UNP

Protocolo

DE CONTINGENCIA PARA ATENCIÓN DE CRISIS EN TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

GTE-PT-02-V1

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
29-11-2024

Tabla de Contenido

INTRODUCCIÓN

El protocolo de contingencia para atención de crisis se aplicará en caso de que un desastre interfiera con temas de seguridad de la información para atender las aplicaciones de operación misional y no misional critica de la entidad, el protocolo de contingencia para atención de crisis debe ser utilizado por las personas responsables en la coordinación y recuperación de la capacidad de la plataforma tecnológica y soporte de la operación misional de la entidad. El protocolo de contingencia para atención de crisis está diseñado para contener o proporcionar referencia a toda la información que podría ser necesaria en el momento de la recuperación de la capacidad de la plataforma tecnológica.

Este protocolo de contingencia para atención de crisis no pretende cubrir las operaciones del Equipo de Respuesta a Emergencias estructurado por la Subdirección de Talento Humano, Grupo de Seguridad y Salud en el Trabajo.

Índice de acrónimos: (EOC) Centro de operaciones de emergencia - (EMT) Equipo de administración de emergencias - (ERE) Equipo de respuesta a emergencias - (PAC) El protocolo de contingencia para atención de crisis (IT) Tecnología de la información

El presente protocolo, establece responsabilidades para las pruebas de continuidad en la operación tecnológica, capacitación y actividades de mantenimiento que son necesarias para garantizar la viabilidad continua del protocolo de contingencia para atención de crisis.

De otra parte, describe la estrategia del Grupo de Gestión de las Tecnologías con el fin de mantener la continuidad del negocio en caso de una interrupción causada por un desastre en las instalaciones de la UNP. Estas decisiones determinarán el contenido de los planes de acción, y podrán cambiarse en cualquier momento, en consecuencia, el protocolo de contingencia para atención de crisis se deberá ajustar.

En el capítulo Equipos de recuperación, se enumeran las funciones del Equipo de recuperación, las personas a las que se asignan responsabilidades específicas y los procedimientos de notificación a cada uno de los miembros del equipo.

La capitulo Procedimientos del equipo, determina qué actividades y tareas se deben realizar, en qué orden y quién debe hacerlo para adelantar la recuperación de la plataforma tecnológica de la entidad.

1. OBJETIVO

El objetivo del protocolo de contingencia para atención de crisis es tener una herramienta metodológica para la recuperación de las aplicaciones misionales y no misionales críticas instaladas en la Infraestructura Tecnológica de la entidad, esto en caso de una interrupción por desastre. Lo anterior puede incluir desastres de pequeña y gran magnitud, tales como incendios, inundaciones, terremotos, explosiones, terrorismo, tornados, interrupciones prolongadas del suministro eléctrico, derrames químicos peligrosos y otros desastres naturales o causados por el hombre.

Un desastre se define como cualquier evento que hace que una instalación comercial sea inoperable o inutilizable, de modo que interfiera con la capacidad de la organización para brindar servicios esenciales usuarios tanto internos como externos de la UNP.

Un protocolo de contingencia de atención de crisis suele incluir los siguientes elementos:

- **Identificación de riesgos**: El primer paso en la creación de un protocolo es identificar los riesgos específicos a los que está expuesta la organización. Esto puede hacerse mediante una evaluación de riesgos que considere factores como la ubicación de la organización, sus operaciones y sus sistemas informáticos.
- **Estrategias de mitigación**: Una vez que se han identificado los riesgos, la organización debe desarrollar estrategias para mitigarlos. Esto puede implicar medidas como la implementación de copias de seguridad, la contratación de un seguro y la capacitación del personal en respuesta a desastres.
- **Procedimientos de respuesta:** El protocolo debe identificar los procedimientos que la organización seguirá en caso de un desastre. Estos procedimientos deben ser claros y concisos, y deben estar diseñados para garantizar que la organización pueda continuar operando de forma eficaz.
- **Procedimientos de recuperación:** El protocolo también debe identificar los procedimientos que la organización seguirá para recuperar sus operaciones después de un desastre. Estos procedimientos deben ser detallados y deben incluir un cronograma para la recuperación.

Las prioridades en una situación de desastre son:

1. Garantizar la seguridad de los servidores públicos, contratistas y visitantes en los edificios de oficinas. (Responsabilidad de la Equipo de Respuesta a Emergencias)

2. Mitigar las amenazas que puedan causar un daño potencial. (Responsabilidad de la Equipo de Respuesta a Emergencias)

3. Contar con medidas avanzadas para garantizar que las funciones misionales críticas de la entidad puedan continuar.

4. Tener planes y procedimientos documentados para garantizar la ejecución rápida y efectiva de las estrategias de recuperación para funciones misionales críticas.

5. El protocolo de contingencia para atención de crisis incluirá procedimientos para la recuperación de las aplicaciones misionales y no misionales críticas de la entidad, tal como se define en la sección Estrategia de este documento.

