación de los conocimientos recopilados en el ataque pasivo, para intentar violar la seguridad existente.

- Intrusivo: Una vez violada la seguridad existente, se intentar obtener un mayor nivel de acceso al servidor y a la red interna. En ningún caso se realizarán actividades potencialmente peligrosas para la integridad del sistema o servicio, ya que este tipo de ataques tiene por fin el recoger evidencias.

En caso de detectar vulnerabilidades potenciales que requieran de confirmación, las pruebas se realizarán sobre set de datos facilitados por el IPS. Además, se identificarán claramente los datos introducidos en las pruebas para facilitar, si fuera necesario, su eliminación de los sistemas.

6.1.5 Informe Auditoria Técnica

Una vez terminado el escaneo de vulnerabilidades, el programa que realizó el escaneo, crea el Informe de Auditoría Técnica (Ver Anexo 3), el cual contiene lo siguiente:

- Objetivo
- Alcances del Documento
- Resumen Ejecutivo
- Vulnerabilidades Detectadas (Entrega un detalle con la descripción, los elementos afectados, el riesgo y las recomendaciones asociadas al tipo de vulnerabilidad). Ejemplo:

En este capítulo se describen las vulnerabilidades detectadas.

Clickjacking
Descripción
[redacted]
Elementos afectados
[redacted]
Riesgo: Bajo
[redacted]
Recomendaciones
[redacted]

- Recomendaciones:
  En la imagen siguiente se muestra un detalle con las recomendaciones que el mismo sistema entrega, la criticidad y el responsable (ejecutor probable) de mitigar la vulnerabilidad encontrada.

Nº	Recomendación	Criticidad	Ejecutor probable
1	Configurar el servidor de ambos portales para que incluya la cabecera X-Frame-Options en las páginas	Baja	Sistemas
2	Eliminar páginas suministradas como ejemplo por el fabricante del portal nuevoips	Baja	Sistemas
3	Configurar el servidor para que marque las cookies de sesión indicadas con el flag HTTPOnly	Baja	Sistemas
4	Comprobar, y modificar en su caso, el código de los formularios indicados para asegurar que los valores de los parámetros son saneados antes de que se utilicen en la ejecución de comandos o sentencias SQL	Alta	Desarrollo
5	Actualizar el servidor web apache de contactoips a una versión no vulnerable	Alta	Sistemas
6	Configurar el servidor contactoips para que no permita el listado de directorios	Media	Sistemas
7	Actualizar la versión de PHP del servidor contactoips	Media	Sistemas
8	Eliminar o restringir el acceso a la URL que muestra información sobre el código	Alta	Desarrollo

- Escalas de Evaluación de Vulnerabilidades:
  A continuación, se muestra una escala para calificar el grado de gravedad de la vulnerabilidad encontrada.

PONDERACIÓN	CARACTERÍSTICAS
MUY BUENO	Las vulnerabilidades encontradas son sólo informativas. Los segmentos públicos tienen implementado algún sistema de detección de intrusos. La información de la IP's externas es segura y no se encuentran vulnerabilidades Altas a considerar.
BUENO	Las vulnerabilidades encontradas son sólo de un nivel de riesgo Bajo. Las IP's externas tienen implementado algún sistema de detección de intrusos. Se logra obtener información adicional no relevante, desde la Internet.
REGULAR	Las vulnerabilidades encontradas son de nivel de riesgo Bajo y Medio. Las IP's externas, no tiene implementado algún sistema de detección de intrusos. Se logra obtener información adicional relevante a través de Internet.
DEFICIENTE	Algunas de las vulnerabilidades encontradas son de un nivel de riesgo Alto. Se Logra obtener información confidencial desde Internet. Las IP's externas, no tiene implementado algún sistema de detección de intrusos Se logra obtener información adicional relevante a través desde Internet.
MUY DEFICIENTE	Las vulnerabilidades encontradas son de un nivel de riesgo Crítico. Las IP's externas, no tiene implementado algún sistema de detección de intrusos. Se logra obtener información crítica y confidencial, desde Internet con respecto a las IP's públicas involucradas.

- Nivel de Riesgo Vulnerabilidades:

NIVEL RIESGO	DESCRIPCION
CRÍTICA	Es cuando la vulnerabilidad es muy fácil de explotar y pone en riesgo el activo o aplicativo web o dispositivo de la organización afectando la integridad, disponibilidad y confidencialidad del mismo, afectado en relación a la gravedad de la vulnerabilidad, esta puede permitir como por ejemplo tomar control total del dispositivo o aplicativo web o incluso tomar control de base de datos. No se necesita Exploits o tools adicional para explotar. Esta vulnerabilidad debe ser resuelta inmediatamente.
ALTA	Es cuando la vulnerabilidad afecta la disponibilidad, integridad y confidencialidad del dispositivo, aplicativo web o activo, a diferencia de la crítica, esta debe ser explotada por algún medio o Exploits adicional o por lo menos toma más tiempo para llegar al objetivo, y en algunos casos no puede ser 100% Explotable. Esta vulnerabilidad debe ser resuelta a breve plazo.
MEDIA	Es cuando la vulnerabilidad está presente afectando la confidencialidad y en algunos casos afecta también la integridad o funcionamiento del aplicativo, bases de datos o activo de la organización, solo da indicios de la falla y que al explotaría muestra información del dispositivo, que puede ser utilizada para futuros ataques. Esta vulnerabilidad puede ser resuelta en un plazo más largo.
BAJA	Es cuando la vulnerabilidad afecta sólo a nivel de la confidencialidad, entregando información sensible (datos de versión de aplicación, firmware de dispositivo, tipo de base de datos, etc.) y no afecta su funcionamiento del aplicativo Web, dispositivo, activo o bases de datos, muestra información que podría ser útil para futuros ataques de un hacker. Se puede "vivir" con esta vulnerabilidad o puede ser resuelta a largo plazo.

