Dirección de Gestión de la Información y Procesos

CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD (CSIRT-EPN)

TLP:AMBER

EPN-DGIP-CSIRT-10-PR

PROCEDIMIENTO PARA GENERAR Y GESTIONAR LOS RESPALDOS DE LOS ACTIVOS DE INFORMACIÓN CRÍTICOS E INFORMACIÓN CRÍTICA INSTITUCIONAL

Elaborado por:	Dirección de Gestión de la Información y Procesos	Ing. Javier Erazo	JAVIER ERNESTO ERAZO HIDALGO Firmado digitalmente por JAVIER ERNESTO ERAZO HIDALGO Fecha: 2021.12.16 15:54:00 -05'00'
Revisado por:		Ing. Daniela Córdova	MARIA DANIELA CORDOVA PINTADO Firmado digitalmente por MARIA DANIELA CORDOVA PINTADO Fecha: 2021.12.16 22:01:18 +01'00'
Aprobado por:	Director DGIP	Ing. Juan Pablo Ponce	Firmado electrónicamente JUAN PABLO PONCE VASQUEZ

EPN-DGIP-CSIRT-10-PR

HOJA DEL ESTADO DEL DOCUMENTO

TÍTULO DEL DOCUMENTO: Procedimiento para generar y gestionar los respaldos de los activos de información críticos e información crítica institucional.

ESTADO DEL DOCUMENTO: Aprobado

1. QUIEN EDITA	2. QUIEN REVISA	3. FECHA	4. RAZONES DE CAMBIO/QUIEN CAMBIA
Ing. Valeria Velastegui	Ing. Juan Carlos Proaño, Ing. Liliana Córdova, Ing. Roberto Andrade	10/11/2015	Aprobación del procedimiento
Ing. Javier Erazo	Ing. Daniela Córdova	09/11/2021	Nombre del procedimiento, ajustar a formato, marco legal, definiciones, actualización diagrama de flujo

1. OBJETIVO

Describir el Procedimiento para generar los respaldos de la información crítica institucional para envío al Centro de Datos Externo, como un mecanismo de protección contra pérdidas de la información.

2. ALCANCE

Con este procedimiento, se respaldará la información crítica institucional, de las diferentes unidades académicas y administrativas de la Escuela Politécnica Nacional (EPN).

Aplica a los procesos gobernantes, sustantivos, adjetivos y desconcentrados.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar y revisar este procedimiento es:	**Centro de Respuesta a Incidentes de Seguridad – CSIRT-EPN**
El responsable de aprobar este procedimiento es:	**Director de Gestión de la Información y Procesos – DGIP**
Los responsables de hacer cumplir este procedimiento son:	**Autoridades de las Unidades Académicas y Administrativas de la EPN**
Los responsables de cumplir este procedimiento son:	**Personal de la institución que gestiona los activos de información críticos institucionales y la información crítica institucional**

4. MARCO LEGAL

A continuación en la siguiente tabla se presenta la normativa legal y vigente que sustenta la implementación de este procedimiento.

Nro.	Normativa	Fecha	Título de la Normativa	Artículos
1	Normas de Control Interno de la Contraloría General del Estado	2014	410-10 Seguridad de tecnología de información	2, 4

Nro.	Normativa	Fecha	Título de la Normativa	Artículos
2	Estatuto Escuela Politécnica Nacional	2013, última reforma octubre 2019	Título V de la Disciplina y Sanciones	94 - 99
3	Política de uso de la Información, activos de información institucional y seguridad informática	2021	Del uso de la información y los activos de información institucional: Respaldos de información Ámbito de sanciones: Medidas correctivas o disciplinarias	6 21
4	Reglamento Interno de Trabajo Escuela Politécnica Nacional	2015	Capítulo VIII del Régimen Disciplinario	51 - 57
5	Reglamento Interno de Administración del Talento Humano de la Escuela Politécnica Nacional	2018	Capítulo XI Régimen Disciplinario Capítulo XII De la Competencia, procedimiento y recursos	59 – 71 72 – 73

Tabla 1. Base legal aplicable al presente procedimiento.

