certificados-digitales.pe

Certificados Digitales.pe

ENTIDAD DE REGISTRO

POLÍTICA DE SEGURIDAD

VERSIÓN 1.1

dnp corp

Hardware - Software - Network - Recovery - Energy

ÍNDICE

1. TRATAMIENTO DEL DOCUMENTO

CONTROL DE ACTUALIZACIONES				
VERSIÓN	**FECHA**	**DESCRIPCIÓN**	**REALIZADO POR**	**CALIDAD DE APROBADOR**
1.0	12/10/2018	Generación de documentos	Operador de registro	Responsable de la ER
1.1	21/12/2018	Actualización de documentos	Operador de registro	Responsable de la ER

1.1. MANTENIMIENTO DEL DOCUMENTO

Se requiere mantenimiento y/o revisión de este documento cada vez que varíen algunas de las fases del proceso, las funciones del personal involucrado o las herramientas utilizadas en el mismo.

1.2. VALIDEZ

Hasta su actualización. Cualquier copia local se considera una copia no controlada. Es responsabilidad de quienes utilizan copias no controladas verificar su nivel de actualización.

1.3. TRATAMIENTO Y CONFIDENCIALIDAD

Documento de uso público, pudiendo acceder a él los empleados de la organización, clientes, auditores externos e internos en proceso de inspección.

1.4. DISTRIBUCIÓN

Distribución al público a través de la web de la ER DNP CORP.

2. INTRODUCCIÓN

DNP CORP S.A.C. es una persona jurídica constituida en el Perú que opera como Entidad de Registro o Verificación (ER) dentro del marco de la Infraestructura Oficial de Firma Electrónica (IOFE). En tal condición, ejerce sus funciones adscrita a una Entidad de Certificación (EC) acreditada por la autoridad administrativa competente (INDECOPI), así como a otras entidades homólogas con las cuales mantenga convenios interinstitucionales vigentes. Su objeto operativo principal consiste en la gestión y ejecución de los procesos de recepción, validación y trámite de solicitudes para la emisión y revocación de certificados digitales, dirigidos a personas naturales y jurídicas, garantizando el cumplimiento de los estándares de seguridad establecidos por la Entidad de Certificación vinculada y la normativa nacional vigente.

3. OBJETIVO DE DNP CORP S.A.C. COMO ENTIDAD DE REGISTRO O VERIFICACIÓN

Garantizar el máximo nivel de confiabilidad y certeza en la comprobación de la identidad de los solicitantes que requieran servicios de emisión, reemisión o revocación de certificados digitales. Para tal fin, la organización implementa procesos estrictos de registro, validación y verificación de la autenticidad de la información y documentación técnica o legal provista, con carácter previo a la remisión de la conformidad y autorización a la Entidad de Certificación (EC). Asimismo, el objetivo se extiende a asegurar el cumplimiento irrestricto de las normas, políticas de seguridad, declaraciones de prácticas y directrices internacionales dictadas por las respectivas EC con las cuales se mantenga un convenio operativo vigente.

4. PARTICIPANTES

- **Entidades de Certificación**: Entidades que genera los certificados digitales, de la cual DNP CORP S.A.C. utiliza los servicios de registro.
  La EC vinculada, como Entidad de Certificación acreditada, brinda el servicio web de registro, mediante el cual DNP CORP S.A.C. gestionará la aprobación de las solicitudes de los servicios de certificación digital, por lo que la responsabilidad de la disponibilidad y seguridad de estos sistemas depende de EC vinculada. La información respecto a la Entidad de Certificación vinculada, así como sus Políticas de Certificación, sus Declaraciones de Prácticas y respectivos convenios se encuentran publicados en la dirección web de la EC vinculada.

- **Entidades de Registro o Verificación:** DNP CORP S.A.C. reside en el Perú y se somete ante el proceso de acreditación del INDECOPI. Las comunicaciones entre la ER y la EC vinculada. se realizan vía web de manera ininterrumpida, según los niveles de disponibilidad y recuperación brindados y declarados por cada EC. La ER dispone de más de un proveedor para acceder a los sistemas en casos de corte del servicio de Internet. La disponibilidad del servicio web de registro es provista por cada EC y es responsabilidad de la EC vinculada el mecanismo de contingencia utilizado.