2. ALCANCE

El protocolo de contingencia para atención de crisis tiene un alcance limitado para la recuperación y la continuidad de las funciones misionales críticas, en el caso que se presente una interrupción seria de los servicios de infraestructura tecnológica en la UNP, el protocolo de contingencia para atención de crisis se enfocará en recuperar la funcionalidad de las aplicaciones, plataformas, software, internet y demás aspectos críticos para la seguridad de la información. Este protocolo de contingencia para atención de crisis, enfocándose solo en la recuperación de las aplicaciones críticas para dar cumplimiento al objeto misional de la entidad, como aplicaciones, bases de datos, servidores u otra infraestructura tecnológica requerida dada la necesidad. A menos que se modifique, este protocolo no aborda las interrupciones temporales y que están en el marco de los tiempos determinados como críticos para las operaciones de terceros enmarcadas en los acuerdos de nivel de servicios.

3. DEFINICIONES

Activo: En relación con la seguridad de la información se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. https://gobiernodigital.mintic.gov.co/692/articles-237872_maestro_mspi.pdf

Amenaza: Toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información, lo cual significa que podría tener un potencial efecto negativo sobre algún elemento de los sistemas. Las amenazas pueden originarse de ataques (fraude, robo, virus), sucesos naturales (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). En una organización pueden ser internas o externas https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Por%20su%20parte%2C%20una%20amenaza,alg%C3%BAn%20elemento%20de%20nuestros%20sistemas.

Árbol de Llamadas (Call tree): Proceso (sistema) en cascada de un grupo de personas, roles y/u organizaciones para que sean contactados como parte del procedimiento de activación del plan ante un evento de interrupción. Elaboración propia a partir de la red

BIA - Business Impact Analysis: Proceso de evaluación de las operaciones y del efecto que una interrupción tendría en ellas. Incluye no sólo el análisis de impacto al negocio, que es la identificación de los procesos críticos, sino también la evaluación de los posibles daños o

pérdidas que pudieran afectar a la Organización como resultado de una interrupción. Elaboración propia a partir de la red

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, manuales, procedimientos, guías y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal. https://web.icetex.gov.co/documents/20122/75168/modelo-seguridad-privacidad-digital.pdf

Continuidad de Negocios: Capacidad de la organización para continuar desarrollando los productos o servicios en un nivel aceptable predefinido, posterior a un incidente. https://www.sire.gov.co/iw_IL/pcn?p_p_auth=AxUHeK2T&p_p_id=49&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&_49_struts_action=%2Fmy_sites%2Fview&_49_groupId=82884&_49_privateLayout=false

Copias de Seguridad: Copias de la información que se realizan utilizando medios de almacenamiento como cintas, discos compactos, etc., que sirven como respaldo en caso de que la información original sea afectada. Elaboración propia a partir de la red

Capacidad institucional o de negocio: Una habilidad particular que una entidad puede poseer o intercambiar para lograr un propósito específico. Elaboración propia a partir de la red

Canales de Comunicación: Identifica los mecanismos que se utilizarán para comunicarse con los grupos de interés y permitir el acceso a la información como reuniones, boletines, repositorios, fondos de escritorio, etc. https://gobiernodigital.mintic.gov.co/692/articles-272872_Conceptos_clave_Arquitectura.docx#:~:text=Canales%20de%20Comunicaci%C3%B3n,%2C%20fondos%20de%20escritorio%2C%20etc.

Criterios de aceptación: Son un conjunto preciso y bien definido de condiciones que un producto que se va a adquirir o construir debe satisfacer en el momento de su entrega, para que sea aceptado por una entidad. https://colaboracion.dnp.gov.co/CDTI/Oficina%20Informatica/Sistemas%20de%20informaci%C3%B3n/Gu%C3%ADas%20Formatos%20Plantillas/Gu%C3%ADa%20para%20la%20Elaboraci%C3%B3n%20y%20Presentaci%C3%B3n%20de%20Casos%20de%20Uso.pdf?#:~:text=%2D%20Criterios%20de%20aceptaci%C3%B3n.,entrega%2C%20para%20que%20sea%20aceptado.

Desastre: Situación que produce pérdidas humanas, materiales, económicas o ambientales que superan la capacidad de la organización, comunidad o sociedad que se ve afectada para responder y recuperarse a partir de sus propios recursos. Elaboración propia a partir de la red

Disponibilidad: Cuando el activo está accesible en el momento que lo desee un usuario autorizado. Elaboración propia a partir de la red

Integridad: Exactitud y consistencia generales de los datos, dicho de otro modo, la ausencia de alteración al momento de realizar cualquier tipo de operación con los datos, lo que significa

que estos permanecen intactos y sin cambios. https://www.normaiso27001.es/referencias-normativas-iso-27000/

Crisis: Evento crítico que, si no se maneja de manera adecuada, podría afectar drásticamente la rentabilidad, reputación o capacidad operativa de una Organización, o bien, un suceso o percepción de amenaza a las operaciones, al personal, los accionistas, las partes interesadas, la marca, la reputación y la confianza o los objetivos estratégicos o de negocio. https://drimexico.org/inicias-tu-carrera-en-continuidad-de-negocio/

