SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

PROCESO DE "CERTIFICACIÓN DIGITAL"

Gerencia de Registros de Certificación Digital – GRCD

CONCEPTOS BÁSICOS

INFORMACION

Es un conjunto organizado de datos procesados, que constituyen un **mensaje** ...

AREA	Nº	NOMBRE Y APELLIDO		ROLES	TIPO DE ROL	RELAC. LABORAL
GCRD	1	Ricardo Javier Enrique Saavedra Mavila		Gerente	Contrato / SIG / Acreditación	Planilla
	2	Ana Lidia del Carmen Ampuero Paiss		Coordinador General de Usabilidad y Entrenamiento	Contrato	CAS
	3	Alfredo Rafael Gallo Montani		Especialista	Contrato	CAS
	4	Miluzka Paola Cazaz Caycho		Secretaria de Gerencia	Contrato	CAS
	-	----------	P	Técnico en Gestión de Proyectos		
	-	----------	P	Supervisor de Desarrollo Continuo		
	5	Sergio Ozcar Gonzalez Bacca		Técnico en Control de Accesos	Contrato	CAS
	6	Mareille Erika Astolfi Galván		Oficial de Privacidad de Datos	Contrato	CAS
			P	Asesor Legal 6800		
	-	----------	P	Especialista en Identidad Digital		CAS
	7	Tany Villalba Villalba		Jefe de la ECERNEP	Contrato / SIG / Acreditación	CAS
			P1	Administrador de Servicios PKI (SGCD) 5000	SIG / Acreditación	
	8	Jessica del Pilar Huerta Poma		Analista Estadístico	Contrato	CAS
	9	Joel Martín Visurraga Agüero		Analista de Acceso Web	Contrato	CAS
	-	----------	P	Auxiliar Administrativo		
	-	----------	P	Supervisor de Servicios en Certificación Digital		
	10	Edson Alberto Alvarez Navarro		Técnico Estadístico	Contrato	CAS
	11	Edith del Rocio Igue Llave		Supervisión de verificación de firmas	Contrato	CAS
	12	Delicia Brionez Linarez		Coordinador de Seguridad de Información	Contrato / SIG	CAS
			P	Oficial de Seguridad de Información 5500	SIG / Acreditación	
			P	Analista de Control Interno en Certificación Digital 6200		
	13	Alvaro Ernesto Cuno Parari		Especialista en Valor Añadido de la ECERNEP		CAS
	14	Julio Cézar Nuñez Ponce		Especialista Legal en Protección de Datos	Contrato	CAS

ACTIVO

Es algo que tenga **valor** para la Organización...

ACTIVO DE INFORMACIÓN

Son los **recursos** del sistema de **información** y su **entorno**, que son necesarios para que la organización funcione correctamente y alcance los **objetivos del negocio**.

SEGURIDAD DE LA INFORMACIÓN

Es básicamente…. «la Preservación de la **Confidencialidad**, **Disponibilidad** **e** **Integridad** de la Información…..»

CONFIDENCIALIDAD

La información sólo puede ser accedida por personas, entidades o procesos autorizados.

SI

NO

INTEGRIDAD

Característica que indica que los datos o un documento electrónico no ha sido alterado (en forma no autorizada) desde su transmisión hasta su recepción.

SI

NO

DISPONIBILIDAD

La información puede ser accedida por todas las personas autorizadas cuando lo requieren.

SI

NO

INCIDENTE

Es cualquier evento inesperado o no deseado que tiene una probabilidad alta de comprometer las operaciones de negocio y amenazar la confidencialidad, disponibilidad e integridad de la información.

Robo de información

Acceso no autorizado a archivos físicos

Disturbios sociales

NORMATIVA

- Norma ISO 27001.
- Guías de Acreditación – INDECOPI.
- Política de Seguridad de la Información del RENIEC.
- Política de Seguridad de la Información – Certificación Digital (Versión 5).

POLÍTICA DE SEGURIDAD DEL RENIEC

EL REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL, TIENE COMO ACTIVO PRINCIPAL LA INFORMACIÓN DE TODOS LOS PERUANOS REGISTRADOS E IDENTIFICADOS; PRESERVA SU CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD EN CADA UNO DE LOS PROCESOS A TRAVÉS DE INCORPORACIÓN DE CONTROLES, PROCEDIMIENTOS Y METODOLOGÍAS DEFINIDAS, PERSONAL CAPACITADO, TECNOLOGÍA ADECUADA Y MECANISMOS DE MEJORA CONTINUA EN EL CUMPLIMIENTO DEL MARCO LEGAL VIGENTE Y ESTÁNDARES INTERNACIONALES.