- **Titulares de Certificados:** La comunidad de usuarios definidos como titulares de los certificados digitales será definida según lo establecido en la Política de Certificación y Declaración de Prácticas de la EC con la cual se tenga convenio. DNP CORP S.A.C. brinda servicios a personas jurídicas y naturales.

- **Terceros que confían:** Los terceros que confían son personas naturales o jurídicas que confían en el contenido y la aplicación de un certificado digital. En este sentido, los terceros que confían pueden ser todas aquellas personas naturales y jurídicas que requieren evaluar la validez de un certificado para proceder con sus respectivas transacciones electrónicas, incluyendo entidades de otras infraestructuras además de la IOFE.

La comunidad de usuarios definidos como terceros que confían dependerá de lo establecido en la Política de Certificación y Declaración de Prácticas de la EC vinculada. https://www.camerfirma.com/practicas-de-certificacion-ac-camerfirma-cps-dpc/

5. GLOSARIO, ABREVIACIONES Y ACRÓNIMOS

ENTIDADES DE CERTIFICACIÓN	**EC**: Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
ENTIDADES DE REGISTRO O VERIFICACIÓN	**ER**: Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
DECLARACIÓN DE PRÁCTICAS DE REGISTRO	**RPS**: Conjunto de declaraciones sobre políticas y prácticas de la Entidad de Registro, que sirve para comunicar el cumplimiento legal y regulatorio a los suscriptores y terceros que confían.
OPERADOR DE REGISTRO	Persona responsable de representar a DNP CORP S.A.C. en calidad de ER en las actividades de recepción, validación y procesamiento de solicitudes.
PRÁCTICAS DE REGISTRO	Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.
ROLES DE CONFIANZA	Roles que tienen acceso a la información crítica de las operaciones de registro de DNP CORP S.A.C. en calidad de ER.

SUSCRIPTOR	Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.
TERCERO QUE CONFÍA	Se refiere a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.
TITULAR	Es la persona jurídica a quien se le atribuye de manera exclusiva un certificado digital.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DNP CORP S.A.C., en su calidad de Entidad de Registro (ER), establece como objetivo fundamental garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información gestionada en los procesos de registro y validación de identidad. Para ello, la alta dirección se compromete a gestionar eficazmente los riesgos de seguridad de la información mediante la implementación de controles, políticas y estándares estrictos. Estas medidas regulan las actividades críticas de las operaciones de registro realizadas por el personal interno y terceros subcontratados, asegurando el estricto cumplimiento de las obligaciones legales, regulatorias y contractuales aplicables a la IOFE.

7. GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

DNP CORP S.A.C. adopta un enfoque proactivo para la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar a los activos de información de la Entidad de Registro. Para ello, se establece un proceso continuo de gestión de riesgos basado en la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de

Información), en armonía con los estándares internacionales de seguridad de la información aceptados por el regulador.

Este proceso se ejecuta de manera periódica y ante cualquier cambio significativo en la infraestructura o procesos con el objetivo de mantener los riesgos en niveles aceptables para la organización y garantizar la continuidad y confianza del servicio de registro.

8. SEGURIDAD FÍSICA

8.1. UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

La ubicación y diseño de las instalaciones de DNP CORP S.A.C. en calidad de Entidad de Registro (ER), debe prever el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre, manteniendo vigente su acreditación ante el Instituto Nacional de Defensa Civil.

8.2. SEGURIDAD FÍSICA DEL PERSONAL Y EL EQUIPAMIENTO

A fin de proteger al personal y el equipamiento en las instalaciones de DNP CORP S.A.C. en calidad Entidad de Registro, se implementan medios que garanticen la seguridad física de los equipos y del personal. Se tienen los siguientes controles:

- Señalización de zonas seguras
- Provisión de extinguidores contra incendios
- No debe existir cableado eléctrico expuesto
- Uso de estabilizadores y supresores de picos

8.3. PERÍMETROS DE SEGURIDAD Y CONTROL DE ACCESO FÍSICO

Las áreas de archivo de documentos en papel y archivos electrónicos deben estar protegidas constantemente contra acceso no autorizado:

- Deben estar en ambientes separados de las áreas públicas de registro.
- Sólo debe ingresar personal autorizado.
- El ingreso y salida del personal debe ser registrado.
- Los terceros y el personal de limpieza pueden ingresar con autorización del responsable de Seguridad, deben ser previamente identificados y deben ser registrados y supervisados durante su estancia en el área.
- El ingreso y salida de documentos debe ser registrada.
- Debe estar cerrada bajo llave cuando no esté siendo usada.
- Cuando sea asignado un personal nuevo se deberán verificar sus antecedentes

Las operaciones de validación y registro pueden realizarse en las instalaciones de DNP CORP S.A.C. o en las instalaciones del cliente o cualquier otro lugar definido por él en presencia del operador de registro, el cual será responsable de proteger la información proporcionada por el cliente.

