IGP V.B.
Firmado digitalmente por: TOVALINO YAPIAS Ivan James FAU 20131367008 soft
Motivo: Doy V° B°
Fecha: 02/12/2020 15:13:19-0500

IGP V.B.
Firmado digitalmente por: LUNA GUZMAN Maria Rosa FAU 20131367008 soft
Motivo: Doy V° B°
Fecha: 02/12/2020 15:25:44-0500

IGP V.B.
Firmado digitalmente por: DELGADO ORTEGA Edgar FAU 20131367008 hard
Motivo: Doy V° B°
Fecha: 02/12/2020 15:29:55-0500

INSTITUTO GEOFÍSICO DEL PERÚ

Resolución de Gerencia General

N° 036-IGP/2020

Lima, 2 de Diciembre del 2020

VISTOS:

El Informe Legal N° 0118-2020-IGP/GG-OAJ y el Informe N° 0209-2020-IGP/GG-OPP; y

CONSIDERANDO:

Que, mediante el Decreto Legislativo N° 136, se crea el Instituto Geofísico del Perú (IGP) como un Organismo Descentralizado del Sector Educación, cuya finalidad es la investigación científica, la enseñanza, la capacitación, la presentación de servicios y, la realización de estudios y proyectos, en las diversas áreas de la Geofísica;

Que, la Primera Disposición Complementaria Final del Decreto Legislativo N° 1013, Ley de Creación, Organización y Funciones del Ministerio del Ambiente, dispone la adscripción del IGP como un organismo público ejecutor del Ministerio del Ambiente;

Que, mediante el Decreto Supremo N° 001-2015-MINAM, se aprobó el Reglamento de Organización y Funciones (ROF) del Instituto Geofísico del Perú (IGP);

Que, el numeral 1 de la Décima Séptima Disposición Complementaria Final del Decreto de Urgencia N° 021-2020 establece que el Instituto Geofísico del Perú es el Ente Rector de las investigaciones teóricas y aplicadas en la Ciencia Geofísica orientada a la ejecución de la Política Nacional de Gestión del Riesgo de Desastres;

Que, es necesario precisar que de acuerdo al Cuadro N° 2. Tipo de Documento de la Directiva DI 001-2020-IGP Aprobación, Modificación o Derogación de Documentos Normativos, aprobada mediante Resolución de Gerencia General N° 029-IGP/2020, de fecha 16 de octubre de 2020, los procedimientos de una entidad son aprobadas mediante Resolución de Gerencia General;

Que, el artículo 4° de la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado establece que:

"El proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos (…)".

Que, mediante el Informe N° 0209-2020-IGP/GG-OPP el Jefe de la Oficina de Planeamiento y Presupuesto señala que la propuesta de modificación de procedimientos del Sistema de Gestión de Calidad del Informe N° 037-2020-IGP/GG-OTIDG, presentada por la Jefa de la Oficina de Tecnologías de la Información y Datos Geofísicos es viable;

Que siendo así, de la revisión del Informe N° 0209-2020-IGP/GG-OPP se advierte que cumple con la normativa y resulta favorable la propuesta de modificación de los procedimientos del Sistema de Gestión de Calidad del Informe N° 037-2020-IGP/GG-OTIDG;

Que, mediante Informe Legal N° 0118 -2020-IGP/GG-OAJ se emite opinión legal favorable para aprobar la propuesta de modificación de los procedimientos del Sistema de Gestión de Calidad del Informe N° 037-2020-IGP/GG-OTIDG;

Con el visado de la Oficina de Asesoría Jurídica y de la Oficina de Planeamiento y Presupuesto, y;

De conformidad con el Decreto Supremo N° 001-2015-MINAM, la Directiva DI 001-2020-IGP Aprobación, Modificación o Derogación de Documentos Normativos, aprobada mediante Resolución de Gerencia General N° 029-IGP/2020, la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado;

SE RESUELVE:

Artículo 1.- Aprobar la modificación de los siguientes procedimientos:

1. PROCEDIMIENTO PR 014-2020-IGP DESARROLLO DE SOLUCIONES INFORMÁTICAS
2. PROCEDIMIENTO PR 016-2019-IGP GESTIÓN DE ATENCIONES TIC Y EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
3. PROCEDIMIENTO PR 020-2019-IGP RESPALDO DE LA INFORMACIÓN

Los que como anexos forman parte integrante de la presente Resolución de Gerencia General.

Artículo 2.- Disponer la publicación de la presente Resolución de Gerencia General en el Portal Institucional del Instituto Geofísico del Perú (www.igp.gob.pe).

Artículo 3.- Notificar la presente Resolución de Gerencia General a los interesados.

Regístrese, publíquese y comuníquese.

Raúl Javier Bueno Cano
Gerente General

IGP

Firmado digitalmente por:
BUENO CANO Raul Javier
FAU 20131367008 soft
Motivo: Soy el Autor del
Documento
Fecha: 02/12/2020 15:40:27-0500

PROCEDIMIENTO PR 014-2020-IGP

DESARROLLO DE SOLUCIONES INFORMÁTICAS

Versión 03

IGP V.B.

