QUITO
REGISTRO DE LA PROPIEDAD

MEMORANDO N.- RPDMQ-TICS-2017-239

PARA: Byron Guevara
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN RPDMQ

DE: Doris Ochoa
COORDINADORA TICS

ASUNTO: SIREL y Seguridad de la Información

FECHA: 29 de septiembre de 2017

Estimado Sr. Oficial de Seguridad, dentro del proyecto de Modernización del RPDMQ uno de los elementos de software a implementarse es la herramienta SIREL, que reemplazará al actual core registral, con la implementación del SIREL se cambia de forma radical el esquema de trabajo actual del Registro de la Propiedad, que actualmente esta orientado a un trabajo interno, sin exposición de servicios críticos en Internet, por este motivo y otros de tipo regulatorio, dentro del proyecto de Modernización se tenía planificado que el subcomponente de Gestión de Calidad y Seguridad de la Información, sea implementado en forma paralela al componente de Sede Electrónica, donde el core registral tiene una exposión hacia el Internet y requiere de controles y seguridades adicionales a las implementadas hasta el momento, por tal motivo solicito que se analice ***antes de la salida a producción de la herramienta SIREL, la implementación de las seguridades evaluadas como necesarias, en al menos los siguientes aspectos***:

- Políticas de control de Acceso (teniendo en cuenta la gestión de privilegios en el SIREL y Gestor Documental).
- Políticas de Claves (priorizando en enfoque a Directorio Activo, SIREL y Gestor Documental).
- Políticas de Uso de Controles Criptográficos.
- Política de creación de copias de seguridad.
- Complementar con lo que se refiere a el ítem A.14 Adquisición, desarrollo y mantenimiento del Sistema del Anexo A de la norma ISO 27001-2013.
- Tener en cuenta lo relacionado a lo especificado en la Resolución No. 040-NG-DINARDAP-2016, sobre la implementación del EGSI (Esquema Gubernamental de Seguridad de la Información) y los hitos a evaluarse, con un enfoque relacionado al esquema de trabajo que se esta modificando con el proyecto de Modernización Integral del RPDMQ

Y los demás controles que se consideren necesarios.

Sin otro particular al momento, aprovecho la oportunidad para reiterarles mis más altos sentimientos de consideración y estima.

TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES · QUITO REGISTRO DE LA PROPIEDAD · REGISTRO DE LA PROPIEDAD

Atentamente

Doris Ochoa

COORDINADORA TIC`S
REGISTRO DE LA PROPIEDAD
DISTRITO METROPOLITANO DE QUITO

Recibido
02/10/2017
10:17

ANEXOS: Oficio No. DINARDAP-DINARDAP-2017-3582-OF

	FUNCIONARIO	SIGLAS UNIDAD	FECHA	SUMILLA
APROBADO POR:	D. Ochoa	Coordinador TICS	29-09-2017	
ELABORADO POR:	A.Medina	Asistente TICS	29-09-2017	

Ejemplar impreso 1: OFICIAL DE SEGURIDAD DE LA INFORMACIÓN RPDMQ
Ejemplar impreso 2: DIRECCION DE ARCHIVO
Ejemplar impreso 3: TICS

CC.para conocimiento:
Ejemplar impreso 4: Lcda. Liliana Molina Salazar, MBA
DIRECCION ADMINISTRATIVA FINANCIERA
Ejemplar impreso 5: Pablo Durán
ADMINISTRADOR DEL CONTRATO DE FISCALIZACION (E)
Ejemplar impreso 6: Andrés Eguiguren
ADMINISTRADOR DEL CONTRATO DE MODERNIZACION
Ejemplar impreso 7: Verónica Tobar
COORDINADORA GESTIÓN DE PLANIFICACIÓN

REPÚBLICA DEL ECUADOR

DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS

Oficio Nro. DINARDAP-DINARDAP-2017-3582-OF

Quito, D.M., 13 de septiembre de 2017

Asunto: Evaluación de controles de seguridad de interconexión y manejo de la información entre la DINARDAP y el Registro de la Propiedad de Quito

Abogado
José Luis Aucancela Pérez
Registrador de la Propiedad (encargado) (jose.aucancela@quito.gob.ec)
REGISTRO DE LA PROPIEDAD DEL DISTRITO METROPOLITANO DE QUITO
En su Despacho

De mi consideración:

La Constitución de la República del Ecuador en su Art. 66 numerales 19 y 20 reconoce el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley, así como el derecho a la intimidad personal y familiar.

A su vez la Constitución de la República en su Disposición Transitoria Primera manda al órgano legislativo en el plazo máximo de trescientos sesenta días a aprobar las leyes que organicen los registros de datos, en particular los registros civil, mercantil y de la propiedad, así como los sistemas de control cruzado y bases de datos nacionales.

Con fecha 18 de marzo de 2010 se expidió la Ley del Sistema Nacional de Registro de Datos Públicos, publicada mediante Registro Oficial Suplemento 162, de 31 de marzo de 2010, reformada por última vez con fecha 12 de septiembre de 2014.

La Ley Orgánica del Sistema Nacional de Registro de Datos Públicos en su Disposición Transitoria Séptima dispone: "Las instituciones del sector público que posean información pública como: el Servicio de Rentas Internas, el Instituto Ecuatoriano de Seguridad Social, Dirección Nacional de Migración, Dirección Nacional de Tránsito, Dirección Nacional de Registro Civil, Identificación y Cedulación, Policía Nacional, Comisión de Tránsito del Guayas, Ministerio de Relaciones Laborales, Instituto Ecuatoriano de Propiedad Intelectual, Municipios, Función Judicial, entre otras, deberán integrarse paulatinamente al Sistema Nacional de Registro de Datos Públicos dentro del plazo de tres años contados a partir de la entrada en vigencia de la presente ley. En caso de que cualquier institución que estuviese en la obligación de interconectarse en virtud de la presente Ley, no lo hiciere, la máxima autoridad de la referida institución podrá ser destituida por el Director Nacional de Registro de Datos Públicos".

La precitada norma dispone en su Art. 13 inciso segundo *"Los Registros son dependencias públicas, desconcentrados, con autonomía registral y administrativa en los términos de la presente ley, y sujetos al control, auditoría y vigilancia de la Dirección Nacional de Registro de Datos Públicos en lo relativo al cumplimiento de políticas, resoluciones y disposiciones para la interconexión e interoperabilidad de bases de datos y de información pública, conforme se determine en el Reglamento que expida la Dirección Nacional".*

La Ley Orgánica del Sistema Nacional de Registro de Datos Públicos en su Art. 31 determina las

REPÚBLICA DEL ECUADOR

DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS

Oficio Nro. DINARDAP-DINARDAP-2017-3582-OF

Quito, D.M., 13 de septiembre de 2017

REGISTRO DE LA PROPIEDAD DE QUITO **Del 18 al 20 septiembre de 2017**

Lidcrada por los siguientes funcionarios, según acta de reunión del 19 de junio de 2017:

- Ing Fernanda Betancourt.
- Ing. Paúl Jácome.
- Ing. César Salinas(Apoyo)
- Ab. Mayra Aragundi (Apoyo).