5. DEFINICIONES

A continuación, las siguientes definiciones utilizadas durante el desarrollo de presente procedimiento, se encuentran listadas en orden alfabético.

Activos de información crítica: Son los activos de información indispensables para la operación de la Institución (como, por ejemplo: información de configuraciones sobre sistemas operativos, software de bases de datos, código fuente, entre otros).

Cifrado: Transformación criptográfica de datos (denominada "texto sin formato") en una forma diferente (llamada "texto cifrado") que oculta el significado original de los datos y evita que la forma original de estos sea usada. El proceso inverso correspondiente es el “descifrado", que representa una transformación que restaura los datos cifrados a su forma original. [1]

Custodio de información: responsable de almacenar y mantener la información. [2]

Hash: Se trata de una función algorítmica de resumen seguro de un documento, volumen o dispositivo de almacenamiento cuyo valor es único. [3]

Información crítica[1]**:** Es la información que se considera indispensable para la operación de la Institución (ejemplo: datos personales, información académica, entre otros).

Información sensible: Información para la cual la divulgación, alteración, la destrucción o la pérdida pudieran afectar negativamente a los intereses, o negocio de su propietario o usuario. [2]

Integridad: Propiedad de proteger la precisión y completitud de los activos. [4] Refiere a que la información está completa y es precisa.

Propietario de la información: responsable de las diferentes Unidades Académicas y Administrativas de la EPN, quien decide sobre el uso y acceso a cada uno de los activos de la información, que utilizan para el soporte de sus procesos en el ámbito de sus competencias.

TLP: Traffic Light Protocol, es un conjunto de designaciones que se utilizan para garantizar que la información se comparta con la audiencia adecuada. Emplea cuatro colores para indicar los límites de compartición esperados que aplicarán los destinatarios [5].

TLP:AMBER: Es información de divulgación limitada, está restringida a las organizaciones de los participantes.

TLP:GREEN: Es información de divulgación limitada, es información pública comunitaria, está restringida a la comunidad politécnica.

TLP:WHITE: La información es pública general, su divulgación no está limitada.

TLP:RED: Esta información no puede ser divulgada y está limitada solo a los participantes.

[1] Es la información que se considera indispensable para que una unidad académica/administrativa de la EPN pueda seguir trabajando o realizando sus actividades, tras recuperarse de un evento que afecte su actividad normal, provocado por un desastre de origen natural, industrial o provocado por el hombre. Es considerada la línea base para el inicio de las actividades si se suscitara un evento como el mencionado.

6. DIRECTRICES

Los propietarios de la información crítica serán las autoridades de las unidades académicas y administrativas de la institución.

Toda la información crítica enviada por las unidades académicas y administrativas de la institución será etiqueta como TLP: RED y tendrá un tiempo de retención de 7 años a partir de su entrega al CSIRT-EPN.