Imagen 4: Niveles de Riesgo identificados en el sistema de análisis.

DEPTO. CONTROL JURIDICO I.P.S.

6.1.6 Resumen Informe Análisis Técnico

Paralelo a la entrega del informe oficial, el equipo de trabajo del Departamento de Seguridad de Información envía un resumen del informe, clasificando los elementos en un cuadro Excel (Ver Anexo A.4).

En total, además de los 2 documentos mencionados, se le entrega un tercer documento "Formulario Aceptación Riesgo Vulnerabilidades de Seguridad" (Ver Anexo 5) que es utilizado en los proyectos que no gestionan la solución de las vulnerabilidades detectadas y quieren continuar con el proceso de paso a producción.

El jefe de proyecto recibe la documentación y determina internamente si gestiona o no la solución sugerida a través de los Departamentos de Tecnologías y/o el Departamento de D y M.

6.1.7 Generar Solución Vulnerabilidades de Seguridad

El Jefe de proyecto envía el informe y el resumen del Departamento de Seguridad de Información a los Departamentos de DyM y Tecnología,

Los Departamentos de DyM y Tecnología, definen los tiempos de trabajo (Horas Hombre) para solucionar las brechas y lo informan al Jefe de Proyecto.

El Jefe de Proyecto envía la información al Jefe Departamento de Seguridad de Información vía correo electrónico, adjuntando el documento de resumen de análisis técnico, donde se pide detallar el responsable de la vulnerabilidad informada y el SLA para dar solución a las vulnerabilidades encontradas.

El Jefe del Departamento de Seguridad de la Información coordina con su equipo de trabajo la supervisión de los SLA informados.

Estos SLA permiten coordinar los nuevos análisis de vulnerabilidades a los sistemas con fallas, una vez cumplidos los plazos informados por el Jefe de Proyecto. De no cumplirse el plazo se entienden aplicados los SLA.

Una vez solucionada la vulnerabilidad, los Departamentos de DyM y/o Tecnologías involucrados informan al Jefe de Proyecto el estado de la situación.

Recibida la información, el Jefe de Proyecto indicará al Jefe Departamento de Seguridad de la Información que las brechas fueron solucionadas. En esta instancia, comienza nuevamente desde cero el análisis de las vulnerabilidades de seguridad y se entrega un nuevo informe que detalla si las brechas de seguridad se mitigaron efectivamente o no. De no mitigarse las brechas, nuevamente se envía el informe al Jefe de Proyecto para que gestione la solución de las vulnerabilidades con los Departamentos de DyM y/o Tecnología.

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

De eliminarse las vulnerabilidades, el Jefe Departamento de Seguridad de la Información coordina internamente con su departamento e informará vía correo electrónico al Jefe de Proyecto su visto bueno para que dé inicio al análisis QA.

En este punto, el Jefe del Departamento de Seguridad de la Información verificará que el plazo comprometido se cumpla. En caso de mantenerse un ciclo donde el Jefe de Proyecto no cumpla con las fechas establecidas para solucionar las vulnerabilidades detectadas, el tema se escala internamente con las jefaturas correspondientes.