Firmado digitalmente por:
DELGADO ORTEGA Edgar FAU
20131367008 hard
Motivo: Doy V° B°
Fecha: 22/11/2020 17:28:59-0500

PROCEDIMIENTO PR 014-2020-IGP

DESARROLLO DE SOLUCIONES INFORMÁTICAS

VERSIÓN	FECHA	DESCRIPCIÓN
01 02	12/10/2019 22/11/2020	1. Documento Inicial 2. Se modifica la estructura y codificación y se actualiza la secuencia de actividades.
FORMULADO **OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y DATOS GEOFÍSICOS**	**REVISADO Y VISADO** **OFICINA DE PLANEAMIENTO Y PRESUPUESTO**	**REVISADO Y VISADO** **OFICINA DE ASESORÍA JURÍDICA**
APROBADO **GERENCIA GENERAL**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ÓRGANO/UNIDAD ORGÁNICA)**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ÓRGANO/UNIDAD ORGÁNICA)**

DESARROLLO DE SOLUCIONES INFORMÁTICAS

IGP Instituto Geofísico del Perú	INSTITUTO GEOFÍSICO DEL PERÚ		
	FICHA TÉCNICA DEL PROCEDIMIENTO		
DATOS DEL PROCEDIMIENTO			
Nombre del procedimiento	DESARROLLO DE SOLUCIONES INFORMATICAS	Objetivo del procedimiento	Establecer la metodología de desarrollo de soluciones informáticas que cumplan los requisitos funcionales y de seguridad, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) del IGP, incluyendo las mejores prácticas de desarrollo posibles en cumplimiento a la Norma ISO/IEC 27001:2013 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos”
Código del Proceso relacionado	S03	Alcance del procedimiento	El presente procedimiento es aplicable para la Oficina de Tecnología de Información y Datos Geofísicos – OTIDG y abarca las actividades de ingeniería de software y desarrollo de aplicaciones que esta oficina realice.
Versión	2		

Base Normativa (Son disposiciones legales que soportan el procedimiento)	
Resolución Ministerial N° 004-2016-PCM y modificatorias.	Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
Decreto Supremo No 001-2015-MINAM	Reglamento Organización de Funciones (ROF) del Instituto Geofísico del Perú
Directiva DI 001-2020- IGP/OPP	Aprobación, Modificación o Derogación de Documentos Normativos del Instituto Geofísico del Perú – IGP
Resolución de Presidencia N° 140-IGP/2019 (31 de Diciembre del 2019)	Plan Operativo Institucional del IGP 2020
Norma NTP ISO/IEC 27001:2014 (basada en ISO/IEC 27001:2013)	8.1 Planificación y control operacional Anexo A. A.14.2 Seguridad en procesos de desarrollo y soporte

Siglas y Definiciones (Abreviaturas y acrónimos)
IGP: Instituto Geofísico del Perú
SGSI: Sistema de Gestión de la Seguridad de la Información
OTIDG: Oficina de Tecnología de Información y Datos Geofísicos
UIS: Unidad de Ingeniería de Software
UO: Unidad Orgánica

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.
Confidencialidad: Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.
Control: Medida que modifica un riesgo. Los controles incluyen cualquier proceso, la política, dispositivo, práctica, u otras acciones que modifiquen un riesgo. Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.
Desarrollo de aplicaciones: El desarrollo de aplicaciones, también conocido como proceso de software, ciclo de vida del software y desarrollo de software, es el desarrollo de un producto de software en un proceso planificado y estructurado.
Disponibilidad: Propiedad de la información de ser accesible y utilizable por petición de una entidad autorizada.
Integridad: Propiedad de exactitud y lo completitud de la información.
Probabilidad: Posibilidad de que algún hecho se produzca.
Proceso: Conjunto de actividades interrelacionadas o interactivas que utilizan entradas para entregar un resultado previsto. El "resultado previsto" de un proceso se denomina salida, producto o servicio dependiendo del contexto de la referencia. Las entradas a un proceso son generalmente las salidas de otros procesos y las salidas de un proceso son generalmente las entradas a otros procesos.
Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.
Sistema de Gestión de Seguridad de la Información (SGSI): Consiste en un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionado de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos del negocio. Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos. El análisis de los requisitos para la protección de los activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI.
Vulnerabilidad: Debilidad de un activo o de control que puede ser explotado por una o más amenazas.

Elemento de Entrada (Requisitos para iniciar el procedimiento)	
Descripción del Requisito	**Fuente**
Expresión de necesidades de automatización o funcionalidades que pueden ser satisfechas a través del desarrollo de software	Correo y/o Memorándum

ACTIVIDADES (Actividad, Unidad de Organización y Responsable)			
Nº	**Descripción de la Actividad**	**Unidad de Organización (*)**	**Responsable**
1	**Realizar el requerimiento del software, aplicación o sistema.**	Unidad Orgánica	Jefe/Director de la Unidad Orgánica
2	**Recibir y evaluar requerimiento.**	OTIDG	Jefa de la OTIDG
3	**Informar no viabilidad de requerimiento**, si el requerimiento no cumple con los objetivos de la Institución	OTIDG	Jefa de la OTIDG
4	**Actualizar el Plan de Proyectos TI** y el Cronograma de Proyectos TI	OTIDG	Coordinador de Ingeniería de Software
5	**Asignar los roles de desarrollo** Asignar y documentar los roles en Ficha de Desarrollo Soluciones Informáticas, de acuerdo con el Anexo I Roles de Desarrollo	OTIDG	Coordinador de Ingeniería de Software
6	**Recabar elementos de entrada.** Realizar entrevistas, recibir documentos de referencia e identificar potenciales productos con los cuales hacer benchmarking para	OTIDG	Coordinador de Ingeniería de Software

	tener los requisitos del objeto a desarrollar. Incorporar a estos requisitos los niveles mínimos aceptables de seguridad y privacidad. Utilizar como guía el Anexo II: Formulación de Preguntas de Seguridad		
7	**Resumir los requisitos funcionales**, los requisitos de seguridad (resultantes de responder al Anexo II) y los criterios de aceptación acordados con el Representante del Usuario Final en la Ficha de Desarrollo de Soluciones Informáticas	OTIDG	Coordinador de Ingeniería de Software
8	**Elaborar la base de datos Entidad - Relación**	OTIDG	Coordinador de Ingeniería de Software
9	**Revisar el Anexo III:** Top 10 Riesgos de Seguridad en Aplicaciones Web, identificando si el desarrollo a realizarse puede ser susceptible a alguno de estos riesgos con fines preventivos.	OTIDG	Coordinador de Ingeniería de Software
10	Establecer capas de seguridad, tomando en cuenta los conceptos y controles en el Anexo IV Estándares de Desarrollo Seguro	OTIDG	Coordinador de Ingeniería de Software
11	**Entorno de Desarrollo** Realizar el desarrollo software, tomando en cuenta los roles previamente establecidos, las respuestas a las preguntas de seguridad, las capas de seguridad establecidas y las medidas de separación de entornos de desarrollo, prueba y producción establecidas	OTIDG	Coordinador de Ingeniería de Software