Equipo Funcional: Grupo de personas encargadas de la recuperación operativa de las actividades y/o procesos críticos de la organización ante un evento de Interrupción, de llevar a cabo todas las estrategias de recuperación y los procedimientos necesarios para retomar las funciones del negocio. Elaboración propia a partir de la red

Escenarios de Interrupción: Escenarios que pueden ser activados por uno o varios eventos de riesgo, independientes o combinados. Elaboración propia a partir de la red

Estrategia de Continuidad de Negocio: Mecanismo de respuesta de una organización, que busca asegurar el cumplimiento de los objetivos de recuperación requeridos por los procesos críticos del negocio, frente a la materialización de cualquier evento que pueda conllevar a la indisponibilidad de la operación o una interrupción de las actividades de misión crítica de los procesos. Elaboración propia a partir de la red

Evento de Interrupción: Un evento que impacta la capacidad de la organización para continuar sus operaciones. Elaboración propia a partir de la red

Gestión de Riesgo: Es un enfoque estructurado para manejar el grado de incertidumbre relativa frente a una amenaza, mediante una secuencia de actividades humanas que incluyen la evaluación de riesgo, las estrategias de desarrollo su tratamiento y mitigación utilizando recursos administrativos y gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, eliminarlo, reducir sus efectos negativos y aceptar algunas o todas las consecuencias de este. https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_riesgos#:~:text=La%20gesti%C3%B3n%20de%20riesgos%20(traducci%C3%B3n,las%20estrategias%20de%20su%20tratamiento

Interdependencias: Se estudian las dependencias o interrelaciones que cada una de las unidades de negocio de la Organización tiene con las demás, realizando el análisis a nivel tanto interno como externo. Elaboración propia a partir de la red

Incidente: Evento adverso que podría causar alteración, pérdida o emergencia, pero no satisface los criterios de la organización para la crisis o su definición. Elaboración propia a partir de la red

Procesos Críticos: Aquellos a los que se les definirá e implementará una Estrategia de Continuidad de Negocio a los cuales se les dará prioridad después de la ocurrencia de un incidente, para mitigar los posibles impactos. Elaboración propia a partir de la red

Procesos No Críticos: Aquellos que no generan impactos significativos para la Organización ante una detención en un incidente de interrupción. Estos procesos no se tendrán en cuenta dentro de la estrategia y Planes de Continuidad de Negocio. Elaboración propia a partir de la red

Registros Vitales: Información (física o magnética) requerida por los procesos críticos para su operación. Elaboración propia a partir de la red

RPO – Recovery Point Objective: Punto máximo de tolerancia a la pérdida de información para un proceso crítico. Se define como el tiempo máximo permitido para la organización para realizar copias de respaldo y de recuperación de la información. Elaboración propia a partir de la red

RTO – Recovery Time Objective: Tiempo máximo que puede estar detenido un proceso crítico antes de afectar considerablemente a la Organización. Elaboración propia a partir de la red

MTPD – Maximum Tolerable Period of Disruption: Máximo tiempo permitido antes de que para la Organización sea inviable continuar en operación por la imposibilidad de realizar sus actividades críticas. Elaboración propia a partir de la red

Vulnerabilidad: En términos de informática, se trata de la debilidad o el fallo en un sistema de información que coloca en riesgo la seguridad de la información, lo cual facilita que un atacante comprometa la integridad, disponibilidad o confidencialidad de esta. Por lo tanto, es necesario identificarlas y eliminarlas lo antes posible Elaboración propia a partir de la red

4. RESPONSABILIDADES

La viabilidad del protocolo de contingencia para atención de crisis se basó en las siguientes necesidades:

1. Que exista un protocolo de contingencia para atención de crisis viable y probado en caso de que se presente un desastre. El protocolo de contingencia para atención de crisis se pondrá en funcionamiento para restaurar los servicios críticos que presta el centro de datos en un sitio de respaldo dentro de plazo en tiempo (RPO).

2. Que el protocolo de contingencia para atención de crisis se mantenga y actualice correctamente según sea necesario.

3. Las funciones y roles a los que se hace referencia en este protocolo de contingencia para atención de crisis no tienen que existir previamente dentro de la UNP; pueden asignarse a una o más personas como nuevas responsabilidades, o delegarse a un tercero externo si se puede organizar y asignar un presupuesto para tales servicios

4.1 Responsabilidades de Mantenimiento

El protocolo de contingencia para atención de crisis es responsabilidad del Grupo Interno de Trabajo de Tecnología de la Información, en cabeza del Coordinador o líder de tecnología.
El protocolo debe ser evaluado y actualizado cuando se presente un cambio significativo en los servicios de infraestructura tecnológica, teniendo en cuenta los diferentes procesos de prueba, cambios en la infraestructura tecnológica y las auditorías donde se generan las mejoras a desarrollar.