6.1.8 Aceptar Riesgos de Vulnerabilidad de Seguridad

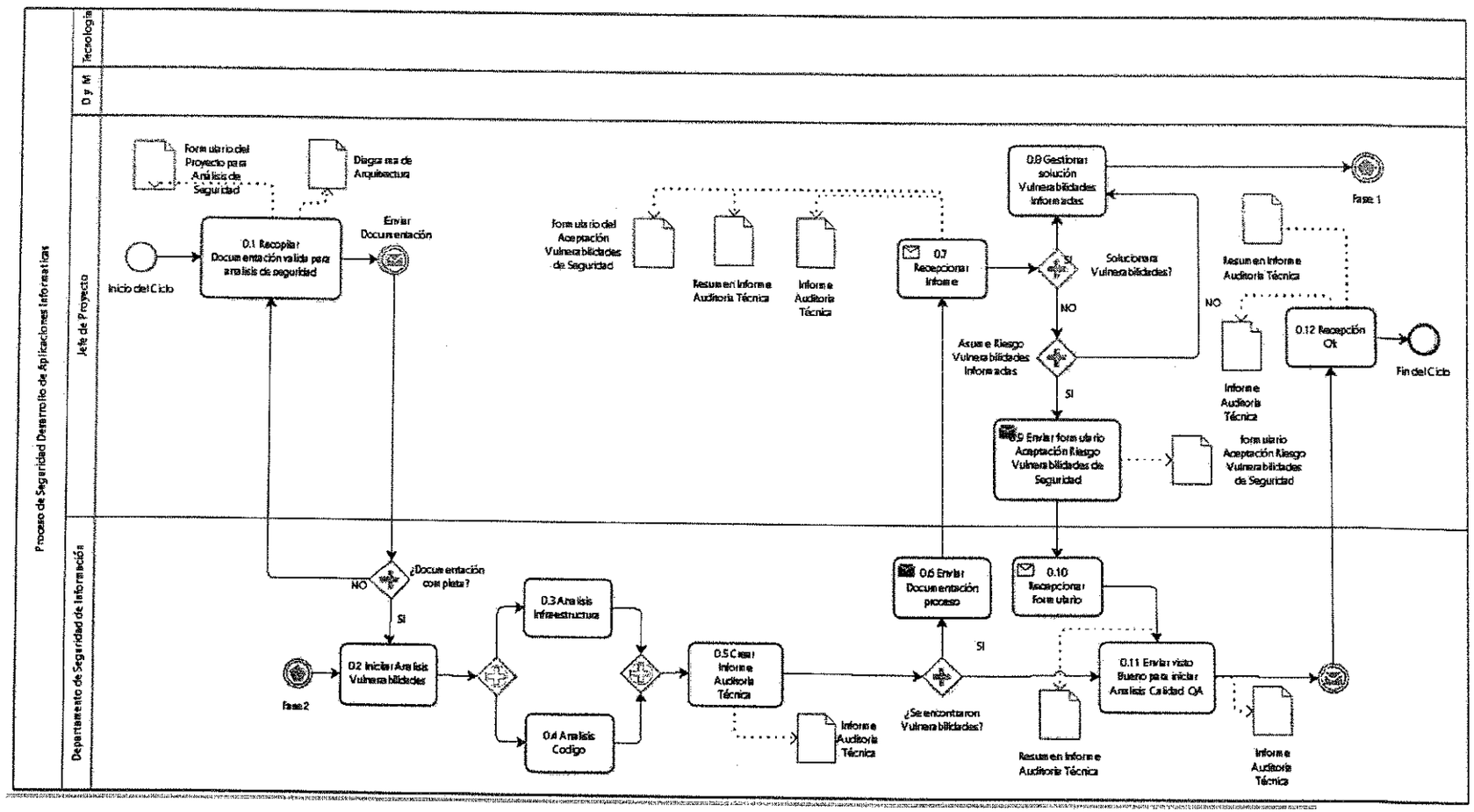
Existen proyectos planificados a largo plazo y otros a corto plazo, en que el tiempo o la urgencia, son puntos clave para terminar los proyectos sin el análisis de vulnerabilidades.

En estos casos, en los cuales se toma la decisión de continuar con el proyecto pese a la ausencia del análisis de vulnerabilidades, el Jefe de Proyecto debe informar al Departamento de Seguridad de la Información a través del "Formulario Aceptación Riesgo Vulnerabilidades de Seguridad de Información" (Anexo 5), indicando el cargo/persona que asume el riesgo.

En caso de posibles fallas, ataques o pérdidas de información en torno a la seguridad de los sistemas, con respecto al sistema en producción, será quien haya asumido los riesgos quien tendrá que ver los temas internos y/o legales según corresponda.

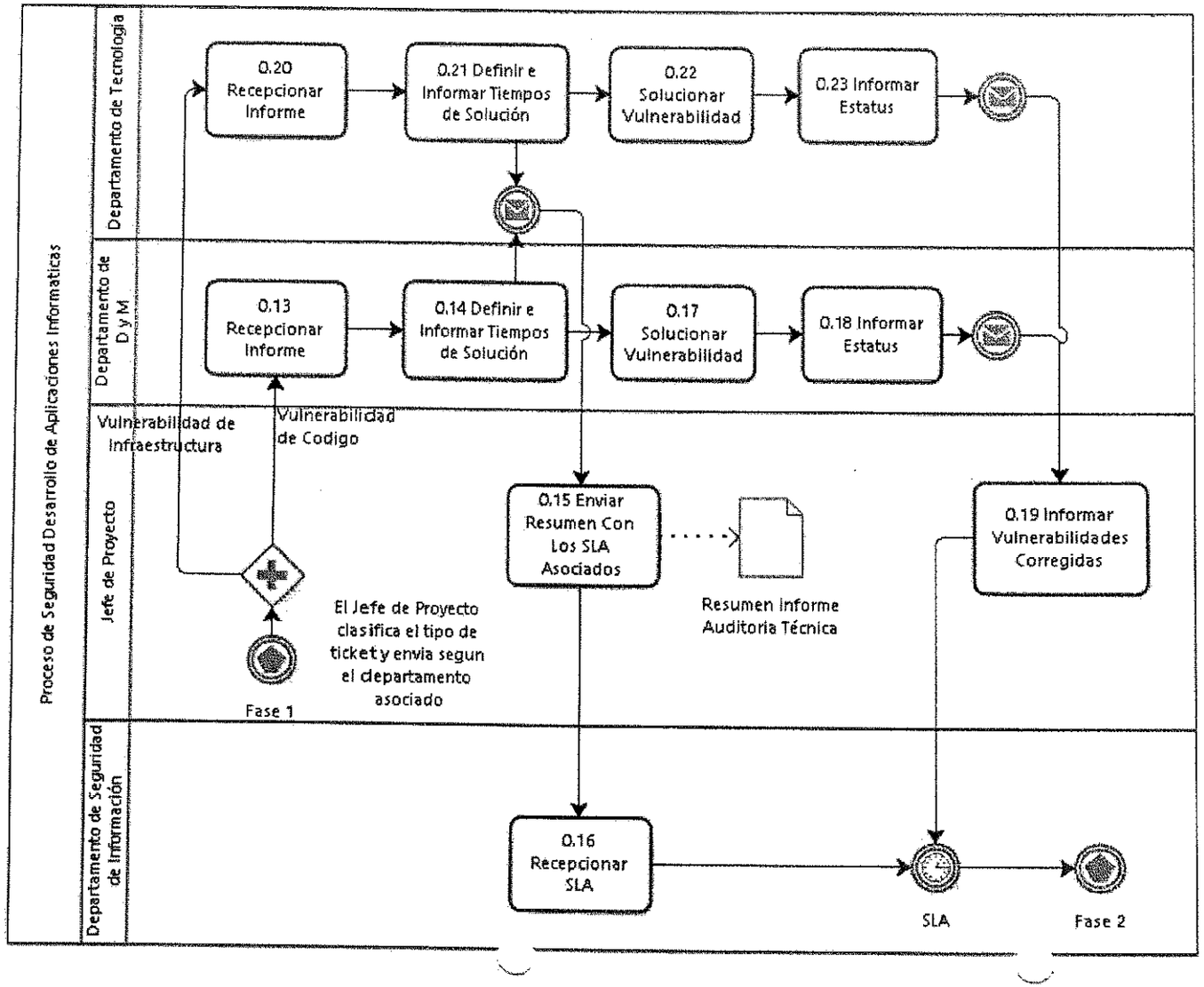
6.2 Diagrama de Flujo Proceso de seguridad desarrollo de aplicaciones informáticas