	en el Anexo IV Estándares de Desarrollo Seguro		
12	**Entorno de Pruebas** Copiar el código al servidor de pruebas (en segmento VLAN de pruebas segregado) a través de SFTP, bajo autenticación.	OTIDG	Coordinador de Ingeniería de Software
13	**Entorno de Pruebas** Realizar las pruebas funcionales y de seguridad al software y registrar los resultados en el formato Pruebas de Sistema de Información, Redes y Aplicativos	OTIDG	Coordinador de Ingeniería de Software
14	**Entorno de Operaciones** El código fuente es copiado a través de SFTP al servidor de producción, bajo autenticación.	OTIDG	Coordinador de Ingeniería de Software
15	**Entorno de Operaciones** Realizar despliegue de software	OTIDG	Coordinador de Ingeniería de Software
16	Capacitar a usuarios y/o difundir desarrollo	OTIDG	Coordinador de Ingeniería de Software
Fin del procedimiento			
DOCUMENTOS QUE SE GENERAN (Documento de salida del procedimiento)			
Correo o memorándum de solicitud de una solución informática			
Correo o memorándum de no viabilidad del requerimiento (Si aplica)			

Plan de Proyectos TI
Cronograma de Proyectos TI
Ficha de Desarrollo de Soluciones Informáticas
Pruebas de Sistema de Información, Redes y Aplicativos
Acta de capacitación

“Toda copia impresa es un Documento No Controlado a excepción del original”

ANEXO I – Roles de Desarrollo

Rol de Desarrollo	Asignado a
Representante de usuario final	Jefe de la Unidad Orgánica solicitante y/o un subordinado
Seguimiento	Realizado por Coordinador de Ingeniería de Software y/o Jefe de OTIDG.
Equipo específico de desarrollo	Otros puestos de OTIDG asignados al proyecto según necesidad y competencias.

ANEXO II - Formulación de Preguntas de Seguridad

- ¿Mi aplicación contiene información confidencial?
- ¿Mi aplicación recopila o almacena datos que exigen que se cumplan estándares normativos nacionales?
- ¿Mi aplicación recopila o contiene datos confidenciales personales o de clientes que pueden utilizarse, solos o con otra información, para identificar, ponerse en contacto o buscar a una persona?
- ¿Mi aplicación recopila o contiene datos que se pueden usar para acceder a información médica, educativa, financiera o de empleo de una persona?
- ¿Dónde y cómo están los datos almacenados? Tenga en cuenta cómo va a supervisar los servicios de almacenamiento que usa la aplicación para detectar cualquier cambio inesperado de comportamiento (por ejemplo, tiempos de respuesta más lentos). ¿Podrá influir en el registro para recopilar datos más detallados y analizar un problema en profundidad?
- ¿Mi aplicación estará disponible para el público (en Internet) o solo internamente? Si la aplicación está disponible al público, ¿cómo protege los datos que puedan recopilarse para que no se utilicen de forma incorrecta? Si la aplicación solo está disponible internamente, tenga en cuenta qué usuarios de la organización han de tener acceso a la aplicación y durante cuánto tiempo.
- ¿Comprende el modelo de identidad antes de empezar a diseñar la aplicación? ¿Cómo va a determinar que los usuarios son quienes dicen ser y lo que un usuario está autorizado a hacer?
- ¿Mi aplicación lleva a cabo las tareas importantes o confidenciales? Tenga en cuenta cómo va a validar que el usuario que realiza una tarea confidencial está autorizado a realizarla y cómo se va a autenticar que la persona es quien dice ser.
- ¿Mi aplicación realiza actividades de riesgo de software, como permitir que los usuarios carguen o descarguen archivos u otros datos? Si la aplicación lleva a cabo actividades de riesgo, tenga en cuenta cómo va a proteger a los usuarios de la manipulación de datos o archivos malintencionados.

ANEXO III – Top 10 Riesgos de Seguridad en Aplicaciones Web

1. Inyección. Las fallas de inyección, como la inyección de SQL, NoSQL, OS y LDAP, ocurren cuando se envían datos que no son de confianza a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a datos sin la debida autorización.
2. Autenticación rota. Las funciones de la aplicación relacionadas con la autenticación y la administración de sesiones a menudo se implementan de manera incorrecta, lo que permite a los atacantes comprometer contraseñas, claves o tokens de sesión, o explotar otras fallas de implementación para asumir las identidades de otros usuarios de forma temporal o permanente.
3. Exposición de datos sensibles. Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales, como los financieros, de salud y PII. Los atacantes pueden robar o modificar esos datos débilmente protegidos para cometer fraude con tarjetas de crédito, robo de identidad u otros delitos. Los datos confidenciales pueden verse comprometidos sin protección adicional, como el cifrado en reposo o en tránsito, y requieren precauciones especiales cuando se intercambian con el navegador.
4. Entidades externas XML (XXE). Muchos procesadores XML más antiguos o mal configurados evalúan las referencias de entidades externas dentro de los documentos XML. Las entidades externas se pueden utilizar para divulgar archivos internos mediante el controlador de URI de archivos, recursos compartidos de archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio.
5. Control de acceso roto. Las restricciones sobre lo que los usuarios autenticados pueden hacer a menudo no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder a funciones y / o datos no autorizados, como acceder a las cuentas de otros usuarios, ver archivos confidenciales, modificar los datos de otros usuarios, cambiar los derechos de acceso, etc.
6. Mala configuración de seguridad. La configuración incorrecta de seguridad es el problema más común. Esto suele ser el resultado de configuraciones predeterminadas inseguras, configuraciones incompletas o ad hoc, almacenamiento en la nube abierta, encabezados HTTP mal configurados y mensajes de error detallados que contienen información confidencial. No solo

todos los sistemas operativos, marcos, bibliotecas y aplicaciones deben configurarse de forma segura, sino que también deben actualizarse o actualizarse de manera oportuna.