Entonces, para lograr la mejora continua del protocolo se considera importante realizar auditorías internas de manera periódica. La revisión constante del protocolo es de gran importancia, dado que hay factores que pueden ocasionar cambios en este y que se generan por aspectos inherentes al modelo de negocio, los cuales podrían ser:

• Cambios en los organigramas en relación con los cargos.
• Cambios de personal.
• Cambio de ubicación de las instalaciones físicas.
• Ingreso de nuevos proveedores para los servicios críticos.
• Modificaciones en las configuraciones de los sistemas o las unidades de almacenamiento.
• Modificaciones en la infraestructura de redes.
• Integración o desarrollo de nuevas aplicaciones.
• Cambios en las estrategias del negocio de la organización y los riesgos identificados inicialmente.

Grupo Interno de Trabajo de Tecnología de la Información

es responsable de:

1. Revisar cada 12 meses la vigencia y adecuación del procedimiento para la aplicación del protocolo de contingencia para atención de crisis.

2. Evaluar el impacto en el protocolo de contingencia para atención de crisis en los de posibles cambios en la misionalidad de la UNP, de posibles cambios de los procedimientos de Grupo Interno de Trabajo de Tecnología de la Información, de los equipos y software mínimos necesarios para que sea funcional la plataforma tecnológica de la entidad.

3. Mantener las funciones del equipo de Servidor Público del área de Tecnología de la Información actualizadas, teniendo en cuenta los cambios, encargos y terminaciones que se puedan dar dentro de la planta de personal.

La oficina asesora de planeación e información - OAPI

es responsable de:

El Coordinador o líder del grupo de tecnología de la información es responsable de:

1. Mantener actualizado el protocolo de contingencia para atención de crisis, de acuerdo a posibles cambios en las funciones críticas de la entidad.

2. Coordinar cambios entre planes y mantener comunicación con la alta dirección cuando se requiera afectar las acciones criticas dentro del protocolo de contingencia para atención de crisis de la entidad.

4.2 Responsable en la aplicación de pruebas del protocolo de contingencia para atención de crisis.

El jefe de la oficina asesora de planeación es responsable de garantizar la viabilidad del plan de contingencia en el tiempo. Esto deberá verificarse periódicamente mediante pruebas.
Asegurar un plan de pruebas, entrenamiento y ejercicios. Las pruebas validan las capacidades de recuperación, mientras que la capacitación prepara al personal de recuperación para la activación del plan y los ejercicios identifican brechas en los planes de contingencia. La realización de estas actividades mejora la eficacia del plan y capacita a las organizaciones ante un evento o incidente de interrupción

Basados en las buenas prácticas del estándar ISO/IEC 22301:2019, el cual establece los lineamientos que se deben llevar a cabo para realizar la implementación de sistemas de gestión de continuidad del negocio, se debe tener presente lo siguiente:

La organización debe implementar y mantener un programa de ejercicios y pruebas para validar, a lo largo del tiempo, la eficacia de sus soluciones y estrategias para la continuidad del negocio. La organización debe conducir ejercicios y pruebas:

- Que sean consistentes con los objetivos para la continuidad del negocio.
- Se basen en escenarios adecuados, bien planificados, con objetivos y propósitos claramente definidos.
- Desarrollen el trabajo en equipo, competencia, confianza y conocimiento para aquellos que tienen que desempeñar funciones, en relación con las interrupciones.
- Validen las estrategias y soluciones para la continuidad del negocio a lo largo del tiempo.
- Produzcan reportes formalizados después de los ejercicios que contengan resultados, recomendaciones y acciones para implementar mejoras.
- Se revisen en el contexto de promoción de mejora continua.
- Se desarrollen en intervalos predeterminados y cuando hay cambios significantes dentro de la organización o el contexto en la cual opera.

En ese sentido, la organización debe actuar de acuerdo con los resultados de los ejercicios y las pruebas para implementar cambios y mejoras. Por lo anterior, resulta imperativo llevar a cumplimiento las obligatoriedades y recomendaciones que están inmersas en el estándar, para materializar la ejecución de los planes de pruebas, con el propósito de verificar la resiliencia de los planes y realizar la actualización de cualquier eventualidad que pudiese presentarse.

5. CONDICIONES GENERALES

La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de la información a través de la definición de un conjunto de procesos, normas y herramientas para la gestión eficaz de acceso a la información y la implementación de mecanismos y controles de seguridad tanto físicos como lógicos, orientados a la prevención y detección de amenazas que puedan afectar la seguridad de la organización y la continuidad del negocio.
La finalidad de la seguridad de la información es su protección, independiente del medio en que se encuentre, ya sea impresa, medio digital, sistemas de información, almacenado en dispositivos de almacenamiento externo, oral u otros, contra las amenazas y eventos que atenten contra el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada y que puedan afectar la confidencialidad, integridad y disponibilidad de la información, el presente documento describe las actividades de cumplimiento y las estrategias de continuidad definidas por la UNP en caso de que se presenten interrupciones de los servicios prestados en cumplimiento de la misionalidad.

6. CONTENIDO

A continuación, se desarrolla el contenido del protocolo de contingencia para la atención de crisis en tecnología y seguridad de la información en la Unidad Nacional de protección – UNP.