Además, sírvase encontrar adjunto los documentos que indican los hitos básicos a evaluarse y las directrices que se tomarán para la evaluación.

Por lo expuesto, solicito de manera cordial coordinar las actividades pertinentes para la evaluación con el equipo correspondiente, a fin de que se prepare la documentación generada en todo el proceso de implementación del EGSI.

Atentamente,

Documento firmado electrónicamente

Sr. Claudio Fabián Massucco
DIRECTOR NACIONAL DE REGISTRO DE DATOS PÚBLICOS, SUBROGANTE

Anexos:
- Resolución DINARDAP-040
- Acta de Reunion
- Documento de Control
- Hitos a ser evaluados

Copia:
Señor Ingeniero
César Patricio Espin Mora
Asesor de Informatica
REGISTRO DE LA PROPIEDAD DE QUITO

Señor Ingeniero
Fernando Andrés Maya Leimberg
Coordinador de Infraestructura y Seguridad Informática

Señor Ingeniero
César Xavier Salinas Herrera
Director de Seguridad Informática

Señorita Abogada
Mayra Alejandra Aragundi Pazmiño
Analista Jurídica en Normativa

Señorita Ingeniera
Erika Fernanda Betancourt Canchignia
Analista de Seguridad Informática 2

Señor Ingeniero

REPÚBLICA DEL ECUADOR

DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS

Oficio Nro. DINARDAP-DINARDAP-2017-3582-OF

Quito, D.M., 13 de septiembre de 2017

Paul Orlando Jácome Cordones
Especialista de Seguridad Informática

fin

(593 2) 2563130
www.datospublicos.gob.ec, info.dinardap@dinardap.gob.ec
Quito – Ecuador

* Documento generado por Quipux

REPÚBLICA DEL ECUADOR

DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS

RESOLUCIÓN N° 040-NG-DINARDAP-2016

LA DIRECTORA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

CONSIDERANDO:

Que, de conformidad con lo previsto en el artículo 227 de la Constitución de la República del Ecuador, la administración pública constituye un servicio a la colectividad que se rige por los principios de eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.

Que, el numeral 19 del artículo 66 de la norma constitucional, manifiesta: "*El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley*";

Que, el artículo 229 del Código Orgánico Integral Penal, establece: "*Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.*";

Que, la Ley del Sistema Nacional de Registro de Datos Públicos, promulgada en el Registro Oficial Suplemento No. 162 de 31 de marzo de 2010, se le dio el carácter de orgánica mediante ley publicada en el Registro Oficial Segundo Suplemento No. 843 de 03 de diciembre de 2012;

Que, el artículo 4 de la Ley del Sistema Nacional de Registro de Datos Públicos señala: "*(...) Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección*

DINARDAP
Av. Río Amazonas N21-147 y Roca, Edificio Río Amazonas, 5° Piso.
(593 2) 2504200 / 2500288
www.datospublicos.gob.ec, info.dinardap@dinardap.gob.ec
Quito – Ecuador

y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información (...)";

Que, el artículo 31 de la Ley del Sistema Nacional de Registro de Datos Públicos determina, entre otras, las siguientes atribuciones y facultades de la Dirección Nacional de Registro de Datos Públicos: "*1. Presidir el Sistema Nacional de Registro de Datos Públicos, cumpliendo y haciendo cumplir sus finalidades y objetivos; 2. Dictar las resoluciones y normas necesarias para la organización y funcionamiento del sistema; (...) 4. Promover, dictar y ejecutar a través de los diferentes registros, las políticas públicas a las que se refiere esta Ley, así como normas generales para el seguimiento y control de las mismas; 5. Consolidar, estandarizar y administrar la base única de datos de todos los Registros Públicos, para lo cual todos los integrantes del Sistema están obligados a proporcionar información digitalizada de sus archivos, actualizada y de forma simultánea conforme ésta se produzca; (...) 7. Vigilar y controlar la correcta administración de la actividad registral...*";

Que, la Ley Orgánica de Transparencia y Acceso a la Información Pública en su artículo 10, expresa: "*Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción. Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública*";

Que, el artículo 2 del Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos, establece: *"El Sistema Nacional de Registro de Datos Públicos.- Está conformado por las instituciones públicas y privadas determinadas en la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, y las que en el futuro determine, mediante resolución, el Director Nacional de Registro de Datos Públicos, en ejercicio de sus competencias"*;

Que, el artículo 5 del reglamento ibídem, indica: *"Responsables de las bases de datos.- El responsable de la información correspondiente a los entes registrales es la máxima autoridad de cada una de las instituciones. Los entes del Sistema deberán comunicar a la Dirección Nacional de Registro de Datos Públicos el nombre del funcionario que gestione la base de datos. En ningún caso el ente registral podrá estar sin un delegado institucional, que será el responsable de la administración de las bases de datos públicos y su correcto funcionamiento"*;

Que, el artículo 13 de la norma ibídem, expresa: *"Responsables de las bases de datos.- El responsable de la información correspondiente a los entes registrales es la máxima autoridad de cada una de las instituciones. Los entes del Sistema deberán comunicar a la Dirección Nacional de Registro de Datos Públicos el nombre del funcionario que gestione la base de datos. En ningún caso el ente registral podrá estar sin un delegado institucional, que será el responsable de la administración de las bases de datos públicos y su correcto funcionamiento"*;

Que, la Secretaría de la Administración Pública, mediante Acuerdo No. 166 publicado en el Registro Oficial No. 88 de 25 de septiembre de 2013, acuerda el uso obligatorio de las Normas Técnicas para la implementación del Sistema Gubernamental de Seguridad de la Información EGSI a todas las Entidades de la Administración Pública Central, Institucional, y que dependen de la Función Ejecutiva;

Que, de conformidad con lo dispuesto en el numeral 2, subnumeral 2.1, literal c) del Esquema Gubernamental de Seguridad de la Información (EGSI), es competencia de la máxima autoridad de la institución, conformar oficialmente el Comité de Gestión de la Seguridad de la Información y designar a sus miembros conforme lo previsto en el Esquema antes puntualizado;

DINARDAP
Av. Río Amazonas N21-147 y Roca, Edificio Río Amazonas, 5° Piso.
(593 2) 2504200 / 2500288
www.datospublicos.gob.ec, info.dinardap@dinardap.gob.ec
Quito – Ecuador

Que, es menester la implementación del Esquema Gubernamental de Seguridad de la Información para todas las instituciones o entidades que integran el Sistema Nacional de Registro de Datos Públicos, al ser instituciones que poseen bases de datos y que alimentan o consumen información del mencionado sistema;

Que, mediante Acuerdo Ministerial No. 003-2015 de 16 de enero de 2015, el ingeniero Augusto Espín Tobar, Ministro de Telecomunicaciones y de la Sociedad de la Información, nombró a la señora abogada Nuria Susana Butiñá Martínez como Directora Nacional de Registro de Datos Públicos.