6.2.1 Parte 1 Proceso de seguridad desarrollo de aplicaciones informáticas



400

6.2.2 Parte 2 Proceso de seguridad desarrollo de aplicaciones informáticas



400

6.3 Matriz de Proceso

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.1	Recopilar Documentación validad para análisis de seguridad	Jefe de Proyecto	• El Jefe de Proyecto envía la documentación solicitada para dar inicio al proceso de análisis de vulnerabilidades según el proceso. →Formulario del Proyecto para Análisis de Seguridad (Anexo A1) →Diagrama Arquitectura Proyecto (Anexo A2) • El Jefe Departamento de Seguridad de Información valida que la documentación está completa, de no ser así solicita al jefe de proyecto la información faltante para dar inicio al proceso.	0.2	Formulario del Proyecto para Análisis de Seguridad, Diagrama de Arquitectura (Ver Anexo 1), Correo Electrónico
0.2	Iniciar Análisis Vulnerabilidades	Jefe Departamento de Seguridad de Información	• Con la documentación correcta el Jefe del Departamento de Seguridad de Información coordina internamente con su equipo de trabajo y da inicio al proceso de análisis de vulnerabilidades de seguridad, por un plazo de 5 días hábiles (plazo que puede variar según el proyecto).	0.3 0.4	
0.3	Análisis Infraestructura	Jefe Departamento de Seguridad de Información	• En forma paralela se realizan estos análisis, en base a la documentación enviada	0.5	
0.4	Análisis Código	Jefe Departamento de Seguridad de Información	• En forma paralela se realizan estos análisis, en base a la documentación enviada	0.5	
0.5	Crear Informe Auditoria Técnica	Jefe Departamento de Seguridad de Información	• Una vez terminado el escaneo de vulnerabilidades se crea el Informe Auditoria Técnica (Ver Anexo 3) (El tamaño de los informes varían según el proyecto.)	0.6 0.11	Informe Auditoria Técnica (Ver Anexo 3).
0.11	Enviar Visto Bueno para iniciar Análisis de Calidad QA	Jefe Departamento de Seguridad de Información	• Al no encontrarse vulnerabilidades, El Jefe Departamento de Seguridad de Información envía la documentación y un resumen del informe de auditoría interna con el estatus Ok.	0.12	Informe Auditoria Técnica (Ver Anexo 3). Resumen Informe Auditoria Técnica (Ver Anexo 4). Correo Electrónico
0.12	Recepción Ok	Jefe de Proyecto	•Recepciona el correo y la documentación asociada, producto que el análisis no presenta vulnerabilidades, se cierra el ciclo	0.13	Fin del Ciclo