6.1 Estrategia Protocolo de Contingencia de la Plataforma Tecnológica

Este capítulo del protocolo de contingencia para atención de crisis se describe la estrategia diseñada para mantener la continuidad de las aplicaciones misionales y no misionales criticas soportadas en Plataforma de Tecnológica de la entidad en caso de que se genere una interrupción operacional por un desastre. Esta estrategia se invocaría si la instalación física principal de la UNIDAD NACIONAL DE PROTECCION, en su área de Infraestructura y Servicios de tecnología de la Información, de alguna manera se ve afectada por un desastre.

Dado a que no se cuenta con un documento maestro de protocolo de contingencia para atención de crisis, cada área dentro de la estructura organizacional y de acuerdo a la criticidad de sus funciones podrá tener su propio protocolo o procedimiento para la recuperación de sus funciones ante un desastre, que es similar a este protocolo, excepto que desde la definición de necesidades y los procesos y procedimientos críticos de recuperación se personalizaran de acuerdo a cada área dentro de la estructura organizacional de la entidad.

Una estrategia de contingencia es un mecanismo que permite la recuperación y continuidad de las funciones críticas de una organización frente a un desastre o una interrupción mayor. Son consideradas como estrategias no sólo los recursos y actividades requeridas frente a la interrupción, sino los requeridos para mitigar la probabilidad de ocurrencia y el impacto de la interrupción.

Para definir las estrategias de contingencia posibles o viables, de manera efectiva y eficiente, se debe contar con un entendimiento sobre los siguientes aspectos:

1. Resultados del Análisis de Impacto al Negocio (BIA).
2. Tiempos y puntos objetivo de recuperación (RTO y RPO) requeridos para los procesos críticos.
3. Procesos críticos a soportar
4. Porcentaje aceptable de degradación de la operación del proceso.
5. Aspectos de carácter jurídico que se deben cumplir según la naturaleza del proceso al momento de implementar una estrategia de recuperación.
6. Resultados del análisis de riesgos y las alternativas de tratamiento de riesgo a implementar sobre los activos asociados a los procesos.
7. Amenazas posibles a los activos de los procesos.
8. Vulnerabilidades existentes en los activos de los procesos.

El propósito consiste en seleccionar las estrategias de recuperación o continuidad, orientadas a brindarle confiabilidad a los servicios, considerando los resultados del BIA, la evaluación de riesgos y complementado lo anterior, con la realización de un análisis cuantitativo de los elementos requeridos para la recuperación.

Parte del desarrollo involucró la definición de los escenarios de interrupción, las amenazas que los pudieran generar y las diferentes alternativas operativas para enfrentar una posible materialización. En la siguiente tabla se visualiza la información referente:

Tabla 1. Escenarios de Interrupción

ESCENARIOS					
	INFRAESTRUCTURA NO DISPONIBLE	**TI NO DISPONIBLE**	**RECURSO HUMANO NO DISPONIBLE**	**PROVEEDOR NO DISPONIBLE**	**INFORMACIÓN NO DISPONIBLE**
AMENAZAS	1. Incendio, inundación, actos de violencia, terremoto 2. Cierre Parcial de la Entidad	1. Falla Eléctrica 2. Incendio 3. Inundación 4. Terremoto 5. Falla Tecnológica	1. Incendio 2. Actos de violencia 3. Terremoto 4. Cierre parcial 5. Ausencia, retiro del personal	1. Falla eléctrica 2. Incendio 3. Inundación 4. Falla tecnológica	1. Falla eléctrica 2. Incendio 3. Inundación 4. Sismo o terremoto 5. Fallas tecnológicas en: Comunicaciones, hardware, software, bases de datos 5. Error humano 6. Hurto o robo.
ALTERNATIVAS OPERATIVAS	1. Trabajo remoto 2. Acuerdos con terceros	1. Estrategias DRP	1. Definición de la estructura de recuperación 2. Capacitación 3. Rotación 4. Documentación de procedimientos operativos	1. Definir proveedores alternos 2. Definir acuerdos de niveles de servicios (ANS) específicos para el PCN	1. Respaldo de la información clave del proceso critico (Backup) 2. Proveedores y/o medios de alternos para el servicio de comunicación.

Fuente: Elaboración Propia

La siguiente información es la relación de alternativas operacionales que tiene la organización, para recuperar la funcionalidad de sus procesos críticos en términos de la ausencia de alguno(s) de sus recursos claves, estas estrategias pueden permitir la continuidad de sus operaciones más importantes en un nivel aceptable y buscan principalmente cumplir y satisfacer los requerimientos del producto solicitado por sus clientes, después de un evento de interrupción.