En ejercicio de las facultades que le otorga el artículo 31 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, resuelve expedir la siguiente:

NORMA DE IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) EN LAS ENTIDADES QUE INTEGRAN EL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS (SINARDAP)

Art. 1.- Disponer a las instituciones que forman y formarán parte del SINARDAP, la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), conforme los lineamientos constantes en el Acuerdo No. 166 de 19 de septiembre de 2013, publicado en el Registro Oficial Suplemento No. 88 de 25 de septiembre de 2013, expedido por la Secretaría Nacional de la Administración Pública.

Art. 2.- Las máximas autoridades de las instituciones pertenecientes al SINARDAP, deberán ser informadas a través del oficial de seguridad, sobre los avances realizados y las actividades ejecutadas en la implementación del EGSI en sus instituciones.

Posteriormente, la máxima autoridad de la institución deberá informar a la máxima autoridad de la DINARDAP, de manera semestral, las actividades desarrolladas y avances en la implementación del Esquema de Seguridad de la Información (EGSI).

Art. 3.- La DINARDAP, sin contradecir las disposiciones emanadas por el EGSI, de conformidad con lo establecido por el artículo 1 de la presente resolución, podrá emitir cualquier disposición relacionada al mejoramiento de la seguridad de la información, para las entidades que integran el SINARDAP.

Av. Río Amazonas N21-147 y Roca, Edificio Río Amazonas, 5° Piso.
(593 2) 2504100 / 2500255
www.datospublicos.gob.ec, info.dinardap@dinardap.gob.ec
Quito – Ecuador

Art. 4.- La DINARDAP, al ser la entidad encargada de administrar y presidir el SINARDAP, a través del Comité de Seguridad realizará y ejecutará planes de control sobre la correcta ejecución del EGSI, a las entidades que lo conforman.

Estos planes en los casos que aplique, serán coordinados con la SNAP, únicamente a las entidades que formen parte del ejecutivo.

Así mismo, dichos planes, serán ejecutados de conformidad con lo establecido en el Plan de Control y Auditoría establecido por la DINARDAP.

Art. 5.- El Comité de Seguridad de la Información podrá delegar la realización de los Controles y Auditorias a un equipo de trabajo especializado en la materia, para lo que deberá designar y nombrar a los funcionarios que integrarán dicho equipo, quienes serán los encargados de elaborar los respectivos planes de control y efectuar las correspondientes auditorias, velando por la correcta aplicación y ejecución de las normas expuestas por el EGSI.

El equipo de auditoría necesariamente deberá integrarse por un representante del área legal, por un representante del área técnica (específicamente del área de seguridad informática) y por un representante del área de Control.

DISPOSICIONES GENERALES:

Primera.- Las Disposiciones constantes en la presente Resolución, tienen carácter de obligatorio para los servidores de las instituciones que integran el SINARDAP.

Segunda.- Encárguese de la ejecución de la presente Resolución al Comité de Gestión de la Seguridad de la Información y al Oficial de Seguridad de la DINARDAP.

DISPOSICIÓN TRANSITORIA:

La DINARDAP, a través del Comité de Seguridad en un plazo de 30 días, contados a partir de la publicación de la presente resolución, elaborará y remitirá la documentación necesaria para el levantamiento de información sobre la situación actual y cumplimiento de los controles basados en el EGSI, a la máxima autoridad de las instituciones que integran el SINARDAP.

Las instituciones que integran el SINARDAP, deberán enviar la información relacionada al levantamiento de información sobre la situación actual y cumplimiento de los controles basados en el EGSI, en un plazo de 60 días

DINARDAP
Av. Río Amazonas N21-147 y Roca, Edificio Río Amazonas, 5° Piso.
(593 2) 2504200 / 2500288
www.datospublicos.gob.ec, info.dinardap@dinardap.gob.ec
Quito – Ecuador

contados a partir de la entrega de la documentación referida en el párrafo que antecede.

Respecto de las entidades registrales, que si son controladas por parte de la SNAP relacionadas a la implementación y uso del EGSI, deberán presentar a la máxima autoridad de la DINARDAP, el informe de nivel de cumplimiento emitido por dicha Secretaría, perteneciente al último año de evaluación.

DISPOSICIÓN FINAL:

Esta Resolución entrará en vigencia a partir de su publicación en el Registro Oficial.

Dada en la ciudad de Quito, Distrito Metropolitano, el 22 de septiembre de 2016.

Abg. Nuria Butiña Martínez
DIRECTORA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

DATOS PÚBLICOS	PROCESO: AUDITORIA RESOLUCIÓN 40
	ACTIVIDAD: REUNIONES DE TRABAJO CONVOCADAS
ACTA DE REUNIÓN	Página 1 de 2

ACTA DE REUNIÓN	
Unidad: Reunión Auditoría Resolución 40	**Acta No: RES40-2017-001**
Responsable de la Unidad:	**Fecha:** 19/06/2017
Lugar: Quito, Av Amazonas N21-147 y Roca, quinto piso	**Hora inicio:** 10:00 **Fin:** 11:30