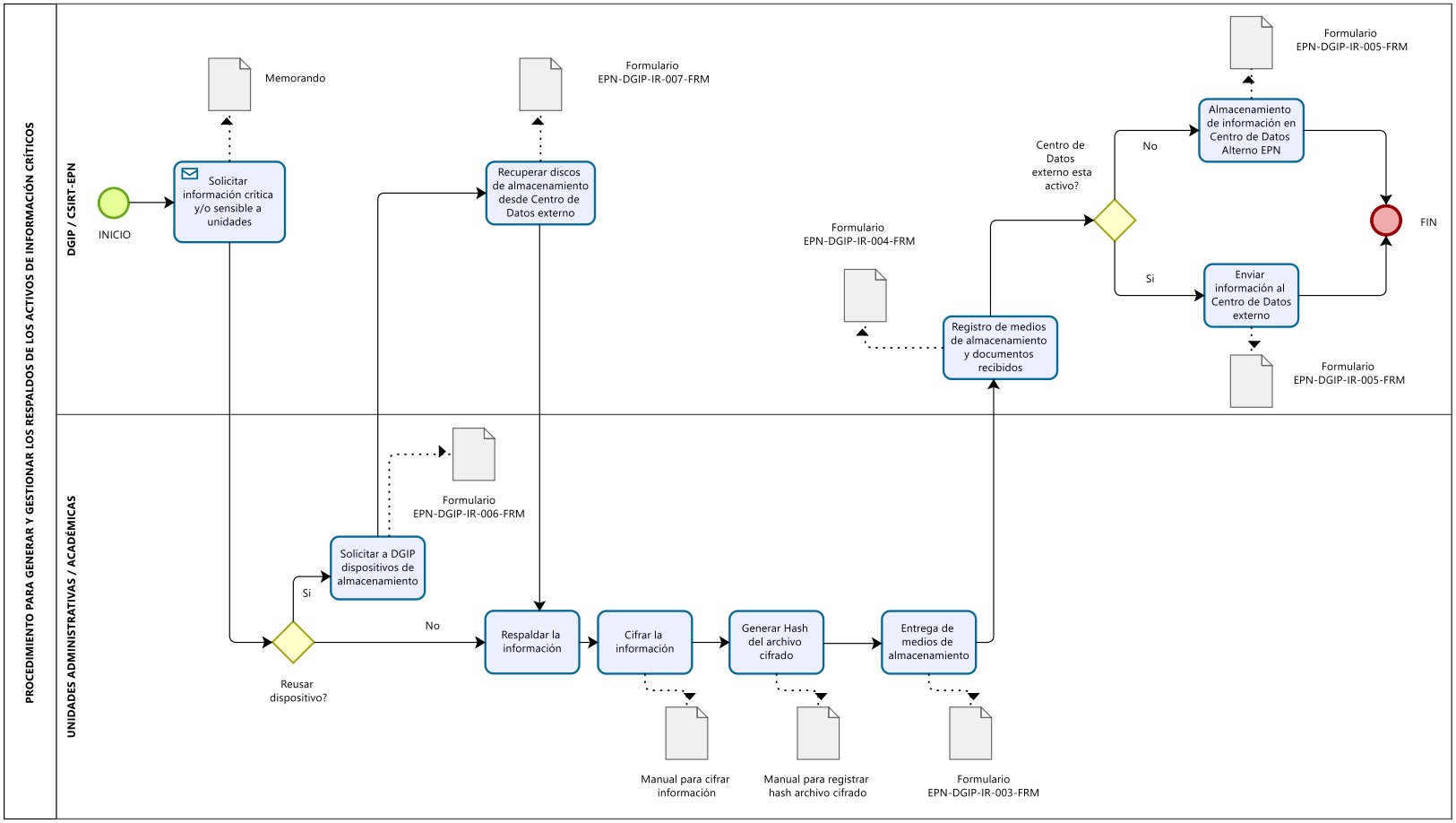
Los propietarios de la Información deberán seguir el presente procedimiento y cumplir con los términos establecidos en el mismo.

El plazo máximo para la entrega de los respaldos de información crítica por parte de los propietarios de la información, será de 5 días hábiles a partir del pedido formal realizado por la DGIP.

Excepciones

Este procedimiento no se ejecutará en períodos de estado de excepción previamente aprobados por las autoridades competentes.

7. **DIAGRAMA DE FLUJO:** PROCEDIMIENTO PARA GENERAR Y GESTIONAR LOS RESPALDOS DE LOS ACTIVOS DE INFORMACIÓN CRÍTICOS E INFORMACIÓN CRÍTICA INSTITUCIONAL



8. DESCRIPCIÓN DEL PROCEDIMIENTO PARA GENERAR Y GESTIONAR LOS RESPALDOS DE LOS ACTIVOS DE INFORMACIÓN CRÍTICOS E INFORMACIÓN CRÍTICA INSTITUCIONAL

8.1. Solicitar información crítica a unidades

El director de la DGIP, solicita mediante memorando en marzo de cada año, la información crítica de la EPN y el nombre del funcionario que será la contraparte del CSIRT en este procedimiento, a los propietarios de la información de las unidades académicas y administrativas de la institución.