Tabla 2. Alternativas Operacionales

ALTERNATIVAS OPERACIONALES		
ESCENARIO DE INTERRUPCIÓN	**AMENAZAS**	**ALTERNATIVAS OPERATIVAS**
 NO DISPONIBILIDAD DE COLABORADORES DEL PROCESO	1. Huelga de Colaboradores 2. Pandemia 3. Intoxicación Colectiva 4. Indisposición del personal (Ausencia, retiro)	1. Definición de árboles de llamada. 2. Capacitación 3. Rotación 4. Documentación de procedimientos operativos

ALTERNATIVAS OPERACIONALES		
ESCENARIO DE INTERRUPCIÓN	**AMENAZAS**	**ALTERNATIVAS OPERATIVAS**
 NO DISPONIBILIDAD DE LA INFRAESTRUCTURA FÍSICA	1. Incendio 2. Inundación 3. Actos de Violencia 4. Sismo o Terremoto 5. Asonadas 6. Fugas de gas 7. Explosión	1. Teletrabajo 2. Acuerdo con terceros 3. Respaldo entre sedes (planta de producción) 4. Centro de Trabajo Alterno trabajo alterno para procesos administrativos
 NO DISPONIBILIDAD DE LOS SERVICIOS TECNOLÓGICOS	1. Falla Eléctrica 2. Incendio 3. Inundación 4. Sismo o Terremoto 5. Fallas tecnológicas en: Comunicaciones, Hardware, Software, Bases de Datos	1. Estrategias de DRP
 NO DISPONIBILIDAD DE INFORMACIÓN	1. Falla Eléctrica 2. Incendio 3. Inundación 4. Sismo o Terremoto 5. Fallas tecnológicas en: Comunicaciones, Hardware, Software, Bases de Datos 6. Error Humano 7. Hurto o Robo	1. Respaldo de la información clave del proceso (Back Up) 2. Proveedores y/o medios Alternos para el servicio de comunicación
 NO DISPONIBILIDAD DE PROVEEDORES Y/O TERCEROS	1. No disponibilidad del Proveedor por eventos propios de su operación: 2. Falla Eléctrica 3. Incendio 4. Inundación 5. Huelgas o Asonadas 6. Pandemias 7. Actos de Violencia 8. Sismo o Terremoto 9. Fallas tecnológicas 10. No disponibilidad de sus Proveedores	1. Definir proveedores alternos del servicio 2. Definir Acuerdos de Niveles de Servicio específicos para BCM

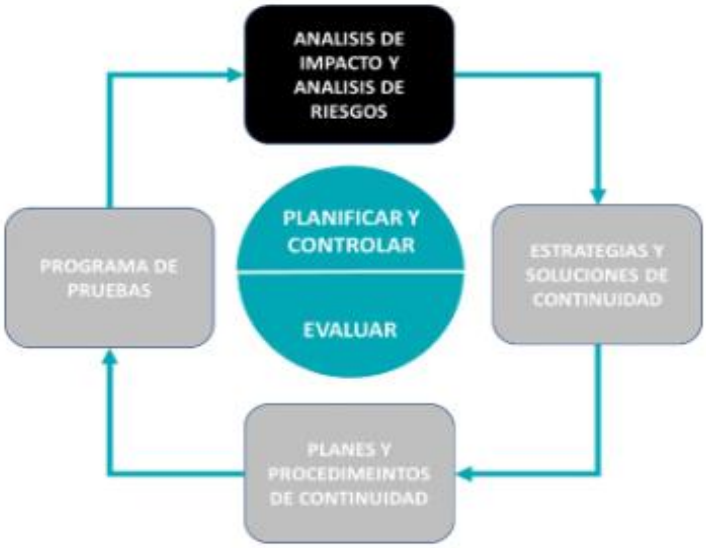
Fuente: Elaboración Propia

A. Evaluación de Riesgos

El propósito principal es conocer cuáles amenazas o riesgos específicos enfrenta la UNP en sus procesos o servicios críticos del negocio, identificados como resultado del Análisis

de Impacto de Negocio (BIA), con el fin de determinar la forma en que algunos riesgos serán controlados y mitigados a un nivel aceptable según criterios previamente definidos.

Figura 1. Análisis y evaluación de riesgos BCP



Fuente: https://controlsolutions360.com/planes-de-continuidad-de-negocio-01-preparando-el-analisis-de-impacto-y-riesgo

La etapa de identificación permite reconocer y describir el riesgo desde el análisis de las actividades ejecutadas por el proceso e identificar los posibles riesgos asociados. La etapa de análisis busca establecer la probabilidad de ocurrencia e impacto de sus efectos mediante la calificación y evaluación cuantitativa y cualitativa. La etapa de valoración comprende la identificación, descripción y calificación de los controles relacionados con el riesgo analizado, los cuales deben estar relacionados con las causas y los efectos identificados. Por último, el tratamiento determinará el manejo que se dará al riesgo considerando las estrategias que pueden incluir asumir, reducir, evitar, compartir o transferir el riesgo.

Las amenazas y vulnerabilidades que se incluyen para el caso específico del plan serán las relacionadas con la no disponibilidad (operación) de los activos asociados a los procesos críticos del negocio. Ahora bien, parte importante de contar con un protocolo de contingencia de atención de crisis, es el hecho de realizar una efectiva gestión de riesgo y así evitar las recursivas activaciones del sitio alterno, actividad que tiene sus propios riesgos, costos y dificultades.