ASISTENTES

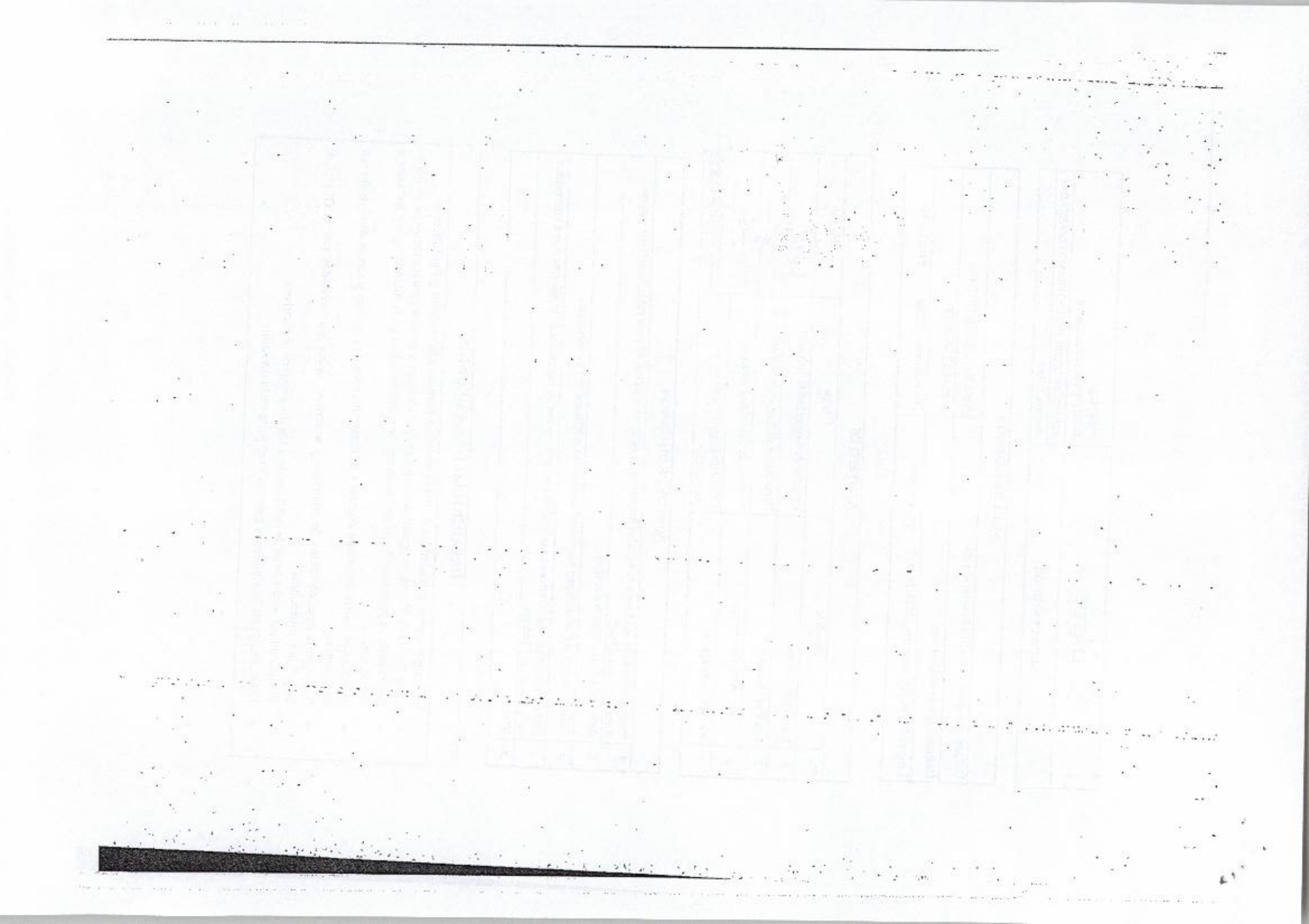
No.	Nombre	Cargo	Firma
1	Ing. César Salinas	Director de Seguridad Informática.	
2	Ing. Paúl Jácome	Especialista de Seguridad Informática.	
3	Ing. Fernanda Betancourt	Analista de Seguridad Informática.	
4	Ab. Mayra Aragundi	Oficial de Seguridad de la Información	

PUNTOS DE DISCUSION

1	Presentación de la Auditoría al EGSI resumido parte de la Resolución 40 para las instituciones que no reportaban a la SNAP.
2	Definición de los Puntos a revisar
3	Definición de los Parámetros a ser considerados y las calificaciones a considerar.
4	Delegación de los responsables de la evaluación de los temas de seguridad de la información e informática por parte de la Dinardap
5	Varios.

DESARROLLO DE LA REUNIÓN

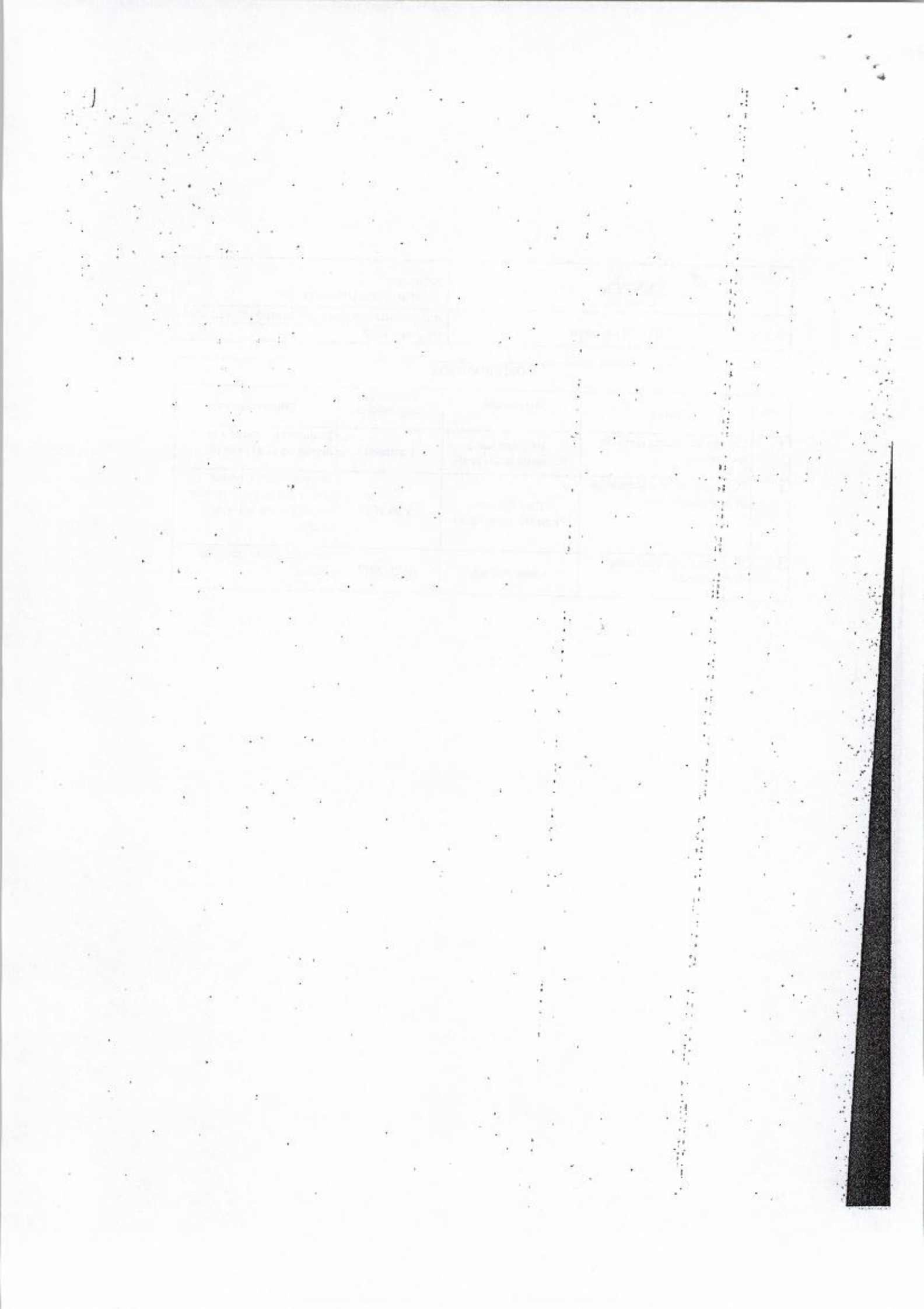
- Se designa como responsables de la evaluación a Fernanda Betancourt y Paúl Jácome.
- César Salinas y Mayra Aragundi, serán los apoyos técnicos y legales para los temas de revisión.
- Revisión de la presentación: respaldo normativo, lineamientos de la metodología y métodos a considerar.
- Se revisa la matriz de hitos a evaluar y se determinan los entregables y temas de revisión por cada punto.
- Se propone que los temas de contratos y acuerdos deben ser revisados por el Oficial de Seguridad informática.
- Se definen los parámetros de calificación a los documentos normativos
- Selección de las instituciones que van a ser parte de la revisión