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.6	Enviar Documentación proceso	Jefe Departamento de Seguridad de Información	• Al encontrarse vulnerabilidades, el Jefe Departamento de Seguridad coordina con su equipo de trabajo la entrega de la Información, y es enviada la documentación y un resumen del informe de auditoría interna con el estatus de análisis. • Además de los 2 documentos mencionados, al correo se le adjunta un tercer documento llamado "Formulario Aceptación Riesgo Vulnerabilidades de Seguridad" (Anexo 5) que es utilizado en los proyectos que no gestionan la solución de las vulnerabilidades detectadas y quieren continuar con el proceso de paso a producción.	0.7	Informe Auditoria Técnica (Ver Anexo 3). Resumen Informe Auditoria Técnica (Ver Anexo 4). Formulario Aceptación Riesgo Vulnerabilidades de Seguridad(Ver Anexo 5), Correo Electrónico
0.7	Recepcionar Informe	Jefe de Proyecto	• El jefe de proyecto recepciona la documentación y determina internamente si gestiona o no, la solución a través de los Departamentos de Tecnologías y/o el Departamento de DyM. • De solucionarse continua en el proceso 0.8 • De no solucionarse, el Jefe de proyecto debe determinar e informar con "Formulario Aceptación Riesgo Vulnerabilidades de Seguridad" (Anexo 5) quien asume el riesgo de no solucionar las brechas detectadas y cerrar el ciclo para continuar con los siguientes procesos. • De no existir un persona que asuma el riesgo, se debe continuar con el proceso 0.8 • De detectar la persona que asume el riesgo se continua con el proceso 0.9	0.8 0.9	Informe Auditoria Técnica (Ver Anexo 3). Resumen Informe Auditoria Técnica (Ver Anexo 4). Formulario Aceptación Riesgo Vulnerabilidades de Seguridad (Ver Anexo 5), Correo Electrónico
0.8	Gestionar solución Vulnerabilidades Informadas	Jefe de Proyecto	• El jefe de proyecto envía el informe y el resumen del análisis técnico de seguridad a los Departamentos de DyM y de Tecnologías	Fase 1	Informe Auditoria Técnica (Ver Anexo 3). Resumen Informe Auditoria Técnica (Ver Anexo 4). Correo Electrónico
Fase 1	Fase 1	Jefe de Proyecto	•Conexión Ciclo 0.8 con 0.13	0.13	Informe Auditoria Técnica (Ver Anexo 3). Resumen Informe Auditoria Técnica (Ver Anexo 4). Correo Electrónico

400

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.9	Enviar Formulario Aceptación Riesgo Vulnerabilidades de Seguridad	Jefe de Proyecto	• Jefe de Proyecto debe informar al Departamento de Seguridad de la Información a través del "Formulario Aceptación Riesgo Vulnerabilidades de Seguridad" (Anexo 5), quien es la persona que asume el riesgo.	0.10	Formulario Aceptación Riesgo Vulnerabilidades de Seguridad (Ver Anexo 5), Correo Electrónico
0.10	Recepcionar Formulario	Jefe Departamento de Seguridad de Información	• El Jefe Departamento de Seguridad de Información recepciona el formulario, coordina internamente con su equipo de trabajo quien guarda la documentación de respaldo como medios de prueba ante incidentes futuros	0.11	Formulario Aceptación Riesgo Vulnerabilidades de Seguridad (Ver Anexo 5).
0.11	Enviar Visto Bueno para iniciar Análisis de Calidad QA	Jefe Departamento de Seguridad de Información	• Al no encontrarse vulnerabilidades, El Jefe Departamento de Seguridad de Información envía la documentación y un resumen del informe de auditoría interna con el estatus OK al Jefe de Proyecto.	0.12	Informe Auditoria Técnica (Ver Anexo 3). Resumen Informe Auditoria Técnica (Ver Anexo 4). Correo Electrónico
0.12	Recepción Ok	Jefe de Proyecto	•Recepciona el correo y la documentación asociada, producto que el análisis no presenta vulnerabilidades, se cierra el ciclo	0.13	Fin del Ciclo
0.13	Recepcionar Informe	D y M	•El Departamento de Desarrollo y Mantención recepciona el Informe y el Resumen de Análisis de Auditoria	0.14	
0.14	Definir e Informar Tiempos de Solución	D y M	• Definen los tiempos de trabajo (Horas Hombre) para solucionar las brechas e Informan de los tiempos al Jefe de Proyectos • Dentro de la información enviada, se solicita detallar el responsable de la vulnerabilidad detectada y los tiempos de SLA en dar solución a la vulnerabilidad detallada en el documento "Resumen Informe Análisis Técnico".	0.15 0.17	Resumen Informe Auditoria Técnica (Ver Anexo 4). Correo Electrónico
0.17	Solucionar Vulnerabilidad	D y M	• Solucionan la vulnerabilidad entre el equipo de trabajo.	0.18	
0.18	Informar status	D y M	• Una vez solucionada la vulnerabilidad los departamentos involucrados informan al Jefe de Proyecto el estado.	0.19	Correo Electrónico
0.19	Informar Vulnerabilidad Corregida	Jefe de Proyecto	• El Jefe de Proyecto indica al Jefe Departamento de Seguridad de Información que las brechas fueron solucionadas	Fase 2	Correo Electrónico

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
Fase 2	Fase 2	Jefe de Proyecto	• Una vez que el Jefe Departamento de Seguridad de Información recibe el correo de confirmación de la solución de las brechas, se conecta con la fase 2. • En esta instancia comienza nuevamente desde cero el análisis de las vulnerabilidades de seguridad, por esta razón se conecta la fase 2 con el proceso 0.2 y con lleva a un nuevo ciclo en el cual se presenta lo siguiente. • Al terminar el nuevo análisis se entrega un nuevo informe que detalla si se mitigaron las brechas. De no mitigarse las brechas, nuevamente se envía el informe al Jefe de Proyecto para que gestione la solución de las vulnerabilidades con los departamentos correspondientes. • De eliminarse las vulnerabilidades, el Jefe Departamento de Seguridad de Información informa vía correo electrónico al Jefe de Proyecto el visto bueno para que dé inicio al análisis QA.	0.2	
0.20	Recepcionar Informe	Tecnología	•El Departamento de Tecnologia recepciona el Informe y el Resumen de Análisis de Auditoria	0.21	
0.21	Definir e Informar Tiempos de Solución	Tecnología	• Definen los tiempos de trabajo (Horas Hombre) para solucionar las brechas e Informan de los tiempos al Jefe de Proyectos • Dentro de la información enviada, se solicita detallar el responsable de la vulnerabilidad detectada y los tiempos de SLA en dar solución a la vulnerabilidad detallada en el documento "Resumen Informe Análisis Técnico".	0.22	Resumen Informe Auditoria Técnica (Ver Anexo 4), Correo Electrónico
0.22	Solucionar Vulnerabilidad	Tecnología	• Solucionan la vulnerabilidad entre el equipo de trabajo.	0.23	
0.23	Informar status	Tecnología	• Una vez solucionada la vulnerabilidad los departamentos involucrados informan al Jefe de Proyecto el estado.	0.19	Correo Electrónico
0.19	Informar Vulnerabilidad Corregida	Jefe de Proyecto	• El Jefe de Proyecto indica al Jefe Departamento de Seguridad de Información que las brechas fueron solucionadas vía correo Electrónico.	Fase 2	Correo Electrónico