7. Cross-Site Scripting XSS . Los defectos de XSS ocurren cuando una aplicación incluye datos que no son de confianza en una nueva página web sin la validación o el escape adecuados, o actualiza una página web existente con datos proporcionados por el usuario mediante una API de navegador que puede crear HTML o JavaScript. XSS permite a los atacantes ejecutar scripts en el navegador de la víctima que pueden secuestrar sesiones de usuario, desfigurar sitios web o redirigir al usuario a sitios maliciosos.
8. Deserialización insegura. La deserialización insegura a menudo conduce a la ejecución remota de código. Incluso si las fallas de deserialización no dan como resultado la ejecución remota de código, pueden usarse para realizar ataques, incluidos ataques de reproducción, ataques de inyección y ataques de escalada de privilegios.
9. Uso de componentes con vulnerabilidades conocidas. Los componentes, como bibliotecas, marcos y otros módulos de software se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, dicho ataque puede facilitar la pérdida de datos o la toma de control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden socavar las defensas de las aplicaciones y permitir varios ataques e impactos.
10. Registro y monitoreo insuficientes. Un registro y una supervisión insuficientes, junto con una integración faltante o ineficaz con la respuesta a incidentes, permiten a los atacantes atacar aún más los sistemas, mantener la persistencia, cambiar a más sistemas y manipular, extraer o destruir datos. La mayoría de los estudios de infracciones muestran que el tiempo para detectar una infracción es de más de 200 días, generalmente detectados por partes externas en lugar de procesos internos o monitoreo.

Fuente: OWASP Foundation, Inc.
https://owasp.org/www-project-top-ten/

ANEXO IV – Estándares de Desarrollo Seguro

Lenguajes de Programación Aprobados por la OTIDG
Javascript
Java
PHP
Python
Swift
Kotlin

Consideraciones Para Establecer Capas de Seguridad
• Uso de una biblioteca de codificación segura y un marco de software. • Búsqueda de componentes vulnerables. • Listar las amenazas a las que es susceptible la solución informática • Reducción de la superficie expuesta a ataques. • Adopción de una directiva de identidad como perímetro de seguridad principal. • Exigencia de re-autenticación con transacciones importantes. • Uso de una solución de administración de claves para proteger las claves, las credenciales y otros secretos. • Protección de datos confidenciales. • Implementación de medidas para notificaciones de error. • Aprovechamiento del control de errores y excepciones. • Uso del registro y las alertas. • Comunicaciones entre servicios. • Generación de logs, gestión de eventos.

Estándares de seguridad para la codificación y pruebas
• No está permitido modificar programas sin que quede registrado el cambio. • En caso de requerirse la implementación de un cambio, este deberá seguir el procedimiento de control de cambios. • No está permitido escribir cambios no autorizados ni código malicioso. • Las pruebas de software deben cubrir instalación, stress, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores. Las pruebas buscan asegurar que el software no muestre detalles de posibles errores o datos confidenciales que puedan ser usados por atacantes. No indexar directorios de recursos y presentar las interfaces de usuario fieles a los prototipos de software aceptados por el usuario final. • Se deberá realizar una gestión de las sesiones, que tenga en cuenta los siguientes aspectos: • Garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos que permita terminar completamente con la conexión asociada. • No exponer los identificadores de sesión en URL, mensajes de error ni logs, y no transmitirlos como parámetros.

- Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Asegurar que la sesión expire después de cierto tiempo.
- No permitir la apertura de sesiones simultaneas con el mismo usuario.
- Todas las funciones de criptografía de las aplicaciones desarrolladas deben ser implementadas en sistemas confiables (por ejemplo: el servidor).
- Se deben considerar los siguientes aspectos en el manejo de errores:
- Garantizar que no se divulgue información sensible en respuestas de error.
- Liberar espacio en memoria cuando ocurra una condición de error.
- Para el manejo de archivos se deberán acatar las siguientes consideraciones:
- Remover todas las funcionalidades y archivos que no sean parte del software.
- Prevenir la revelación de la estructura de directorios del software.
- Para el establecimiento de conexión a las bases de datos se deberán considerar los siguientes aspectos:
- No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
- Cerrar la conexión a las bases de datos desde los aplicativos, tan pronto como estas no sean requeridas.

Separación de Entornos de Desarrollo, Pruebas y Producción

- Se separan los entornos principalmente al funcionar en VLAN distintas.
- El desarrollo se realiza utilizando un terminal en la VLAN de desarrollo.
- El software de desarrollo se realiza en un entorno de desarrollo y en la VLAN de desarrollo.
- El software de producción funciona en un servidor ajeno a los demás entornos.
- Existen reglas que solo permiten a las computadoras del sistema de publicación acceder al mismo.
- Se despliega un servidor para integración continua y entrega continua basado en Jenkins

PROCEDIMIENTO PR 016-2019-IGP

GESTIÓN DE ATENCIONES TIC Y EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Versión 03

IGP V.B.
Firmado digitalmente por:
DELGADO ORTEGA Edgar FAU
20131367008 hard
Motivo: Doy V° B°
Fecha: 22/11/2020 17:28:43-0500