DATOS	PROCESO: AUDITORIA RESOLUCIÓN 40
	ACTIVIDAD: REUNIONES DE TRABAJO CONVOCADAS
ACTA DE REUNIÓN	Página 2 de 2

COMPROMISOS

No	Tarea	Responsable	Período de cumplimiento	Observaciones
1	Entrega de Cronograma de Evaluación	Paúl Jácome Fernanda Betancourt	1 semana	Documento acorde a lo dispuesto en al reunión
2	Definición de la metodología de evaluación	Paúl Jácome Fernanda Betancourt	29/06/2017	Documentación de los temas que se van a revisar considerando los hitos a evaluar
3	Revisión de la metodología de evaluación	Cesar Salinas	30/06/2017	Emisión de comentarios finales



HITOS A EVALUAR

HITOS	DESCRIPCIÓN	ENTREGABLE	RESPONSABLE
	1 1: POLITICA DE SEGURIDAD DE LA INFORMACIÓN		
1.1	Documento de la Política de la Seguridad de la Información		
1.1.2	(P) Difundir la política de seguridad de la información de referencia o propia de la institución.	Memorando Informativo	
1.2	Revisión de la Política		
1.2.1	(P) Garantizar la vigencia de la política de seguridad de la información en la institución.	Política de Seguridad de la Información aprobada	
	2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
2.1	Compromiso de la máxima autoridad de la institución con la seguridad de la información realizada		
2.1.1	(P) Realizar el seguimiento de la puesta en marcha de las normas de este documento	Seguimiento de la puesta en marcha de la norma	
2.1.2	(P) Disponer la difusión, capacitación y sensibilización del contenido de este documento	Memos, documentos de capacitación	
2.2	Coordinación de la Gestión de la Seguridad de la Información		
2.2.1	La coordinación estará a cargo del Comité de Gestión de Seguridad de la información el cual tendrá las siguientes funciones:	Funciones designadas al Comité	
2.2.1.1	(P) Designar formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador del CSI	Designación formal del Oficial	
2.2.1.2	(P) Designar formalmente al responsable de Seguridad del área de Tecnologías de la Información	Designación formal	
2.3	Asignación de responsabilidades para la seguridad de la información		
	El Oficial de Seguridad de la información tendrá las siguientes responsabilidades		
2.3.3	EJECUCIÓN : Procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento definidos	Evidencia de cumplimiento de incidentes de seguridad orientado a medios masivos	
2.3.5	EJECUCIÓN : Controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, garantizar la seguridad de los datos y los servicios conectados a las redes de la institución definidos y documentados	Documento definido y evidencias del procedimiento	
2.3.6	EJECUCIÓN: Procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios desarrollados.	listado y evidencia de procedimientos aprobados	
	El responsable de Seguridad del Área de Tecnologías de la Información tendrá las siguientes responsabilidades		
2.3.17	EJECUCIÓN: Controles de seguridad definidos (ej., evitar software malicioso, accesos no autorizados, etc.), implementados	Políticas y procedimientos aprobados	
2.3.19	EJECUCIÓN: Incidentes de seguridad de la información de acuerdo a los procedimientos establecidos gestionados	Documento definido y evidencias del procedimiento	
2.5	Acuerdos sobre Confidencialidad		
2.5.1	(P) Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI	Evidencia del acuerdo. - Institucionales - Tecnología - DBA - Terceros	
2.5.2	(P) Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción	Evidencia del acuerdo. - Institucionales - Tecnología - DBA - Terceros	
2.5.5	(P) Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros	Evidencia del acuerdo. - Institucionales - Tecnología - DBA - Terceros	
2.6	Contacto con las autoridades		
2.6.3	EJECUCIÓN: Datos de contacto de proveedores de bienes o servicios de telecomunicaciones o de acceso a la Internet para gestionar potenciales incidentes identificados y actualizados	Documento definido y evidencias del procedimiento	
2.11	Consideraciones de la seguridad de los acuerdos con terceras partes		
2.11.1	EJECUCIÓN: Acuerdos firmados entre la organización y terceras partes garantizados y entendidos	Acuerdos firmados	

(P) Hitos prioritarios
Controles clave de cumplimiento de los documentos normativos

