RESOLUCIÓN DE GERENCIA GENERAL N° GG-046-2022

Lima, 18 de abril de 2022

VISTO:

El Informe Ejecutivo N° GCDCG-002-2022, emitido por la Gerencia Corporativa de Desarrollo y Control de Gestión.

CONSIDERANDO:

Que, mediante el Informe Ejecutivo N° GCDCG-002-2022, se solicita la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de las empresas que integran el Grupo Distriluz (Electronoroeste S.A., Electronorte S.A. Hidrandina S.A. y Electrocentro S.A.); proponiendo que dicho equipo esté integrado por cuatro miembros y que se considere también, la conformación de un equipo, a nivel de la sede corporativa;

Que, el Decreto Legislativo N° 1412, Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno; y que, en el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da en todo aquello que le resulte aplicable;

Que, el artículo 30° del Decreto Legislativo N° 1412, define la Seguridad Digital como el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales, en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas;

Gerencia Corporativa de Asesoría Legal V°B° Giancarlo Pérez Salinas Gerente Corporativo de Asesoría Legal

Que, mediante Decreto de Urgencia N° 007-2020 – Decreto de Urgencia que Aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento, se establecen las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional. El artículo 3°, literal e), define el "Incidente de Seguridad Digital", como el evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales; y el literal f), define que la "Gestión de Incidentes de Seguridad Digital", como el proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares;

Gerencia General V°B° Javier Illaro A. Gerente General

Que, asimismo el artículo 9, numeral 9.3 del Decreto de Urgencia N° 007-2020, precisa que las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad

Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital;

Que, a su vez, el Decreto Supremo N° 029-2021-PCM - Reglamento del Decreto Legislativo N° 1412, Ley de Gobierno Digital, establece en el artículo 104°, que un "Equipo de Respuestas ante Incidentes de Seguridad Digital", es aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza, y que dichos equipos forman parte de los órganos o unidades orgánicas de Tecnologías de la Información de la entidad o de la unidad de organización especializada en seguridad de la información o similar prevista en su estructura orgánica o funcional. Asimismo, precisa que, la Secretaría de Gobierno Digital, en su calidad de ente rector de la seguridad digital en el país, emite opinión técnica especializada a pedido de una entidad, a fin de revisar o validar aspectos técnicos sobre la conformación de un Equipo de Respuesta ante incidentes de Seguridad Digital;

Que, en el artículo 105° del citado Reglamento se establecen las obligaciones que deben cumplirse en materia de seguridad digital, entre las cuales se encuentran aquellas relacionadas a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y la adopción de medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad;

Que, conforme al marco normativo antes mencionado, y en atención a la propuesta formulada en el Informe Ejecutivo N° GCDCG-002-2022;

SE RESUELVE:

Artículo Primero.- Conformar el Equipo de Respuestas ante Incidentes de Seguridad Digital del Grupo Distriluz, los que estarán integrados, conforme a lo siguiente:

Gerencia Corporativa de Asesoría Legal V°B° Giancarlo Pérez Salinas Gerente Corporativo de Asesoría Legal

POSICION	DISTRILUZ	ENOSA	ENSA	HIDRANDINA	ELECTROCENTRO
Líder del Equipo	Jefe Corporativo de TIC	Jefe de TI Regional	Jefe de TI Regional	Jefe TIC Regional	Jefe TI Regional
Especialista Infraestructura y Servicios	Supervisor Corporativo TIC	Analista de Sistemas	Supervisor de Servicios	Analista de Infraestructura y Servicios	Supervisor de Servicios TIC
Especialista en Comunicaciones	Analista Corporativo TIC 01	Analista de Comunicaciones	Analista de Telecomunica-ciones	Supervisor de Redes y Telecomunica-ciones	Supervisor de Servicios TIC
Especialista Desarrollo de Aplicaciones	Analista Corporativo TIC 02	Supervisor de Servicio	Supervisor de Sistemas	Supervisor de Aplicaciones de Negocio	Analista de Sistemas

Gerencia General V°B° Javier Illescas R. Gerente General

Artículo Segundo.- Los Equipos de Respuestas ante Incidentes de Seguridad Digital cumplirán las siguientes funciones:

a) Implementar y mantener planes de acción y mecanismos de control para prevenir la ocurrencia de Incidentes de Seguridad Digital.
b) Sensibilizar a los usuarios para que adopten las medidas preventivas y de presentarse algún evento que comprometa la confianza y/o seguridad digital reportarlo de inmediato para la atención oportuna de los Incidentes.
c) Atender, controlar, recuperar la operación y mitigar los daños ante la ocurrencia de Incidentes de Seguridad Digital.
d) Realizar el registro, clasificación y establecer el plan de acción para resolver las causas que han generado Incidentes de Seguridad Digital.
e) Comunicar al Centro Nacional de Seguridad Digital los incidentes de seguridad digital presentados en la Empresa.
f) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la Empresa.
g) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital de la Empresa.
h) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
i) Establecer las medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.
j) Requerir a los proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.
k) Elaborar y reportar en forma semestral un Informe de los Incidentes de Seguridad Digital presentados, las acciones realizadas para la atención inmediata y el tratamiento posterior para resolver las causas de dichos Incidentes.
l) Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

Gerencia Corporativa de Asesoría Legal
VºBº
Giancarlo Pérez Salinas
Gerente Corporativo de Asesoría Legal

Artículo Tercero.- Designar al Jefe de Tecnologías de la Información y Comunicaciones de Electrocentro S.A., como responsable de la coordinación operativa de las acciones del Equipo de Respuesta ante Incidentes de Seguridad Digital con el Centro Nacional de Seguridad Digital de la Presidencia del Consejo de Ministros - PCM.