8.4. ENERGÍA Y AIRE ACONDICIONADO

Se cuenta con equipos de energía y aire acondicionado los cuales cuentan con mantenimiento constante.

8.5. PROTECCIÓN CONTRA LA EXPOSICIÓN AL AGUA

Las instalaciones deben estar protegidas contra exposición al agua, en particular, las áreas de archivo deben estar distantes de zonas de filtración de agua o humedad, ya sea en el techo o en las paredes colindantes.

8.6. PROTECCIÓN CONTRA INCENDIOS

Las instalaciones deben poseer las siguientes medidas para la prevención y protección contra incendios:

Está prohibido fumar o generar cualquier fuente de humo o fuego dentro de las áreas de archivo y en las instalaciones de DNP CORP S.A.C. en calidad Entidad de Registro de AC vinculada.

Se debe contar con un extinguidor visible, destinado a extinguir fuego sobre equipos electrónicos y documentos en papel.

8.7. ARCHIVO DE MATERIAL

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), deben estar protegidos en las áreas de archivo, en contenedores de protección contra fuegos y deben situarse en diversas dependencias para eliminar riesgos asociados a una única ubicación.

El acceso a estos contenedores debe estar restringido a personal autorizado.

8.8. GESTIÓN DE RESIDUOS

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), que requieran ser eliminados o su soporte electrónico requiera ser desechado, deberán ser borrados o destruidos de manera irrecuperable.

8.9. COPIA DE SEGURIDAD EXTERNA

Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores debe ser guardada en un lugar de contingencia protegida por el responsable de la ER, contra acceso no autorizado.

9. GESTIÓN DE ROLES

9.1. ROLES DE CONFIANZA

Los roles de confianza deben ser definidos de la siguiente manera:

- Responsable de la ER
- Responsable de Seguridad y Privacidad
- Operadores de Registro
- Auditor interno
- Auditoría externa

Estos roles deben ser asignados formalmente por el responsable de DNP CORP S.A.C. en calidad Entidad de Registro de la AC vinculada.

La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de estas.

9.2. NÚMERO DE PERSONAS REQUERIDAS POR LABOR

Los cambios en los documentos normativos requieren de la autorización del responsable de la ER y del responsable de Seguridad y Privacidad, dichos roles no son compatibles y deben ser asumidos por diferentes personas.

El auditor deberá ser siempre una persona independiente de las operaciones de registro.

9.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Los roles de confianza se deben emplear controles de acceso físico para el acceso a las áreas de archivo, así como lógicos para las comunicaciones con la EC. Los controles de acceso a los sistemas de Registro dependen de la configuración de los sistemas de cada EC y no de DNP CORP S.A.C. en calidad Entidad de Registro de AC vinculada.

El auditor debe ser elegido de la lista de expertos PKI proporcionada por el INDECOPI, quien deberá ser siempre una persona independiente de las operaciones de registro.

10. GESTIÓN DEL PERSONAL

10.1. CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los roles de confianza deben tener conocimiento y entrenamiento en las operaciones de registro digital, la Política de Seguridad de la Información y la Política y el Plan de Privacidad de Datos.

Asimismo, deben tener conocimientos relacionados a los temas de certificación digital

10.2. PROCEDIMIENTO PARA VERIFICACIÓN DE ANTECEDENTES

Se deben verificar los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes vigentes y normatividad pertinente, que participan y tienen acceso a las operaciones y sistemas de registro, incluyendo:

- Verificación de antecedentes policiales

- Verificación de antecedentes penales
- Verificación de antecedentes crediticios

Las personas que desempeñan roles de confianza deben de tener en claro el nivel de sensibilidad y valor de los bienes y transacciones protegidos por la actividad de la cual ellas son responsables.