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.15	Enviar Resumen Con los SLA asociados	Jefe de Proyecto	• El Jefe de Proyecto envía al Jefe Departamento de Seguridad de Información el Resumen del Informe Auditoria Técnica detallando en la planilla el responsable de la vulnerabilidad y los tiempos en solucionar la vulnerabilidad.	0.16	Resumen Informe Auditoria Técnica (Ver Anexo 4). Correo Electrónico
0.16	Recepcionar SLA	Jefe Departamento de Seguridad de Información	•Recepciona la planilla informando responsables y tiempos a cumplir	Fase 2	Resumen Informe Auditoria Técnica (Ver Anexo 4). Correo Electrónico
Fase 2	Fase 2	Jefe Departamento de Seguridad de Información	• Una vez que el Jefe Departamento de Seguridad de Información recibe el correo de confirmación de la solución de las brechas, se conecta con la fase 2. • En esta instancia comienza nuevamente desde cero el análisis de las vulnerabilidades de seguridad, por esta razón se conecta la fase 2 con el proceso 0.2 y con lleva a un nuevo ciclo en el cual se presenta lo siguiente. • Al terminar el nuevo análisis se entrega un nuevo informe que detalla si se mitigaron las brechas. De no mitigarse las brechas, nuevamente se envía el informe al Jefe de Proyecto para que gestione la solución de las vulnerabilidades con los departamentos correspondientes. • De eliminarse las vulnerabilidades, el Jefe Departamento de Seguridad de Información informa vía correo electrónico al Jefe de Proyecto el visto bueno para que dé inicio al análisis QA.	0.2	

7. INDICADORES DE GESTION

Nombre Indicador	Formula	Clasificación del Resultado o Criterio de Aplicación			Seguimiento	Cumplimiento	Registros (medios de verificación)
		Muy satisfactorio	Satisfactorio	Insatisfactorio			
Porcentaje de proyectos con análisis de vulnerabilidades	(Total de proyectos desarrollados con análisis de vulnerabilidades/ Total de proyectos desarrollados)*100	=100%	> 50% y < 100%	≤ 50%	Anual	Diciembre	- Planilla Indicadores Proyectos con Análisis de Vulnerabilidades

Se contempla para fines del Segundo año de ejecutado este procedimiento los siguientes indicadores de gestión.

Nombre Indicador	Formula	Clasificación del Resultado o Criterio de Aplicación			Seguimiento	Cumplimiento	Registros (medios de verificación)
		Muy satisfactorio	Satisfactorio	Insatisfactorio			
Porcentaje de Informes de análisis técnico de proyectos revisados sin vulnerabilidades encontradas	(Total de Informes de análisis técnico de proyectos revisados sin vulnerabilidades encontradas / Total de Informes de análisis técnico de proyectos revisados)*100	≥90%	> 50% y < 90%	≤ 50%	Anual	Diciembre	- Planilla Indicadores Proyectos con Hacking Ético

400

8. CONTROL DE REGISTRO

Corresponde a los medios de verificación:

Nombre del Registro	Tipo	Responsable	Ubicación	Soporte	Medio de Almacenamiento (Recuperación)	Tiempo de Retención	Disposición
Formulario del Proyecto para Análisis de Seguridad	Documento	Jefe Departamento de Seguridad de la Información	//DSI/AV/NP	Digital	Respaldo del año	6 años	Eliminar
Diagrama de Arquitectura	Documento	Jefe de Proyecto	//Proyectos/NP	Digital	Respaldo del año	6 años	Eliminar
Informe Auditoria Técnica	Documento	Jefe Departamento de Seguridad de la Información	//DSI/AV	Digital	Respaldo del año	6 años	Eliminar
Resumen Informe Auditoria Técnica	Documento	Jefe Departamento de Seguridad de la Información	//DSI/AV	Digital	Respaldo del año	6 años	Eliminar
Formulario Aceptación Riesgo Vulnerabilidades de Seguridad de Información.	Documento	Jefe Departamento de Seguridad de la Información	//DSI/AV/NP	Digital	Respaldo del año	6 años	Eliminar

- AV:
- Análisis Vulnerabilidades
- DSI: Departamento de Seguridad de Información
- NP: Nombre Proyecto.