HITOS A EVALUAR
DIRECCIÒN DE SEGURIDAD INFORMÁTICA

3	GESTIÓN DE LOS ACTIVOS		
3.1.2	Inventario de activos de soporte de Hardware	Inventario documentado de hardware	
3.1.2.5	(P) Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.	Inventario de activos documentado y aprobado	
3.1.2.7	(P) Tableros; de transferencia (bypass) de la unidad interrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.	Inventario de activos documentado y aprobado	
3.1.2.8	(P) Sistemas: de control de accesos, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión; etc.	Inventario de activos documentado y aprobado	
3.1.3.2	(P) Software de mantenimiento o administración de: Gabinetes, servidores de cuchilla, servidores, sistema de redes de datos, sistemas de almacenamiento, telefonía, UPS, etc.	Informes internos y por parte del proveedor.	
3.1.3.4	(P) Aplicativos informáticos del negocio	Inventario de aplicativos del negocio	
3.1.4	Inventario de activos de soporte de redes	Inventario documentado de redes	
3.1.4.1	(P) Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ, interfaz V35, RS232, USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc.	Inventario de activos de soporte de redes documentado y aprobado	
3.1.4.2	(P) Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.)	Inventario de activos de soporte de redes documentado y aprobado	
3.1.4.3	(P) Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.	Inventario de activos de soporte de redes documentado y aprobado	
3.1.4.4	(P) Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.)	Inventario de activos de soporte de redes documentado y aprobado	
3.2	Responsable de activos		
3.2.1	EJECUCIÓN: Asignar los activos asociados (o grupos de activos) a un individuo que actuará como Responsable del Activo. Por ejemplo, debe haber un responsable de los computadores de escritorio, otro de los celulares, otro de los servidores del centro de datos, etc. El término "responsable" no implica que la persona tenga realmente los derechos de propiedad de los activos.	Designación de el o los responsables de manera formal	
3.4	Directrices de clasificación de la información		
3.4.1	(P) Clasificar la información como pública o confidencial	Informe de la clasificación	
3.4.2	EJECUCIÓN: Catálogo de clasificación de la información aprobada y elaborada	catálogo de información	
4	SEGURIDAD DE LOS RECURSOS HUMANOS		
4.1	Funciones y responsabilidades		
4.1.2	(P) Entregar formalmente a los funcionarios sus funciones y responsabilidades	documento de entrega de funciones	
4.1.4	EJECUCIÓN: Oficial de Seguridad de la información notificado sobre los eventos potenciales, intentos de intrusión u otros riesgos que pueden afectar la seguridad de la información de la institución	Informes y notificaciones entregadas al oficial de Seguridad de la información	
4.3	Términos y condiciones laborales		
4.3.1	EJECUCIÓN: Acuerdo de confidencialidad o no-divulgación, antes de que los empleados, contratistas y usuarios de terceras partes, tengan acceso a la información firmado	Acuerdos a firmar con las firmas de aprobación del mismo.	
4.4	Responsabilidades de la dirección a cargo del funcionario		
4.4.1	(P) Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles	Documento de aceptación por el usuario, inducción.	
4.8	Devolución de activos		
4.8.1	EJECUCIÓN: Proceso de terminación del contrato laboral, para incluir la devolución de software, documentos corporativos y los equipos formalizados	Documento de paz y salvo o desvinculación	
4.9	Retiro de los privilegios de acceso		
4.9.1	EJECUCIÓN: Privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc., retirados	Procedimiento de privilegios de acceso aprobado y socializado	

(P) Hitos prioritarios
Ejecución: Hitos de cumplimiento de los documentos normativos

HITOS A EVALUAR
DIRECCIÓN DE SEGURIDAD INFORMÁTICA

	5 SEGURIDAD FÍSICA Y DEL ENTORNO		
5.1	Perímetro de la seguridad física		
5.1.2	EJECUCIÓN: Perímetros de seguridad definidos y documentados	Planos o documentos definidos	
5.1.6	EJECUCIÓN: Ambientes aislados de procesamiento de información	Verificación en sitio	
5.2	Controles de acceso físico		
5.2.1	(P) Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida	Políticas y procedimientos aprobados	
5.2.2	(P) Implementar el uso de una identificación visible para todo el personal y visitantes, quienes deberán ser escoltados por una persona autorizada para el tránsito en las áreas restringidas	Políticas y procedimientos aprobados verificación en sitio	
5.3	Seguridad de oficinas, recintos e instalaciones		
5.3.1	(P) Proteger las instalaciones claves de tal manera que se evite (P) Proteger las instalaciones claves de tal manera que se evite el acceso al público	Documento de designación de sitios clave	
5.3.2	(P) Ubicar las impresoras, copiadoras, etc., en un área protegida	Planos o documentos definidos	
5.3.3	EJECUCIÓN: Reglamentos y las normas en materia de sanidad y seguridad aplicadas.	Memos informativos y socializados, aceptación de los usuarios de la capacitación, controles efectuados	
5.4	Protección contra amenazas externas y ambientales		
5.4.1	(P) Realizar mantenimientos de las instalaciones eléctricas y UPS	Plan de mantenimiento	
5.4.2	(P) Realizar mantenimientos en los sistemas de climatización y ductos de ventilación	Informes de mantenimiento documentados	
5.4.5	EJECUCIÓN: Equipo apropiado contra incendios suministrado y colocado	Revisión en sitio, y verificación del mapa	
5.7	Ubicación y protección de los equipos		
5.7.1	(P) Establecer directrices para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información	Políticas y procedimientos aprobados y difundidos	
5.7.4	EJECUCIÓN: Condiciones ambientales de temperatura y humedad monitoreadas	Revisión en sitio de mecanismos implementados	
5.8	Servicios de suministro		
5.8.1	(P) Tener un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones críticas de los servicios informáticos de la institución	Verificación en sitio Informes de mantenimiento	
5.9	Seguridad del cableado		
5.9.1	(P) Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc.	Planos	
5.9.5	EJECUCIÓN: Cables identificados y rotulados	Documento de respaldo y verificación en sitio	
5.9.6	EJECUCIÓN: Acceso a los módulos de cableado de conexión (patch panel) y cuartos de cableado controlados	Documento de respaldo- procedimiento-bitácoras y verificación en sitio	
5.10	Mantenimiento de los equipos		
5.10.5	EJECUCIÓN: Gestión de mantenimientos planificados	Informes internos y por parte del proveedor.	

(P) Hitos priorizados

HITOS A EVALUAR
DIRECCIÓN DE SEGURIDAD INFORMÁTICA

6 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
6.1	Documentación de los procedimientos de Operación		
6.1.1	(P) Documentar los contactos de soporte, necesarios en caso de incidentes	Documento de respaldo aprobado	
6.1.3	EJECUCIÓN: Proceso de respaldo y restauración de la información documentado	Informe de ejecución de respaldo y pruebas de restauración	
6.1.7	EJECUCIÓN: Procedimientos para reinicio y recuperación del sistema en caso de fallas documentados	Informes de ejecución de los procedimientos de recuperación. Plan de pruebas	
6.2	Gestión del cambio		
6.2.1	EJECUCIÓN: Registro de cambios significativos identificados	Evidencia del cumplimiento del procedimiento de control de cambios	
6.4	Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción		
6.4.6	EJECUCIÓN: Perfiles de usuario para las diferentes instancias o ambientes definidos	Evidencia, segregación de funciones a nivel de sistemas operativos y sistemas de información usados	
6.6	Monitoreo y revisión de los servicios, por terceros.		
6.6.3	(P) Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado	Documento de respaldo, informe -reporte	
6.6.4	EJECUCIÓN: Sistemas sensibles o críticos que convenga tener dentro o fuera de la institución identificados	Documentación de los diagramas	
6.8	Gestión de la capacidad		
6.8.1	(P) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos	Documentos de mejora de capacidad	
6.10	Controles contra código malicioso		
6.10.10	EJECUCIÓN: Filtrado de: virus, spam, programas maliciosos (malware), en el perímetro externo contratado	Informes de las herramientas que cumplen la función indicada	
6.12	Establecer controles criptográficos para autenticar de forma única el código móvil		
6.12.1	(P) Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información	Procedimientos documentados y aprobados	
6.12.2	(P) Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención	Procedimiento documentado y aprobado	
6.12.3	(P) Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución	Procedimiento documentado y aprobado	
6.12.5	EJECUCIÓN: Almacenamiento de respaldos establecido	Verificación de los respaldos almacenados.	
6.12.8	EJECUCIÓN: Información confidencial por medio de encriptación protegida	Procedimiento e informes de ejecución.	
6.13	Controles de la redes		
6.13.5	EJECUCIÓN: Esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva dispuesta	Esquemas de red documentados	
6.14	Seguridad de los servicios de la red		
6.14.1	(P) Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red	Documentos de respaldo de los mecanismos seleccionados	
6.14.2	(P) Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.	Documento de respaldo- informe-procedimiento	
6.19	Políticas y procedimientos para el intercambio de información		
6.19.2	EJECUCIÓN: Procedimientos para detección y protección contra programas maliciosos, cuando se utilizan comunicaciones electrónicas, definidas.	Evidencia de la herramienta o mecanismos documentados	
6.23	Sistemas de información del negocio		