10.3. REQUISITOS DE CAPACITACIÓN

Todos los empleados de la organización que participan de los servicios de registro deben recibir las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral:

- El equipo y software requerido para operar.
- Los aspectos de la RPS, Política de Seguridad, Plan de privacidad y otra documentación relevante que afecte sus funciones.
- Requisitos legislativos con relación a sus funciones.
- Sus roles en relación con el Plan de Contingencias.
- Asignación de funciones.
- Manuales de usuario de acceso a la plataforma a la EC vinculada.

10.4. FRECUENCIA Y REQUISITOS DE LAS RE-CAPACITACIONES

Las sesiones de capacitación y entrenamiento deben ser llevadas a cabo anualmente y cuando existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se adhiera, sustituya o rote al personal encargado.

10.5. FRECUENCIA Y SECUENCIA DE LA ROTACIÓN EN EL TRABAJO

No se implementará rotación de los trabajadores. De presentarse el cese de labores de un miembro de la ER se realizará la transferencia correspondiente a quien asuma la función.

10.6. SANCIONES POR ACCIONES NO AUTORIZADAS

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad, una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.

Dichas sanciones se encuentran establecida en el contrato de confidencialidad de cada empleado y/o contratista.

10.7. REQUERIMIENTOS DE LOS CONTRATISTAS

El personal contratado para fines específicos dentro de las operaciones de DNP CORP S.A.C. en calidad Entidad de Registro de la AC vinculada, será evaluado respecto de sus antecedentes criminales, conocimiento y experiencia. Asimismo, no deberá tener acceso sin supervisión a las áreas de archivo y no tendrá acceso a los sistemas de registro brindados por la EC.

11. PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

11.1. TIPOS DE EVENTOS REGISTRADOS

Los sistemas de información sensible son provistos por la EC, por lo que DNP CORP S.A.C, en calidad Entidad de Registro de la AC vinculada, sólo puede acceder vía web. En este sentido, los logs de auditoría son administrados y definidos por la EC.

Se guardarán los contratos de los titulares y suscriptores, así como las solicitudes de los procesos de registro, como evidencia de las transacciones realizadas y para efectos de auditoría.

La ER de DNP CORP S.A.C. genera reportes de los siguientes eventos:

- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.
- El registro de auditoría de eventos debe registrar la hora, fecha e identificador software/hardware.

11.2. FRECUENCIA DEL PROCESAMIENTO DEL REGISTRO

Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo con el fin de buscar actividades sospechosas o no habituales.

El procesamiento de los registros de auditoría debe incluir la verificación de que dichos registros no hayan sido manipulados.

11.3. PERIODO DE CONSERVACIÓN DEL REGISTRO DE AUDITORÍAS

Como mínimo los contratos de suscriptores y titulares, así como las solicitudes de los procesos de registro deben conservarse por un periodo de diez (10) años.

11.4. PROTECCIÓN DEL REGISTRO DE AUDITORÍA

Las áreas de archivo donde se almacenan los contratos de los suscriptores y los titulares, así como las solicitudes de los procesos de registro estarán protegidos contra acceso no autorizado y los ingresos y salidas de personal serán registrados.

La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

11.5. COPIA DE SEGURIDAD DEL REGISTRO DE AUDITORÍA

Todas las solicitudes y contratos físicos serán generados y digitalizados por los Operadores de Registro. Las copias serán almacenadas en un lugar diferente como contingencia, protegidas contra acceso no autorizado por el responsable de DNP CORP S.A.C. en calidad Entidad de Registro de la AC vinculada.

11.6. AUDITORÍA

Las auditorías internas se llevarán a cabo al menos una vez al año en DNP CORP S.A.C. en calidad Entidad de Registro de AC vinculada.

Las evaluaciones técnicas del INDECOPI se deberán llevar a cabo una vez al año y cada vez que el INDECOPI lo requiera.

11.7. NOTIFICACIÓN AL TITULAR QUE CAUSA UN EVENTO

Las notificaciones automáticas dependen de los sistemas de la ER, para todos los eventos relacionados con el uso de los certificados por parte de un

11.8. VALORACIÓN DE VULNERABILIDAD

La plataforma de registro y solicitud de certificados digitales es administrada por la EC con quien la ER de DNP tiene convenio, la documentación de la ER es administrada y custodiada por la ER.