En esta etapa, se analizaron las amenazas y vulnerabilidades identificadas previamente, analizando el escenario donde puede materializarse el riesgo de interrupción, así como su origen y las afectaciones potenciales a los activos, el análisis contempló 12 escenarios de riesgo que se describen a continuación:

1. **Acceso a la edificación:** Relaciona los controles, los procedimientos y las buenas prácticas que permiten mitigar el riesgo de que personal no autorizado ingrese a las instalaciones y pueda generar daños a los activos de la organización.
2. **Administración y entorno tecnológico:** Relaciona los hábitos y las buenas prácticas que permiten administrar, asegurar, disponer y controlar los sistemas tecnológicos, de tal forma que estén alineados con los estándares internacionales y regulaciones nacionales en temas de seguridad de la información.
3. **Construcción del edificio y materiales:** Relaciona los materiales de construcción, alternativas de mitigación y resistencia frente a riesgos naturales.
4. **Información y administración del edificio:** Relaciona procedimientos de seguridad, responsabilidades del personal, cultura y capacitación para responder a incidentes en el edificio.
5. **Oficina y estaciones de trabajo:** Relaciona las políticas de seguridad de la información definidas por la compañía y las buenas prácticas del personal que aseguren, en el evento de una interrupción del negocio, la disponibilidad, confidencialidad, seguridad e integridad de la información.
6. **Perímetro y estacionamiento:** Relaciona los controles, las políticas y los procedimientos que permitan evitar y responder frente a incidentes de seguridad en el perímetro de la compañía.
7. **Protección anti-incendios:** Relaciona la capacitación del personal, los equipos de extinción y los sistemas de control que permitan responder rápida y eficientemente a un incendio en el edificio y/o en el centro de cómputo.
8. **Riesgos entorno geográfico:** Relaciona las fuentes latentes de riesgo aledañas a la organización.
9. **Riesgos naturales:** Relaciona los aspectos de ubicación geográfica, climática y del entorno natural que puedan afectar a la compañía.
10. **Riesgos potencia eléctrica:** Relaciona las políticas, los controles y los procedimientos que permitan asegurar el suministro de energía eléctrica al edificio y equipos críticos.
11. **Riesgos telecomunicaciones:** Relaciona las políticas, los controles y los procedimientos que permitan mantener la comunicación (voz y datos) de la organización.
12. **Centro de datos:** Relaciona, los controles, infraestructura y procedimientos definidos para los centros de datos (principal y contingencia)

B. Análisis de Impacto de Negocios – BIA

La principal actividad en el diseño de un Protocolo de contingencia y Recuperación de Desastres es el Análisis de Impacto al Negocio (BIA). Con el fin de establecer el nivel de exposición a riesgos que comprometan la continuidad de las operaciones, se analiza la compañía por procesos, donde cada uno debe dar respuesta a la pregunta: ¿Qué pasaría en la Unidad Nacional de Protección, si usted dejara de funcionar abruptamente, bajo el peor escenario de desastre?

En este sentido el Análisis de Impacto al Negocio busca identificar aquellos elementos de hardware, software, comunicaciones, logística, transporte, infraestructura, personal y proveedores que ante una falla ocasionaría la interrupción de los procesos críticos del negocio. Este análisis comprende:

•Identificación de procesos del negocio a evaluar.
•Identificación de amenazas que impactan la continuidad de las operaciones
•Evaluación de los diversos impactos potenciales.
•Definición de las escalas para medir el tiempo de recuperación objetivo (RTO), el punto de recuperación objetivo (RPO) y el periodo máximo tolerable e interrupción (MTPD).
•Fechas o temporadas críticas para el procesamiento de información.
•Tiempos de gestación de crisis debido a interrupciones y otras causas que se pudieran presentar en un proceso respectivo.

Los parámetros son fundamentales para homogenizar las respuestas de los entrevistados y tabular fácilmente los resultados obtenidos. La información se recolecta mediante encuestas, entrevistas, revisión de informes, etc.

C. Objetivos Generales BIA

• El análisis BIA, permite identificar los procesos críticos, mediante la evaluación del impacto en caso de que ocurra un incidente que interrumpa la prestación del servicio.
• Evaluar y estimar el impacto operacional y financiero que un incidente mayor pueda causar; así mismo es un componente fundamental para la toma de decisiones por parte de la Alta Dirección al momento de presentarse un incidente que desencadene un evento de interrupción.
• Un incidente mayor se define como una situación que impacta la capacidad de la UNP para continuar sus operaciones desde su instalación primaria.
• Identificar y actualizar los Procesos Críticos con sus objetivos de recuperación (RTO y RPO), los cuales deben ser tenidos en cuenta por la UNP para atender de forma estratégica y eficiente una situación de interrupción.
• Determinar el máximo tiempo permitido de interrupción (MTPD), el cual representa el momento en que continuar con la operación de la entidad podría ser inviable por las consecuencias de una situación de interrupción prolongada.
• Entregar las herramientas que permitirán establecer la estrategia de continuidad, una vez sean analizados los servicios de tecnología críticos, registros vitales y proveedores críticos para cada uno de los procesos críticos.
• Proporcionar información para la toma de decisiones durante una situación de interrupción, que permita tener un panorama claro del negocio y, en consecuencia, facilite la activación oportuna de la Estrategia de Continuidad de Negocio y del retorno a la normalidad.