(P) Hitos prioritarios
Ejecución: Hitos de cumplimiento de los documentos normativos

HITOS A EVALUAR
DIRECCIÓN DE SEGURIDAD INFORMÁTICA

6.23.6	EJECUCIÓN: Personal con acceso a los sistemas, categorizado.	Registro de usuarios y perfiles asignado (reporte o bitácora)	
6.23.7	EJECUCIÓN: Estado de las cuentas de usuario identificados.	Reporte de los usuarios, a nivel de S.O. y de sistemas de información	
6.26	Registros de auditorías		
6.26.1	(P) Registrar los accesos y tipos de acceso	Política de control de accesos	
6.26.10	EJECUCIÓN: Uso de privilegios registrados.	Reporte de privilegios, roles o grupos de acceso asignados	
6.26.11	EJECUCIÓN: Uso de las aplicaciones y Sistemas registrados.	Bitácora o control de los permisos asignados.	
6.26.2	(P) Registrar las direcciones y protocolos de red	Política de control de accesos	
6.26.3	(P) Definir alarmas originadas por el sistema de control de acceso	Política de control de accesos	
6.26.4	(P) Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS)	Documento de respaldo- procedimiento	
6.26.5	EJECUCIÓN: Nombre de usuario registrado.	Evidencia del control	
6.26.9	EJECUCIÓN: Cambios de la configuración registrados.	Bitácora, mecanismo de control de cambios	
6.27.1	(P) Registrar los accesos autorizados, incluyendo	Política de control de accesos	
6.27.1.1	identificación del ID de usuario	Bitácora de registro de incidente	
6.27.1.2	Fecha y hora de eventos clave	Bitácora de registro de incidente	
6.27.1.3	Tipos de evento	Bitácora de registro de incidente	
6.27.1.4	Archivos a los que se han tenido acceso;	Bitácora de registro de incidente	
6.27.1.5	Programas y utilitarios utilizados;	Bitácora de registro de incidente	
6.27.2	(P) Monitorear las operaciones privilegiadas	Política de control de accesos	
6.27.2.1	Uso de cuentas privilegiadas;	Bitácora de registro de incidente	
6.27.2.2	Encendido y detección del sistema;	Bitácora de registro de incidente	
6.27.2.3	Acople y desacople de dispositivos de entrada;	Bitácora de registro de incidente	
6.27.3	(P) Monitorear intentos de acceso no autorizados	Política de control de accesos	
6.27.3.1	Acciones de usuario fallidas o rechazadas;	Bitácora de registro de incidente	
6.27.3.2	Violación de la política de acceso y notificaciones de firewalls y gateways;	Bitácora de registro de incidente	
6.27.3.3	Alertas de los sistemas de detección de intrusos;	Bitácora de registro de incidente	
6.27.4	(P) Revisar alertas o fallas del sistema	Política de control de accesos	
6.27.4.1	Alertas y/o mensajes de consola;	Bitácora de registro de incidente	
6.27.4.2	Excepciones de registro del sistema;	Bitácora de registro de incidente	
6.27.4.3	Alarmas de gestión de red;	Bitácora de registro de incidente	
6.27.4.4	Alarmas del sistema de control de acceso;	Bitácora de registro de incidente	

(P) Hitos prioritarios
Resultado: Hitos de cumplimiento de los documentos normativos

HITOS A EVALUAR
DIRECCIÓN DE SEGURIDAD INFORMÁTICA

6.27.5	EJECUCIÓN: Cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema, revisados.	Mecanismos de control automáticos o manuales para los cambios de configuración de	
6.29	Violación de la política de acceso y notificaciones de firewalls y gateways;		
6.29.3	(P) Registrar la cuenta de administrador y operador que estuvo involucrado	Política de control de accesos	
6.30	Registro de fallas		
6.30.1	(P) Revisar los registros de fallas o errores del sistema	Revisión del LOGS	
6.30.3	(P) Asegurar que el registro de fallas esté habilitado	Revisión del LOGS	
6.31	Sincronización de relojes		
6.31.1	EJECUCIÓN: Relojes de sistemas de procesamiento de información pertinentes con una fuente de tiempo exacta, sincronizados.	Evidencia de la Sincronización de relojes (NTP)	
6.31.4	EJECUCIÓN: Configuración correcta de los relojes para la exactitud de los registros garantizado.	NTP	
7. CONTROL DE ACCESO			
7.1	Política de control de acceso		
7.1.1	EJECUCIÓN: Accesos de los usuarios a los sistemas de información gestionados.	Informes de control de accesos	
7.1.3	EJECUCIÓN: Autorizadores de los permisos de acceso a la información definidos.	lista de Administradores, Delegación como administrador.	
7.3	Gestión de privilegios		
7.3.1	EJECUCIÓN: Asignación de privilegios a través de un proceso formal de autorización, controlado.	Formularios o documentos de control	
7.3.2	EJECUCIÓN: Usuarios y privilegios asociados con cada servicio, identificados.	reporte de usuarios y privilegios de acceso revisados.	
7.4	Gestión de contraseñas para usuarios		
7.4.1	(P) Establecer un proceso formal para la asignación y cambio de contraseñas	Procedimiento documentado y aprobado	
7.5	Revisión de los derechos de accesos de los usuarios		
7.5.1	EJECUCIÓN: Depuraciones respectivas de los accesos de los usuarios, realizados.	Informe de validación de usuarios y privilegios de acceso revisados.	
7.6	Uso de contraseñas		
7.6.1	(P) Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados	Política de control de accesos	
7.6.2	(P) Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar; es decir, que cumplen una complejidad media y alta	Política de control de accesos, Políticas configuradas en el AD y en los sistemas	
7.6.3	(P) Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables	Política de control de accesos	
7.6.4	(P) Controlar el cambio periódico de contraseñas de los usuarios	Política de control de accesos	
7.6.5	(P) Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la información	Política de control de accesos	
7.7	Equipo de usuario desatendido		
7.7.1	(P) Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave	Política de control de accesos	
7.10	Autenticación de usuarios para conexiones externas		
7.10.1	(P) Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR)	Documentación de respaldo - Políticas de acceso remoto	
7.10.2	EJECUCIÓN: Mecanismo diferenciado para la autenticación de los usuarios que requieren conexiones remotas, realizado.	Evidencia de cumplimiento de la implementación de mecanismos de acceso seguro	