PROCEDIMIENTO PR 016-2020-IGP

GESTIÓN DE ATENCIONES TIC Y EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN
01 02	12/10/2019 22/11/2020	1. Documento Inicial 2. Se modifica la estructura y codificación y se actualiza la secuencia de actividades.
FORMULADO **OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y DATOS GEOFÍSICOS**	**REVISADO Y VISADO** **OFICINA DE PLANEAMIENTO Y PRESUPUESTO**	**REVISADO Y VISADO** **OFICINA DE ASESORÍA JURÍDICA**
APROBADO **GERENCIA GENERAL**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)**

GESTIÓN DE ATENCIONES TIC Y EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

IGP Instituto Geofísico del Perú	INSTITUTO GEOFÍSICO DEL PERÚ
	FICHA TÉCNICA DEL PROCEDIMIENTO

DATOS DEL PROCEDIMIENTO			
Nombre del procedimiento	GESTIÓN DE ATENCIONES TIC Y EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Objetivo del procedimiento	Garantizar la continuidad operativa de los equipos y servicios de tecnología de la información y comunicaciones (TIC) que requieren las diferentes unidades orgánicas del Instituto Geofísico del Perú (IGP) para el desarrollo de sus actividades.
Código del Proceso relacionado	S03	Alcance del procedimiento	Atenciones de T.I. y eventos e incidentes de seguridad de la información reportados por las unidades orgánicas del IGP y los administradores de sistemas informáticos.

Versión	3	

Base Normativa (Son disposiciones legales que soportan el procedimiento)	
Decreto Supremo N° 001-2015-MINAM	Reglamento Organización de Funciones (ROF) del Instituto Geofísico del Perú
Resolución de Presidencia No 129-IGP/2018 (31 de Mayo del 2018)	Plan Operativo Institucional
Decreto de Urgencia N° 007-2020	Decreto de Urgencia que Aprueba el Marco de Confianza Digital y Dispone Medidas Para su Fortalecimiento

Siglas y Definiciones (Abreviaturas y acrónimos)
OTIDG: Oficina de Tecnologías de la Información y Datos Geofísicos
SMA: Sistema de Mesa de Ayuda
STD: Sistema de Trámite Documentario
Atención: Necesidad del personal de una Unidad Orgánica (U.O.) a ser atendida por OTIDG. Puede escalar a evento de seguridad de la información.
Equipo de Respuesta Ante Incidentes de Seguridad Digital: Equipo que cada entidad de la administración pública conforma para la gestión de incidentes de seguridad de la información, incluyendo los incidentes de seguridad digital.

Evento: Sucesos físicos o lógicos que ocurren en el marco del Sistema de Gestión de Seguridad de la Información.
Evento de Seguridad de la Información: Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser relevante la seguridad.
Incidente de Seguridad de la Información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información
Log: Grabación secuencial en un archivo o en una base de datos de todos los eventos que afectan a un proceso particular (aplicación, actividad de una red informática y otros)
Panel de Control: Es la interfaz gráfica que permite gestionar la configuración y observar indicadores, notificaciones, alertas, eventos y en general el comportamiento de las variables relevantes de los sistemas de información.
Requerimiento: En el presente procedimiento, se refiere a la solicitud de una implementación, configuración o acceso ligada a nuevas necesidades de los usuarios para el cumplimiento de sus funciones.

Elemento de Entrada (Requisitos para iniciar el procedimiento)	
Descripción del Requisito	**Fuente**
Solicitud de atención de un problema o requerimiento por parte de una unidad orgánica del IGP a la OTIDG	Correo electrónico, teléfono, presencial

ACTIVIDADES (Actividad, Unidad de Organización y Responsable)			
Nº	**Descripción de la Actividad**	**Unidad de Organización (*)**	**Responsable**

1	Monitorear los paneles de control correspondientes, de acuerdo con el **Anexo I Tabla de Planificación del Monitoreo de Eventos en Sistemas**.	OTIDG	Administradores de sistemas informáticos
2	Identificar eventos sospechosos o anómalos.	OTIDG	Administradores de sistemas informáticos
3	Monitorear los sucesos relacionados con el control de acceso a las sedes de la institución	ULO	Responsable de Servicios Generales / Oficial de Seguridad de la Información
4	Solicitar atención o requerimiento a través de los siguientes canales: Al correo electrónico soporteti@igp.gob.pe Mediante los anexos 191,194, 196 y 197 Sede Camacho o anexo 193 Sede Mayorazgo Mediante los móviles institucionales de OTIDG: 942047526, 942053435 y 943614234 o presencialmente al Coordinador Responsable de Operaciones de Tecnologías de la Información	Unidad Orgánica / OTIDG	Personal Unidad Orgánica / Administradores de sistemas informáticos / Responsable de Servicios Generales
5	Recibir y registrar la atención o requerimiento, abrir caso en el **Registro de Atenciones, Eventos e Incidentes de Seguridad de la Información** y asignar ticket.	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información
6	Clasificar inicialmente la atención o requerimiento en: Atención o Requerimiento.	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información
7	Escalar "Atención" como "Evento de Seguridad de la Información", de acuerdo con los hallazgos iniciales y de acuerdo con las definiciones del procedimiento.	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información
8	Recopilar y analizar toda la información que sea pertinente: Manifestación de fallas, mensajes en	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información