	PROCEDIMIENTO DE SEGURIDAD DESARROLLO DE APLICACIONES INFORMÁTICAS			DIVISION INFORMATICA
	Nivel de Confidencialidad	Uso Interno	Versión	01
			Fecha de Aprobación Legal	03 [illegible] 2016
			Página	26 de 30

ANEXOS

A.1. Formulario del Proyecto para Análisis de Seguridad

	FORMULARIO DEL PROYECTO PARA ANALISIS DE SEGURIDAD		DEPARTAMENTO DE SEGURIDAD DE INFORMACIÓN
	Nivel de Confidencialidad	Uso Interno	Jefe de Proyecto
			Fecha | N° Registro |
			Fecha Compromiso Paso a Producción |

Nombre del Proyecto		Versión	

Se informa que además de estos datos, debe enviar el diagrama de arquitectura del proyecto al Departamento Seguridad de Información para su análisis.

INFORMACIÓN INFRAESTRUCTURA			
ACCESO REMOTO		ACCESO WEB	
Nombre Servidor		Nombre Sistema	
IP Servidor		IP / URL Sistema	
USUARIO ACCESO SERVIDOR		USUARIOS DE PRUEBA	
Usuario Servidor		Usuario Acceso Sistema	
Clave Servidor		Clave Acceso Sistema	

Sistema Operativo Servidor (Linux, Windows, IOS)	Versión Sistema Operativo

INFORMACIÓN BASE DE DATOS			
DB		USUARIOS DE PRUEBA	
Nombre Base de Datos		Usuario Base de Datos	
Motor Base de Datos		Clave Base de Datos	
Versión Base de Datos		Instancia Base de Datos	

Adjunta Diagrama Arquitectura SI_____ | NO_____ (Detallar la causa si indica que no, a continuación).