12. ARCHIVO

12.1. PROTECCIÓN DEL ARCHIVO

El archivo físico está protegido con controles de acceso físico para impedir el acceso a personas no autorizadas. Los documentos deben estar firmados de manera manuscrita y digital respectivamente para prevenir cualquier modificación.

El ingreso y salida de documentos físicos y digitales debe ser registrado para impedir la pérdida o destrucción no autorizada.

Debe tomarse en consideración la posibilidad de re-firmado de los archivos cuando los avances en las tecnologías generen potencialmente una posibilidad de afectación a los mismos o la generación de microformas según Decreto Legislativo 681.

Se cuenta con dos copias de seguridad que son almacenadas en distintas instalaciones.

12.2. PROCEDIMIENTO PARA OBTENER Y VERIFICAR LA INFORMACIÓN DEL ARCHIVO

Semestralmente, la integridad del archivo debe ser verificada.

13. RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

13.1. PLAN DE CONTINGENCIAS

La ER de DNP CORP S.A.C. mantiene un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones de registro de los procesos de atención de solicitudes de emisión y revocación, en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación. El plan asegura que los servicios de registro para los procesos de emisión y revocación puedan ser reasumidos dentro de un plazo máximo de 24 horas.

Los planes son evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, juntamente con la información respecto a las acciones correctivas que pudieran ser necesarias. La recuperación de los sistemas administrados por la EC, incluyendo la disponibilidad de los sistemas de registro, que permiten la comunicación entre la ER y la EC, es responsabilidad de la EC. En esos casos, DNP CORP S.A.C. en calidad Entidad de Registro de AC vinculada. Informará a los titulares y suscriptores el hecho mediante un mensaje de correo electrónico.

En caso de que la Operadora de Registro principal se encuentre de licencia (vacaciones, descanso médico, etc.), la Operadora de Registro alterna tiene la autorización de realizar las gestiones de un operador de registro en este caso también cuenta con un dispositivo criptográfico (token) en donde tiene almacenado su propio certificado digital, para poder ingresar a la plataforma de EC CAMERFIRMA y poder validar toda la información del cliente.

13.2. COMPROMISO DE LA CLAVE PRIVADA

En el caso de compromiso de la clave privada de un empleado que cumpla un rol de confianza, el certificado deberá ser revocado y se deberá solicitar la emisión de un nuevo certificado.

13.3. RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

Se establece un plan de contingencias que permita el restablecimiento y mantenimiento de las operaciones de la ER. Este plan contempla las acciones a realizar, los recursos a utilizar y el personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

14. CONFIDENCIALIDAD DE INFORMACIÓN DE LA ER

14.1. INFORMACIÓN CONSIDERADA CONFIDENCIAL

DNP CORP S.A.C. en calidad Entidad de Registro (ER) mantiene de manera confidencial la siguiente información:

- Material comercialmente reservado de la ER: planes de negocio y diseños e información de propiedad intelectual, e información que pudiera perjudicar la normal realización de sus operaciones.
- Información de los suscriptores y titulares, incluyendo contratos, información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores y titulares.
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores y titulares.

14.2. INFORMACIÓN QUE PUEDE SER PUBLICADA

- Información respecto de la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión, la publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.
- Información de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) y su estado.
- La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

15. RESPONSABILIDADES

El Responsable de la Seguridad es el encargado de gestionar la implementación, mantenimiento y mejora continua de la presente política. Asimismo, tiene la función de velar por su estricto cumplimiento, liderar su revisión periódica y proponer las actualizaciones necesarias ante la Alta Dirección. Es de su competencia asegurar el despliegue de los programas de difusión, concientización y capacitación continua en seguridad dirigidos a todo el personal de la Entidad de Registro y terceros subcontratados, garantizando un adecuado marco de gobernanza y mitigación de riesgos

16. CONFORMIDAD

El presente documento ha sido aprobado por el Responsable de DNP CORP S.A.C., en su calidad de Entidad de Registro (ER). El cumplimiento de esta política es de carácter obligatorio; cualquier vulneración, omisión o incumplimiento por parte de los empleados, contratistas o terceros incluidos en su alcance, será reportado de inmediato al Oficial de Seguridad de la Información y a la Gerencia General para la aplicación de las medidas correctivas y sanciones disciplinarias o legales respectivas, de acuerdo con el Reglamento Interno de Trabajo y el marco contractual vigente.