	pantallas, información en logs y reportes en los elementos citados en el **Anexo I Tabla de Planificación del Monitoreo de Eventos en Sistemas** y otras fuentes de información en la medida de lo necesario.		
9	De tratarse de un evento de S.I. que haya implicado alguna pérdida en confidencialidad, integridad, disponibilidad, clasificarlo como un Incidente de S.I., especificando esto en el **Registro de Atenciones, Eventos e Incidentes de Seguridad de la Información**. Ver **Anexo II – Clasificación de Eventos e Incidentes de Seguridad de la Información**	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Oficial de Seguridad de la Información
10	Comunicar los incidentes de S.I. al Centro Nacional de Seguridad Digital a través de PECERT: pecert@pcm.gob.pe / Teléfono 2197000 Anexo 5109	OTIDG	Equipo de Respuesta Ante Incidentes de Seguridad Digital
11	Realizar la investigación del incidente de S.I., incluyendo la recopilación de la información y el manejo de la evidencia forense (Ver **Anexo III Manejo de Evidencia Forense**)	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Oficial de Seguridad de la Información / Equipo de Respuesta Ante Incidentes de Seguridad Digital
12	Gestionar la realización de una denuncia ante la DIVINDAT en caso lo determine el Oficial de Seguridad de la Información, con base en la investigación interna	OTIDG	Oficial de Seguridad de la Información / Jefe de OTIDG
13	Plantear la solución planteada para el caso (Atención, Requerimiento, Evento o Incidente de S.I.) (Ver **Anexo IV – Responsabilidades Específicas Según Categoría del Caso**)	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Oficial de Seguridad de la Información / Equipo de

			Respuesta Ante Incidentes de Seguridad Digital
14	Aprobar la solución planteada para el caso (Atención, Requerimiento, Evento o Incidente de S.I.) (Ver **Anexo IV – Responsabilidades Específicas Según Categoría del Caso**)	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Oficial de Seguridad de la Información / Equipo de Respuesta Ante Incidentes de Seguridad Digital
15	Comunicar la resolución vía correo electrónico a los involucrados	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información
16	Elaborar **Informe Técnico** para los casos: Incidente de S.I., Evento de S.I.; cambio por ejecución de garantía, baja o alta de equipo, solicitar servicios de terceros o si la unidad orgánica lo requiere	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información
17	Validar el **Informe Técnico**, en caso haya sido aplicable.	OTIDG	Jefe de Oficina de Tecnología de la Información
18	Solicitar a la URH la activación de la directiva correspondiente al proceso disciplinario, en caso sea aplicable de acuerdo con los resultados del informe técnico, cuando concluyan que un servidor cometió una infracción a las políticas y normativas de seguridad de la información.	OTIDG	Jefe de Oficina de Tecnología de la Información
19	Recepcionar la solución planteada de la atención y comunicar la conformidad o no conformidad del servicio	Unidad Orgánica	Personal Unidad Orgánica
20	Derivar el caso para nueva revisión, si no fue resuelto.	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información

21	Cerrar caso.	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información
Fin del procedimiento			
DOCUMENTOS QUE SE GENERAN (Documento de salida del procedimiento)			
Correo electrónico			
Registro de atenciones, eventos e incidentes de Seguridad de la Información			
Informe Técnico (Si aplica)			

"Toda copia impresa es un Documento No Controlado a excepción del original"

ANEXO I – TABLA DE PLANIFICACIÓN DEL MONITOREO DE EVENTOS DE SISTEMAS

N°	Logs que se generan	¿Quién monitorea?	Frecuencia
1	Logs del Firewall (a través del analizador de logs que corresponda)	Coordinador de Operaciones	Diario
2	Sistema de gestión de eventos e información de seguridad (Dashboard y Logs según necesidad)	Coordinador de Operaciones	Diario
3	Antivirus institucional	Coordinador de Operaciones	Diario
4	Logs sistemas publicación	Coordinador de Desarrollo	Mensual
5	Logs Consola Admin Correo	Coordinador de Operaciones	Mensual
6	Logs de Switch Core	Coordinador de Operaciones	Mensual
7	Logs de Acess Points	Coordinador de Operaciones	Mensual
8	Logs de UPS	Coordinador de Operaciones	Diario
9	Logs de aplicaciones	Coordinador de Operaciones, Coordinador de Desarrollo y Coordinador de BDG	Mensual
10	Logs de Servidores como hardware	Coordinador de Operaciones, Coordinador de Desarrollo y Coordinador de BDG	Mensual
11	Logs de sistemas operativos, incluye los del Servicio de Directorio	Coordinador de Operaciones, Coordinador de Desarrollo y Coordinador de BDG	Mensual
12	Logs asociados a periféricos	Coordinador de Operaciones, Coordinador de Desarrollo y Coordinador de BDG	Mensual
13	Logs de actividades de administradores	Oficial de Seguridad de la Información	Mensual

ANEXO II – CLASIFICACIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Definiciones	Evento de seguridad de la información (Ocurrencia identificada en un sistema de información, servicio o estado de la red que indica una posible infracción en la seguridad de la información, en la política o fallo en los controles)	Incidente de seguridad de la información (Un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información)
Criterio de clasificación	Para fines prácticos, consideramos evento de seguridad de la información a toda ocurrencia que implicó un incumplimiento o un intento de trasgresión que no afectó directamente la confidencialidad, disponibilidad o integridad de la información	Para efectos prácticos, consideraremos incidente a todo evento que afectó directamente la confidencialidad, disponibilidad o integridad de la información.
Ejemplos	Puerta de oficina dejada abierta	Robo de archivo de la oficina
	Usuario / Contraseña anotados en post-it sobre la pantalla de terminal	Persona no autorizada ingresó a repositorio y bajó documentos internos
	Extravío de llave asignada a un funcionario	Robo de laptop usando llave extraviada
	Antivirus desactualizado	Ingreso de un e-mail worm, haciendo inservibles reportes operativos históricos
	Activo de información físico	Activo de información físico se

	es trasladado sin cumplir con el método específico de embalaje para su protección	daña como consecuencia de ser trasladado sin el embalaje apropiado.
	Generador eléctrico sin combustible diesel	Ante falla de energía eléctrica prolongada, los UPS se descargaron y hubo interrupción de servicios
	Detectar un posible ataque de denegación de servicio en la web “Ultimo Sismo”, sin consecuencias.	Detectar un ataque de denegación de servicio en la web “Último Sismo”, con consecuencias negativas, como conexiones abortadas para personas que requerían consultar esta web con fines legítimos.