Artículo Cuarto.- Las Gerencias Corporativas, Regionales y de Línea, deberán brindar las facilidades para el cabal cumplimiento de las disposiciones antes señaladas.

Regístrese, comuníquese y cúmplase

Javier Muro Rosado
Gerente General

Distriluz

Enosa • Ensa • Hidrandina • Electrocentro

Lima, 15 de abril de 2022

INFORME EJECUTIVO N° GCDCG-002-2022

Conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de las empresas que integran el Grupo Distriluz

1. Objetivo

Solicitar autorización a la Gerencia General, la aprobación de la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de las empresas que integran el Grupo Distriluz.

2. Antecedentes

Mediante el Decreto Legislativo N° 1412, Ley de Gobierno Digital, se establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno; y que, en el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da en todo aquello que le resulte aplicable.

A través del Decreto de Urgencia N° 007-2020, se aprueba el Marco de Confianza Digital que tiene como objetivo establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

Los Decretos antes mencionados definen Incidente de Seguridad Digital como el evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales; asimismo, define que la Gestión de incidentes de Seguridad Digital es el proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.

Por lo que precisan que las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital, mediante Decreto Supremo N° 029-2021-PCM, Reglamento del Decreto Legislativo N° 1412, Ley de Gobierno Digital (Art. 104-105)

3. Justificación

Dentro de las obligaciones que establece la Ley de Gobierno Digital y que deben cumplir las entidades públicas, como mínimo deben de considerar la aplicación de las obligaciones que están relacionadas a la Seguridad de la Información y el tratamiento de Incidentes de Seguridad Digital.

Actualmente las empresas del Grupo Distriluz están en proceso de implementación de un Sistema de Gestión de Seguridad del a Información, el cual estaría cubriendo parte de las obligaciones de Ley antes mencionada. Sin embargo, el marco normativo antes descrito la Ley de Gobierno Digital obliga a constituir el Equipo de Respuestas ante Incidentes de Seguridad Digital de las empresas del Grupo Distriluz, que será responsable de la gestión de incidentes de seguridad digital que afectan los activos de las empresas que conforman el Grupo Distriluz.

Este equipo debe formar parte de las áreas de Tecnologías de la Información de las empresas del Grupo Distriluz, debiendo considerarse las siguientes funciones:

a) Implementar y mantener planes de acción y mecanismos de control para prevenir la ocurrencia de Incidentes de Seguridad Digital.

b) Sensibilizar a los usuarios para que adopten las medidas preventivas y de presentarse algún evento que comprometa la confianza y/o seguridad digital reportarlo de inmediato para la atención oportuna de los Incidentes.

c) Atender, controlar, recuperar la operación y mitigar los daños ante la ocurrencia de Incidentes de Seguridad Digital.

d) Realizar el registro, clasificación y establecer el plan de acción para resolver las causas que han generado Incidentes de Seguridad Digital.

e) Comunicar al Centro Nacional de Seguridad Digital los incidentes de seguridad digital presentados en la Empresa.

f) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la Empresa.

g) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital de la Empresa.

h) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.

i) Establecer las medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.

j) Requerir a los proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.

k) Elaborar y reportar en forma semestral un Informe de los Incidentes de Seguridad Digital presentados, las acciones realizadas para la atención inmediata y el tratamiento posterior para resolver las causas de dichos Incidentes.

l) Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

4. Conclusión

Solicitar autorización a nuestra Gerencia General para la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de las empresas del Grupo Distriluz, conforme al marco normativo mencionado en el presente informe, cuya propuesta es la siguiente:

Equipo de Respuestas ante Incidentes de Seguridad Digital
de las empresas del Grupo Distriluz

POSICIÓN	DISTRILUZ	ENOSA	ENSA	HIDRANDINA	ELECTROCENTRO
Líder del Equipo	Jefe Corporativo de TIC	Jefe de TI Regional	Jefe de TI Regional	Jefe TIC Regional	Jefe TI Regional
Especialista Infraestructura y Servicios	Supervisor Corporativo TIC	Analista de Sistemas	Supervisor de Servicios	Analista de Infraestructura y Servicios	Supervisor de Servicios TIC
Especialista en Comunicaciones	Analista Corporativo TIC 01	Analista de Comunicaciones	Analista de Telecomunica-ciones	Supervisor de Redes y Telecomunica-ciones	Supervisor de Servicios TIC
Especialista Desarrollo de Aplicaciones	Analista Corporativo TIC 02	Supervisor de Servicio	Supervisor de Sistemas	Supervisor de Aplicaciones de Negocio	Analista de Sistemas

PEÑA PAJUELO Simeon Raimundo FAU 20132023540 soft

Firmado digitalmente por PEÑA PAJUELO Simeon Raimundo FAU 20132023540 soft
Nombre de reconocimiento (DN): c=PE, st=Trujillo-La Libertad, l=Trujillo, o=EMPRESA REGIONAL DE SERVICIO PUBLICO DE ELECTRICIDAD ELECTRONORTEMEDIO SOCIEDAD ANONIMA - HIDRANDINA, 2.5.4.97=NTRPE-20132023540, ou=EREP_PJ_RENIEC_SOLICITUD-00000375935, ou=20132023540, sn=PEÑA PAJUELO, givenName=Simeon Raimundo, serialNumber=PNOPE-09158237, cn=PEÑA PAJUELO Simeon Raimundo FAU 20132023540 soft
Fecha: 2022.04.22 20:08:23 -05'00'

Simeón Peña Pajuelo
Gerente Corporativo de Desarrollo
y Control de Gestión