8.2. Solicitar al CSIRT-EPN dispositivos de almacenamiento

Si el propietario de la información requiere reusar las cintas, discos externos, cd, DVD o flash/USB, deberá solicitar dichos dispositivos de almacenamiento al CSIRT-EPN, llenando el formulario EPN-DGIP-IR-006-FRM.

8.3. Recuperar dispositivo de almacenamiento desde centro de datos externo

El CSIRT-EPN, solicitará las cintas, discos externos, cd, DVD o flash/USB que se encuentran en el centro de datos externo y entregará a la unidad solicitante el dispositivo. Formulario EPN-DGIP-IR-007-FRM

8.4. Respaldar la información

El propietario de la información de las unidades académicas y administrativas, respaldará la información crítica en cintas, discos externos, cd, DVD o flash/USB. Una vez realizado el respaldo, se deberá verificar la integridad de la información.

8.5. Cifrar la información

La información que será enviada debe ser cifrada, para lo cual se seguirán los pasos del Manual para cifrar información (Anexo 1).

8.6. Generar Hash del archivo cifrado

El propietario de la información de las unidades académicas y administrativas, generará el Hash del archivo cifrado, el mismo que servirá para identificar la información. Siguiendo el Manual para registrar el hash del archivo cifrado (Anexo 2).

8.7. Entrega de medios de almacenamiento al CSIRT-EPN

El propietario de la información de las unidades académicas y administrativas, entregará los medios de almacenamiento al CSIRT-EPN llenando el formulario EPN-DGIP-IR-003-FRM, en este se registrará el Hash del archivo cifrado. Es responsabilidad del propietario de la información, verificar que los datos se hayan almacenado en el dispositivo, que el hash esté registrado en el formulario y que la información pueda ser recuperada de manera íntegra y completa.

8.8. Registro de medios de almacenamiento y documentos recibidos

El CSIRT-EPN registrará los medios de almacenamiento (que contienen los respaldos de información crítica) recibidos, en el formulario EPN-DGIP-IR-004-FRM y verificará que los formularios adjuntos estén completos.

El CSIRT-EPN, registrará en una bitácora por cada unidad de la EPN que realiza la entrega de información crítica, entre otros datos:

- Unidad.
- Medio de almacenamiento.
- Fecha de entrega.

8.9. Envío de información crítica al Centro de Datos Externo

El CSIRT-EPN enviará los medios de almacenamiento (que contienen los respaldos de información crítica), al Centro de Datos Externo con el registro del formulario EPN-DGIP-IR-005-FRM.

8.10. Almacenamiento de información crítica en Centro de Datos Alterno de la EPN

En caso de que el Centro de Datos Externo no este activo, los medios de almacenamiento (que contienen los respaldos de información crítica) reposarán en la caja de seguridad de información crítica institucional, en el Centro de Datos alterno de la EPN, bajo custodia del CSIRT-EPN.

9. CUMPLIMIENTO

El cumplimiento del presente procedimiento es obligatorio, y son los órganos competentes de la Escuela Politécnica Nacional quienes de ser el caso y con hechos demostrados, aplicarán sanciones disciplinarias conforme las leyes y

reglamentos aplicables al personal académico, personal de apoyo académico, servidores públicos, trabajadores y estudiantes.

10. REFERENCIAS

[1] IETF RFC 4949 Ver 2. Internet Security Glossary, páginas 119, 278, https://www.rfc-editor.org/rfc/pdfrfc/rfc4949.txt.pdf

[2] COBIT5-Framework-Spanish.pdf (informatica.edu.bo)

[3] https://www.eicyc.es/que_es_el_codigo_hash/

[4] NTE INEN-ISO/IEC 27000:2012, página 3, sección 2, Términos y definiciones.

[5] FIRST, Forum of Incident Response and Security Teams, https://www.first.org/tlp/

11. ANEXOS

Anexo 1: Manual para cifrar información.
Anexo 2: Manual para obtener hash archivo cifrado.
Anexo 3: Formularios.