ANEXO III – MANEJO DE EVIDENCIA FORENSE

Cuando sea requerido para fines relacionados con acciones disciplinarias o legales (con una denuncia policial), se debe preservar y proteger la evidencia relacionada con el incidente de seguridad de la información. Esto incluye:

- Si es posible, identificar a la persona u organización bajo investigación.
- Identificar y recolectar los activos que pueden ser o contener evidencias, recabando información sobre sus características técnicas (marca, modelo, número de serie y otros según corresponda)
- Cuando se tenga que custodiar un activo, esto solo será realizado por el Oficial de Seguridad de la Información, de modo que no exista una cadena de custodia larga que pueda incorporar mayores riesgos.
- Asegurar la escena y proteger la evidencia. En la medida de lo posible, asegurar de manera especial los ambientes físicos involucrados, por ejemplo, a través del lacrado de oficinas. El hardware también será protegido a través de su lacrado. De esta manera se evita que no sea confiable el posterior análisis.
- En caso la investigación sea para fines de acciones disciplinarias, la adquisición de evidencia podrá ser realizada por el equipo de OTIDG (como la revisión de logs, reportes de los sistemas informáticos o solicitud de registros de videovigilancia); en caso la investigación sea para fines de acciones legales, como denuncias policiales, la adquisición de evidencia y análisis forense (como imágenes forenses o copias bit a bit de un dispositivo de almacenamiento y otras técnicas de análisis forense) serán requeridos a la División de Investigación de Delitos de Alta Tecnología – DIVINDAT, de la Policía Nacional del Perú.
- En casos donde sea necesario, poner en funcionamiento los sistemas redundantes para minimizar la manipulación de los sistemas para preservar la disponibilidad.

Datos de contacto de DIVINDAT		
Teléfono fijo	Teléfono móvil	Correo electrónico
431-8898	942440729	dirincri.divindat.pi@pnp.gob.pe

ANEXO IV – RESPONSABILIDADES ESPECÍFICAS SEGÚN CATEGORÍA DEL CASO

Categoría del Caso	Responsable de Plantear la Solución o Respuesta	Responsable de Aprobar la Solución o Respuesta
Atención	Coordinador Responsable de Operaciones de Tecnologías de la Información	Coordinador Responsable de Operaciones de Tecnologías de la Información
Requerimiento	Coordinador Responsable de Operaciones de Tecnologías de la Información	Jefe de OTIDG
Evento de Seguridad de la Información	Coordinador Responsable de Operaciones de Tecnologías de la Información	Oficial de Seguridad de la Información
Incidente de Seguridad de la Información	Coordinador Responsable de Operaciones de Tecnologías de la Información Oficial de Seguridad de la Información	Equipo de Respuesta Ante Incidentes de Seguridad Digital

PROCEDIMIENTO PR 020-2019-IGP

RESPALDO DE LA INFORMACIÓN

Versión 03

IGP V.B.

Firmado digitalmente por:
DELGADO ORTEGA Edgar FAU
20131367008 hard
Motivo: Doy V° B°
Fecha: 22/11/2020 17:29:10-0500

PROCEDIMIENTO PR 020-2019-IGP

RESPALDO DE LA INFORMACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN
01 02	12/10/2019 22/11/2020	1. Documento Inicial 2. Se modifica la estructura y codificación y se actualiza la secuencia de actividades.
FORMULADO **OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y DATOS GEOFÍSICOS**	**REVISADO Y VISADO** **OFICINA DE PLANEAMIENTO Y PRESUPUESTO**	**REVISADO Y VISADO** **OFICINA DE ASESORÍA JURÍDICA**
APROBADO **GERENCIA GENERAL**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)**	**REVISADO Y VISADO** **(DENOMINACIÓN DE ORGANO/UNIDAD ORGANICA)**

RESPALDO DE LA INFORMACIÓN

IGP Instituto Geofísico del Perú	INSTITUTO GEOFÍSICO DEL PERÚ
	FICHA TÉCNICA DEL PROCEDIMIENTO

DATOS DEL PROCEDIMIENTO			
Nombre del procedimiento	RESPALDO DE LA INFORMACIÓN	Objetivo del procedimiento	Garantizar la disponibilidad, seguridad y confidencialidad de la información Institucional mediante la gestión de las copias de respaldo+
Código del Proceso relacionado	S03	Alcance del procedimiento	Este procedimiento aplica a todos los respaldos de información realizados por la Oficina de Tecnología de Información y Datos Geofísicos.
Versión	3		

Base Normativa (Son disposiciones legales que soportan el procedimiento)	
Ley Nº 27658, Decreto Legislativo Nº 1446 (modificatoria)	Ley Marco de Modernización del Estado
Decreto Supremo Nº 004-2013-PCM	Política Nacional de Modernización de Gestión Pública al 2021

Siglas y Definiciones (Abreviaturas y acrónimos)
Sistema Operativo: Programa o conjunto de programas que actúan como intermediarios entre las aplicaciones de los usuarios (Software) y el equipo físico (Hardware) de la máquina, ocultando las características particulares de este último.