POLÍTICA DE SEGURIDAD "CERTIFICACIÓN DIGITAL"

OBJETIVO:

ESTABLECER EL MARCO GENERAL Y LOS LINEAMIENTOS PARA LA SEGURIDAD DE LA INFORMACIÓN PROVENIENTE DEL PROCESO DE CERTIFICACIÓN DIGITAL, A FIN DE GARANTIZAR LA DISPONIBILIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN DURANTE EL DESARROLLO DE LAS OPERACIONES Y ACCIONES QUE SE REALIZAN.

ALCANCE

AREA DE ALCANCE:

LA PRESENTE POLÍTICA ASÍ COMO LAS REGLAS O NORMAS Y PROCEDIMIENTOS QUE SE DERIVEN DE ELLA, SERÁN DE CUMPLIMIENTO OBLIGATORIO PARA EL PERSONAL INVOLUCRADO EN EL PROCESO DE CERTIFICACIÓN DIGITAL, ASÍ COMO DEL PERSONAL DE LOS DISTINTOS ÓRGANOS DEL RENIEC QUE PARTICIPEN EN LA EJECUCIÓN DE LAS ACTIVIDADES QUE SON PARTE DEL PROCESO DE CERTIFICACIÓN DIGITAL.
TAMBIÉN ES DE CUMPLIMIENTO OBLIGATORIO PARA LOS PROVEEDORES DEL SERVICIO O TERCEROS

SERVICIOS DE ALCANCE:

ECERNEP–RENIEC: COMPRENDE LOS SERVICIOS DE EMISIÓN Y CANCELACIÓN DE CERTIFICADOS DIGITALES DE AUTORIDAD INTERMEDIA, Y PARA PRESTADOR DE SERVICIOS DE VALOR AÑADIDO.

ECEP–RENIEC: COMPRENDE LOS SERVICIOS DE EMISIÓN Y CANCELACIÓN DE CERTIFICADOS DIGITALES, ADMINISTRACIÓN DE SU CICLO DE VIDA, ADMINISTRACIÓN DE REPOSITORIO Y CONSULTA DE ESTADO DE CERTIFICADOS DIGITALES.

EREP–RENIEC: COMPRENDE LOS SERVICIOS DE EMISIÓN, CANCELACIÓN Y ENTREGA DE CERTIFICADOS DIGITALES, ASÍ COMO LA PROTECCIÓN DE LOS DOCUMENTOS SUSTENTATORIOS Y SU ARCHIVO YA SEAN EN FORMATO FÍSICO O DIGITAL.

OTROS SERVICIOS RELACIONADOS CON CERTIFICACIÓN DIGITAL COMO SELLADO DE TIEMPO Y OTROS.

RESPONSABILIDADES

Responsables de implementar la Política de Seguridad

Los órganos del RENIEC involucrados en el proceso de certificación digital, en los aspectos que les correspondan.

Responsables de supervisar el cumplimiento de la Política de Seguridad

- El Oficial de Seguridad de Información - SGREGD.
- Cada Gerente y sub Gerente de los órganos del RENIEC involucrados en el proceso de certificación digital.
- Los Supervisores de Seguridad de Información y Privacidad de Datos.

CONTENIDO DE LA POLITICA

POLITICA GENÉRICA:

EL RENIEC RECONOCE COMO ACTIVO PRINCIPAL DEL PROCESO DE CERTIFICACIÓN DIGITAL A LA INFORMACIÓN RESULTANTE DEL PROCESO Y QUE PERMITE LA GENERACIÓN DE LA IDENTIDAD DIGITAL; EN TAL SENTIDO, SE EFECTÚA EL ANÁLISIS Y EVALUACIÓN DE LOS RIESGOS, LA APLICACIÓN DE CONTROLES Y LA TOMA DE CONCIENCIA EN EL PERSONAL, DE MODO QUE NOS PERMITA MANTENER LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA MISMA, ASÍ COMO DAR CUMPLIMIENTO A LOS REQUISITOS TÉCNICOS Y LEGALES VIGENTES.