(P) Hitos prioritarios
Ejecución: Hitos de cumplimiento de los documentos normativos

HITOS A EVALUAR
DIRECCIÓN DE SEGURIDAD INFORMÁTICA

7.11	Identificación de los equipos en las redes		
7.11.2	EJECUCIÓN: Comunicación permitida desde un equipo o lugar específico, controlada.	Verificación en sitio, reglas de acceso remoto	
7.12	Protección de los puertos de configuración y diagnostico remoto		
7.12.1	(P) Los puertos, servicios (ej., ftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados	Documentación de respaldo - Políticas de acceso remoto - Políticas de firewall	
7.15	Control del enrutamiento en la red		
7.15.1	(P) Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución	Documentación de respaldo - Políticas de acceso remoto - Políticas de firewall	
7.16	Procedimiento de registro de inicio seguro		
7.16.1	(P) Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada	Política de control de accesos	
7.16.2	(P) Llevar un registro de definición para el uso de privilegios especiales del sistema	Política de control de accesos AD y Sistemas de información	
7.17	Identificación y autenticación de usuarios		
7.17.3	(P) Evitar el uso de usuarios genéricos	Política de control de accesos	
7.17.4	(P) Utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación	Política de control de accesos	
7.17.5	EJECUCIÓN: Actividades de usuarios regulares desde cuentas privilegiadas, evitadas.	Custodios de los Usuarios privilegiados definidos y validacion del procedimiento	
7.17.6	EJECUCIÓN: Políticas de acceso para identificación de usuario definidas.	Lista de usuarios con el responsable	
7.18	Sistema de gestión de contraseñas		
7.18.1	(P) Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible	documentos de respaldo para el control de accesos	
7.18.2	(P) Controlar el cambio de contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad	Política de control de accesos	
7.18.3	(P) Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión	Política de control de accesos	
7.18.4	EJECUCIÓN: Procedimiento formal para la administración y custodia de las contraseñas de acceso, generado.	validacion del procedimiento de control de accesos	
7.18.6	EJECUCIÓN: Contraseñas en formatos protegidos, almacenadas y restringidas.	validacion del procedimiento de control de accesos	
7.26	Trabajo remoto		
7.26.10	EJECUCIÓN: Trabajo remoto al personal, permitido.	Documentación de respaldo - Formularios, revisiones de acceso	
8	ADQUISICIÓN, DESARROLLO, Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
8.1	Análisis y especificaciones de los requerimientos de seguridad		
8.1.1	(P) Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.	Documento de respaldo - procedimiento	
8.1.2	(P) Definir los controles apropiados, tanto automatizados como manuales	Informes y documentación de respaldo de la ejecución de controles	

HITOS A EVALUAR
DIRECCIÓN DE SEGURIDAD INFORMÁTICA

8.9	Protección de los datos de prueba del sistema		
8.9.10	EJECUCIÓN: Procedimientos para la gestión de excepciones en los casos que se requiera realizar modificaciones directamente sobre la base de datos, establecidos.	Formularios o documentación de respaldo de acuerdo a la política	
8.9.3	EJECUCIÓN: Autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba, solicitada.	Formularios o documentación de respaldo de acuerdo a la política	
8.9.5	EJECUCIÓN: Datos críticos que deberán ser modificados o eliminados del ambiente de pruebas, identificados.	Formularios o documentación de respaldo de acuerdo a la política o procedimiento	
8.9.6	EJECUCIÓN: Procedimientos de control de acceso que existen en la base de producción, aplicados.	Formularios o documentación de respaldo de acuerdo a la política o procedimiento	
8.16	Control de las vulnerabilidades técnicas		
8.16.11	EJECUCIÓN: Controles de acceso; adaptados y agregados, por ejemplo, cortafuegos (firewalls), en las fronteras de la red.	Evidencia de la implementación de las herramientas	
	9 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN		
9.1	Reporte sobre los eventos de seguridad de la información		
9.1.1	(P) Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente	Procedimientos documentados y aprobados	
9.1.2.1	(P) Identificar el incidente	Procedimiento control de incidentes	
9.1.2.10	(P) Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto	Procedimiento control de incidentes	
9.1.2.2	(P) Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente	Procedimiento control de incidentes	
9.1.2.3	(P) Notificar al Oficial de Seguridad de la Información de la Institución	Procedimiento control de incidentes	
9.1.2.4	(P) Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad	Procedimiento control de incidentes	
9.1.2.5	(P) Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultanea	Procedimiento control de incidentes	
9.1.2.6	(P) Realizar un diagnóstico inicial, determinando mensajes de error producidos; identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas	Procedimiento control de control de incidentes o eventos de los servidores	
9.1.2.7	(P) Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes.	Procedimiento control de incidentes	
9.1.2.8	(P) Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente	Procedimiento control de incidentes	
9.1.2.9	(P) Resolver y restaurar el servicio afectado por el incidente debido a la par de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes	Procedimiento control de incidentes	
9.3	Responsabilidades y procedimientos		
9.3.1	EJECUCIÓN: Procedimiento para la gestión de incidentes y monitoreo establecido.	Formatos, bitácoras del procedimiento	
9.3.4	EJECUCIÓN: Acciones correctivas para evitar la recurrencia del incidente, planificados e implementadas.	Informes de acciones tomadas ante la ocurrencia de un incidente	
9.3.7	EJECUCIÓN: Pistas de auditoría y toda la evidencia relacionada con el incidente, recolectada y asegurada.	Revisión en sitio de mecanismos implementados	
	11 CUMPLIMIENTO		
11.8	Verificación del cumplimiento técnico		
11.8.1	Verificar el cumplimiento técnico bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia, y/o con la ayuda de herramientas automáticas que generen un informe técnico para la interpretación posterior por parte del especialista técnico.	Informes técnicos de la operación de las herramientas de control	
11.8.2	EJECUCIÓN: Evaluaciones de vulnerabilidad o pruebas de penetración aplicadas.	Documentación de respaldo - análisis de vulnerabilidad, pen test externos	
11.8.5	EJECUCIÓN: Pruebas de penetración y evaluaciones de la vulnerabilidad, ejecutadas o contratadas.	Documentación de respaldo - evidencia	

(P) Hitos prioritarios
Ejecución: Hitos de cumplimiento de los documentos normativos