Aplicaciones: Nombre que reciben los programas especializados en tareas concretas y de una cierta complejidad.
Bases de Datos: Es la colección de información, que está organizada de forma tal que su contenido sea fácilmente accedido, administrado y actualizado.
Custodia: Se entrega al cuidado de una persona natural o jurídica.
Respaldo: Sinónimo de Backup.
Backup: Copia idéntica de algo, copia de seguridad o copia respaldo de algo

Elemento de Entrada (Requisitos para iniciar el procedimiento)	
Descripción del Requisito	**Fuente**
Cronograma de respaldo de información o solicitud por correo	Unidad Orgánica, OTIDG

ACTIVIDADES (Actividad, Unidad de Organización y Responsable)			
Nº	**Descripción de la Actividad**	**Unidad de Organización (*)**	**Responsable**
1	Realizar el respaldo periódico en el servidor de respaldo asignado a cada responsable o en el servidor temporal de acuerdo con el **Anexo I Planificación del Respaldo Periódico en Servidores de Producción y Servidor Temporal**	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Coordinador de Ingeniería de Software / Especialista en Sistemas de Información Administrativa
2	Validar condiciones para el inicio del **Programa de Respaldo de la información**	OTIDG	Analista en Sistemas de Tecnologías de la Información

3	Reprogramar inicio de respaldo, registrar esto en el **Programa de Respaldo de la Información**	OTIDG	Analista en Sistemas de Tecnologías de la Información
4	Coordinar con responsables de ejecutar respaldo, según **Anexo I Planificación del Respaldo Periódico en Servidores de Producción y Servidor Temporal**	OTIDG	Analista en Sistemas de Tecnologías de la Información
5	Notificar y coordinar con interesados (para respaldo de PCs).	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Coordinador de Ingeniería de Software / Especialista en Sistemas de Información Administrativa
6	Ejecutar Backup en servidor de respaldo (de PCs)	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Coordinador de Ingeniería de Software / Especialista en Sistemas de Información Administrativa
7	Verificar el resultado de la ejecución del respaldo de PCs.	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Coordinador de Ingeniería de Software / Especialista en Sistemas de Información Administrativa
8	Informar el término del respaldo de backup de PCS.	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Coordinador de Ingeniería de Software / Especialista en Sistemas de Información Administrativa
9	Centralizar copia de respaldo de servidores asignados a cada responsable.	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Coordinador de Ingeniería de Software / Especialista en Sistemas de Información Administrativa
10	Ejecutar respaldo en cintas.	OTIDG	Responsable de ejecutar respaldo en cintas
11	Verificar el resultado de la ejecución del respaldo en cintas. Registrar en **Registro de respaldo de la información**	OTIDG	Responsable de ejecutar respaldo en cintas

12	Informar el término del respaldo en cintas y el cumplimiento de las condiciones de conservación y seguridad de las cintas según **Anexo II Condiciones de almacenamiento y funcionamiento de cintas de respaldo**	OTIDG	Responsable de ejecutar respaldo en cintas
13	Verificar registro e informar a jefatura OTIDG el término del Backup y coordinar la programación de pruebas de validación.	OTIDG	Analista en Sistemas de Tecnologías de la Información
14	Realizar periódicamente una prueba de recuperación de información con base en los respaldos vigentes y generar el registro correspondiente, según **Cronograma de Pruebas de Recuperación de Información Respaldada** y según las responsabilidades en **Anexo I Planificación del Respaldo Periódico en Servidores de Producción y Servidor Temporal,** generando un **Informe Técnico**	OTIDG	Coordinador Responsable de Operaciones de Tecnologías de la Información / Coordinador de Ingeniería de Software / Especialista en Sistemas de Información Administrativa

Fin del procedimiento
DOCUMENTOS QUE SE GENERAN (Documento de salida del procedimiento)
Programa de respaldo de la información
Registro de respaldo de la información
Cronograma de Pruebas de Recuperación de Información Respaldada
Informe Técnico

“Toda copia impresa es un Documento No Controlado a excepción del original”

ANEXO I – PLANIFICACIÓN DEL RESPALDO PERÓDICO EN SERVIDORES DE PRODUCCIÓN Y SERVIDOR TEMPORAL

Información	Responsable	Origen de la información	Destino en servidor de backup	Frecuencia	Tipo de copia
Sistema de trámite documentario (STD) (base de datos)	Coordinador Responsable de Operaciones de Tecnologías de la Información	Servidor de producción de STD	D:\Backup-STD\incremental	Diario	Incremental
Sistema de trámite documentario (STD) (base de datos, aplicaciones y almacén de archivos)			D:\Backup-STD\backup	Semanal	Completo
Máquinas virtuales (Servicio de Directorio, DNS, Controlador de Dominio, DHCP, servidor de impresiones)		Servidor de producción de cada servicio	Servidor temporal	Trimestral	Completo
Copias de respaldo de las computadoras del sistema de publicación (imagen)		Computadoras del sistemas de publicación	Servidor temporal	Semestral	Completo
Código fuente de soluciones informáticas	Coordinador de Ingeniería de Software	Servidor de producción	/data/backup/<ip_server>	Diario	Sobreescritura
Datos de las soluciones informáticas (de producción)					
SIAF (base de datos no relacional y aplicaciones)	Especialista en Sistemas de Información Administrativa	Servidor de producción de cada sistema	D:/3.-BK-DATA-2020\mes	Diario	Completo
SIGA (base de datos y aplicaciones)			D:/BACKUP/MES		Completo

ANEXO II – CONDICIONES DE FUNCIONAMIENTO Y ALMACENAMIENTO DE CINTAS DE RESPALDO

Condición	Especificación
Condiciones de funcionamiento	• 10°C – 45°C (50°F – 113°F); 10% – 80% RH; 26°C (79°F) máximo del bulbo húmedo
Condiciones de almacenamiento en periodos cortos	• 16°C – 35°C (61°F – 95°F); 20% – 80% RH; 26°C (79°F) máximo del bulbo húmedo
Condiciones de almacenamiento en periodos largos	• 16°C – 25°C (61°F – 77°F); 20% – 50% RH; 26°C (79°F) máximo del bulbo húmedo
Condiciones de envío	• -23°C – 49°C (-9°F – 120°F); 20% – 80% RH; 26°C (79°F) máximo del bulbo húmedo

Fuente: https://www.ibm.com/pe-es/marketplace/ibm-lto-ultrium-6-data-cartridge/details