POLÍTICAS ESPECÍFICAS:

m. Administración de Claves

a. Organización

l. Medios de almacenamiento

b. Evaluación de riesgos

k. Auditoria y detección de intrusiones

Información

c. Control de acceso

j. Respuesta a incidentes

d. Seguridad de Personal

i. Plan de Contingencia

e. Seguridad Física

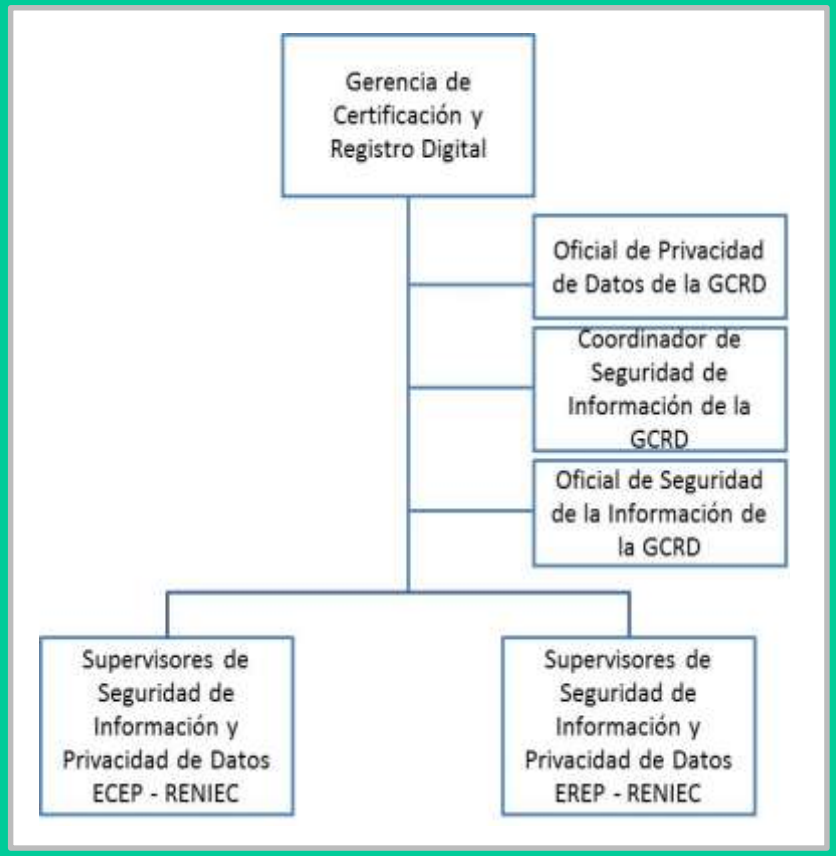
h. Control de cambios y configuración

f. Seguridad de comunicaciones y redes

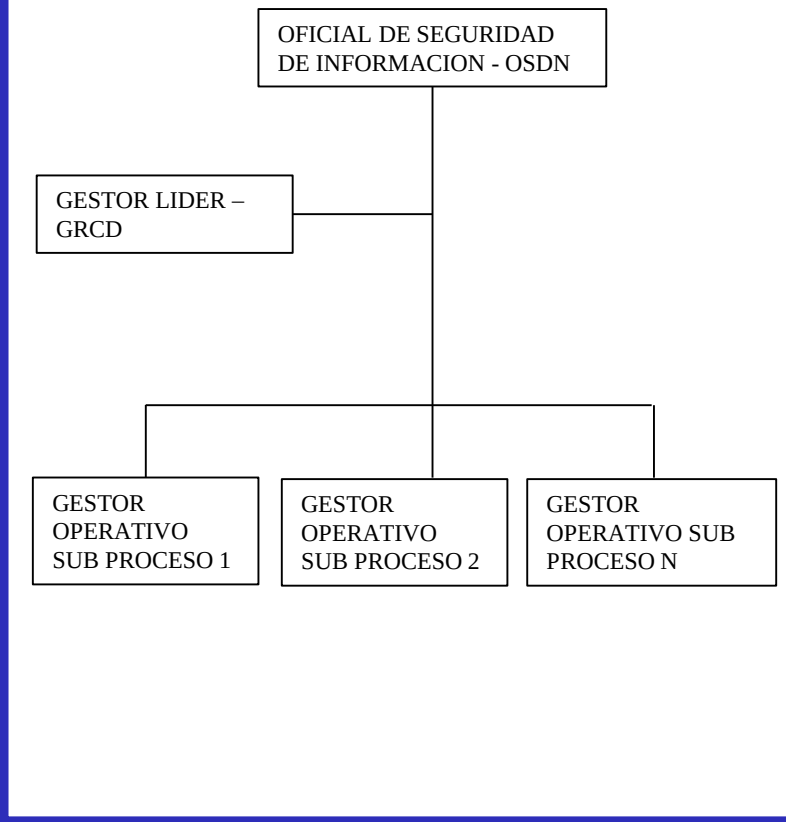
g. Mantenimiento de equipo y su desecho

Organización de la Seguridad de la Información

ACREDITACIÓN



SGSI - PCD



GRCD

POLÍTICA DE SEGURIDAD

- Inventario de Activos.
- Valoración de los activos.
- Identificación de amenazas y vulnerabilidades de los activos críticos.
- Evaluación del impacto de los riesgos.
- Tratamiento de los riesgos.

Evaluación de Riesgos

- Controles de Acceso para protección de información sensible (física y electrónica).
- Controles de Acceso a los ambientes donde se encuentra la información sensible.

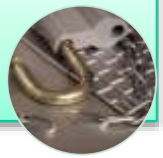
Control de Acceso

- Métodos de verificación de Datos y Antecedentes.
- Establecer Roles.
- Responsabilidades del personal.
- Capacitación y Sensibilización.

Seguridad de Personal

- Seguridad física y ambiental para prevenir accesos no autorizados y accidentes en los ambientes en que se procesa o resguarda información confidencial o sensible.

Seguridad Física



- Medidas de seguridad de comunicaciones y redes tanto internas como externas.
- La ECEP-RENIEC debe asegurar que los datos disponibles en los repositorios públicos se encuentren protegido.

Seguridad de Comunicaciones y Redes

POLÍTICA DE SEGURIDAD

- Reemplazo, manipulación y desecho de equipos.
- Antes de su desecho o reúso se revisará que toda información sensible haya sido removida.
- Plan de mantenimiento preventivo de equipos.

Mantenimiento de equipo y su desecho