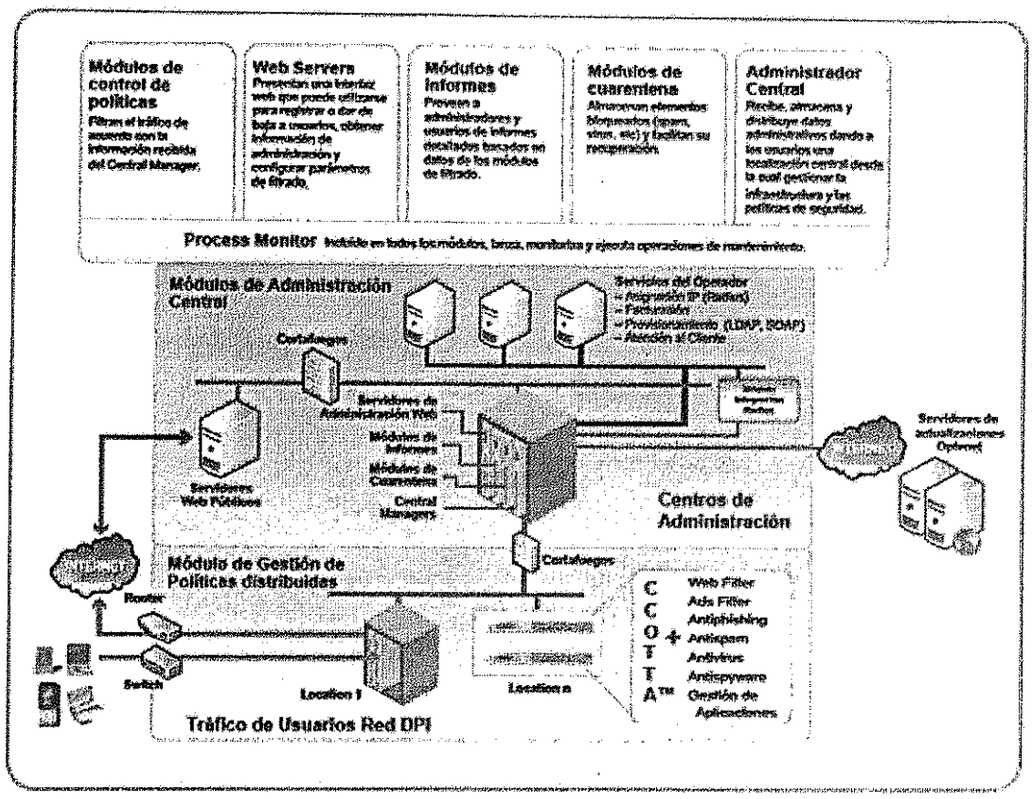
Detalle

_____

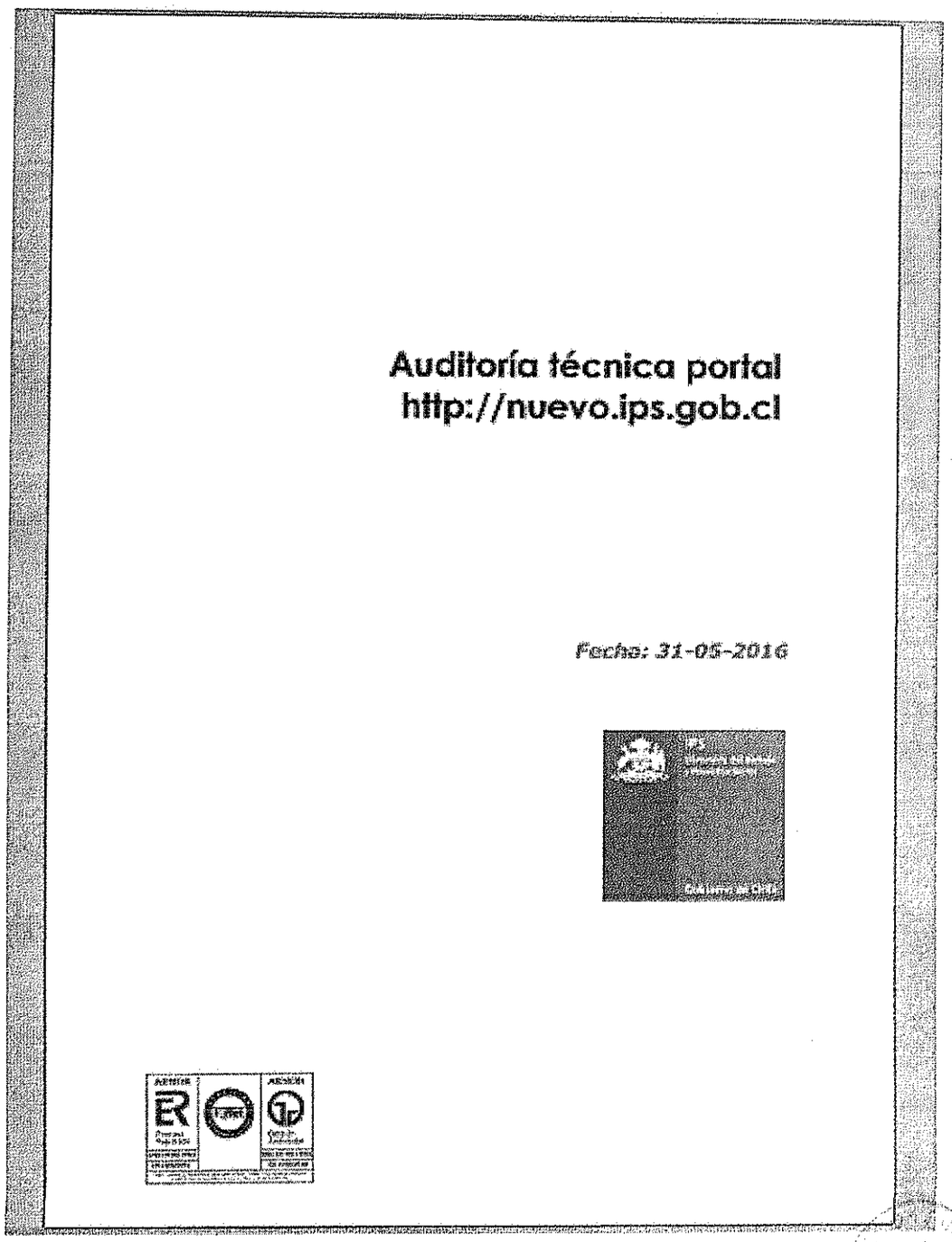
FIRMA JEFE DEL PROYECTO

De ser encontradas vulnerabilidades en torno a la seguridad de los sistemas, se aconseja al jefe de proyecto solucionar estas brechas antes de pasar a producción, de no corregirse estas brechas el responsable y/o el líder de proyecto asume(n) los riesgos de seguridad informados del documento de auditoria técnica.

A.2. Diagrama de Arquitectura



A.3. Informe Auditoria Técnica



Auditoría técnica portal
http://nuevo.ips.gob.cl

Fecha: 31-05-2016

A.4. Resumen Informe Auditoria Técnica

Nombre del Proyecto _____
Jefe de Proyecto _____
N° Registro Formulario del Proyecto para Análisis de Seguridad de Información _____

IP Publica	Respuesta DNS	Puertos abiertos WAN	Vulnerabilidad	Total Vulnerabilidades	Fecha detección	Tarea (Solución)	Responsable	Fecha Implementación	Criticidad

	PROCEDIMIENTO DE SEGURIDAD DESARROLLO DE APLICACIONES INFORMATICAS			DIVISION INFORMATICA
	Nivel de Confidencialidad	Uso Interno	Versión	01
			Fecha de Aprobación Legal	03 AGO 2016
			Página	30 de 30

A.5. Formulario Aceptación Riesgo Vulnerabilidades de Seguridad de Información

	FORMULARIO ACEPTACIÓN RIESGO VULNERABILIDAD DE SEGURIDAD			DEPARTAMENTO DE SEGURIDAD DE INFORMACIÓN
	Nivel de Confidencialidad	Uso Interno	Jefe de Proyecto	
			Fecha |	N° Registro |
			N° Informe Auditoria Técnica	

Nombre del Proyecto		Versión	

DETALLE VULNERABILIDADES			
Cantidad de Vulnerabilidades Encontradas		Vulnerabilidad en la Infraestructura	| SI | NO |
Cantidad de Vulnerabilidades Criticas		Vulnerabilidad en el Codigo	| SI | NO |
Nivel de Riesgo		Acepta el Riesgo	| SI | NO |

DATOS RESPONSABLE RIESGO

Nombre y Apellidos	
Rut	
Departamento	
Cargo	
Mail	
Fono	

FIRMA ACEPTACIÓN

En caso de detectar fallas, ataques o pérdidas de información en torno a la seguridad con respecto al sistema en producción será el responsable de los riesgos quien tendrá que ver los temas internos y/o legales según corresponda.