- Aprobación de cambios a los sistemas.
- Previo al cambio se efectuará un análisis de impacto a los sistemas y procesos, comunicando el cambio a todos los involucrados.
- Modificaciones se efectúen de preferencia, fuera del horario de atención a los clientes o en horas de menor demanda.

Control de Cambios y Configuración

- Aplicación de Plan de Contingencias, general o para tareas especificas.
- Pruebas periódicas del Plan de Contingencias y actualización del Plan.
- Roles dentro del Plan de Contingencias.

Planificación de Contingencias

- Auditorías internas semestrales o según lo definido.
- Auditorias anuales de INDECOPI.
- También pruebas para detección de intrusos y vulnerabilidades.

Auditoria y detección de Intrusiones

- Respaldo y recuperación, se ha establecido de acuerdo a los procedimientos de la Planta PKI.
- Almacenamiento en un local externo.

Medios de Almacenamiento

POLÍTICA DE SEGURIDAD

- Que debemos reportar:
- Incidentes que afecten la disponibilidad de las operaciones.
- Incumplimiento a las disposiciones SI establecidas por el RENIEC.
- Alguna vulnerabilidad o evento que pueda generar una situación de riesgo.

Gestión de incidentes

- Asegurar la confidencialidad de las claves criptográficas e implementar para su protección los controles requeridos de acuerdo al nivel de seguridad acreditado.

Administración de Claves

DOCUMENTOS DEL SISTEMA Y SU ACCESO

LOS DOCUMENTOS DEL SGSI-PCD, SE ENCUENTRAN ARCHIVADOS EN LOS SIGUIENTES MEDIOS**:**

- **EN LA INTRANET (LINK DOCUMENTOS NORMATIVOS):** LOS DOCUMENTOS QUE SE RIGEN POR LA DIRECTIVA DI-200-GPP/001 COMO: DI, GP, GS, NAI, IN.

- **EN UN REPOSITORIO VIRTUAL DE LA PLANTA PKI:** LOS DOCUMENTOS DE CARÁCTER TÉCNICO.

- **POR LOS GESTORES LIDERES Y OPERATIVOS:** LOS DOCUMENTOS ADMINISTRATIVOS O DE GESTIÓN RELACIONADOS CON EL SISTEMA.

Gracias por su atención