D. Metodología Aplicada

El desarrollo del Análisis de Impacto al Negocio en la UNP obedeció a la realización de los siguientes pasos metodológicos:

Tabla 3. Metodología BIA

Ítem	Paso Metodológico	Observaciones
1	Conocimiento del negocio	• Estudio del mapa y caracterización de los procesos. • Lectura y análisis de la documentación de continuidad del negocio existente. • Conocimiento preliminar del negocio mediante entrevistas con el personal. • Definición de parámetros requeridos por el BIA
2	Levantamiento de información	• Se realizaron entrevistas con los responsables de los procesos, con el fin de validar la información existente y completar otros datos identificados como esenciales para la realización del BIA.
3	Análisis de Información Levantada	• Se analizan los objetivos de cada proceso. • Se analizan las consecuencias de una interrupción, el grado de dependencia de TIC, fechas críticas, impactos, registros vitales y los RTO, RPO y MTPD por proceso.
4	Producción de Resultados	• Se selecciona la información a consolidar. • Se elabora el informe y se revisa con el grupo de trabajo.
5	Divulgación de Resultados	• Se socializan los resultados a los grupos de interés de la UNP

Fuente: Elaboración Propia

E. Análisis de Parámetros BIA

Los principales parámetros utilizados en el BIA de la UNP fueron:

• Tiempo de recuperación objetivo (RTO)
El Tiempo de Recuperación Objetivo (Recovery Time Objective) es el periodo de tiempo, después de la interrupción, en el cual el proceso o servicio debe ser restaurado o reanudado a un nivel mínimo aceptable. Este parámetro se incluyó como una pregunta dentro de las entrevistas que se realizaron a los diferentes responsables de cada proceso. Esta información fue registrada de forma individual en los formatos BIA para mayor detalle**.**

• Punto de recuperación objetivo (RPO)
El Punto de Recuperación Objetivo (Recovery Point Objective), es la pérdida máxima de datos tolerable por el proceso y que se pueden recuperar en un tiempo razonable sin generar riesgos importantes para la Entidad. El RPO se encuentra estrechamente relacionado con la copia de seguridad de datos. Todos los negocios que se basan en gran medida en el procesamiento o custodia de datos son vulnerables a la indisponibilidad de estos. Este parámetro se incluyó como una pregunta dentro de las entrevistas que se realizaron a los diferentes responsables de cada proceso. Esta información fue registrada de forma individual en los formatos BIA para mayor detalle.

• Periodo máximo tolerable a interrupción (MTPD)
El Periodo Máximo Tolerable de Interrupción (Maximum Tolerable Period of Disruption) es el tiempo máximo que puede soportar la UNP después de la interrupción de un proceso sin incurrir en una pérdida inaceptable para la Entidad. Se asume que si el proceso no se logra recuperar en la franja de tiempo definida como MTPD las pérdidas son tan elevadas que comprometen la viabilidad de la Entidad como empresa en marcha. Este parámetro se incluyó como una pregunta dentro de las entrevistas que se realizaron a los diferentes responsables de cada área. Esta información fue registrada de forma individual en los formatos BIA para mayor detalle.

F. Criterios de Impacto

Para establecer el impacto de una interrupción o desastre en los procesos de la Entidad se ubica al entrevistado en el siguiente escenario de desastre: **"Los sistemas de información y servicios de tecnología no funcionan por un largo periodo de tiempo en la fecha más crítica de su operación".** A partir de dicho escenario se identifican con cada responsable de los procesos el tiempo de materialización de los impactos, posibles crisis que se generarían en la Entidad, recursos mínimos para trabajar en contingencia, así como los clientes y proveedores tanto internos como externos que se verían afectados.
Los tipos de impacto incluidos en el BIA desarrollados son:

a) Impacto Económico
b) Impacto Servicio al Cliente
c) Impacto Reputacional
d) Impacto Legal (Incumplimiento de obligaciones legales)

La escala utilizada para medir el nivel de impacto se presenta en la siguiente tabla:

Tabla 4. Niveles De Impacto

Nivel de Impacto	Explicación
Alto	Si el hecho se llegara a presentar tendría consecuencias o efectos graves para la UNP y el sector. Se requiere la atención de la Dirección General para su solución.
Medio	Si el hecho se llegara a presentar tendría consecuencias o efectos negativos para la UNP. Se requiere la atención de las Subdirecciones para su solución.
Bajo	Si el hecho se llegara a presentar, tendría consecuencias o efectos mínimos sobre la UNP. Su solución se puede llevar a cabo por procedimientos de rutina y exige máximo la participación de los coordinadores.

Fuente: Elaboración Propia

En la medida que una interrupción de los procesos de negocio se extiende, los impactos son mayores debido a que se acumula trabajo, los usuarios elevan el volumen de las protestas, intervienen medios de comunicación y la imagen de la Entidad queda en entredicho, entre otros efectos.
Se establecieron las siguientes franjas de tiempo para tener una idea cercana de la evolución de los impactos negativos ante una interrupción de los procesos.

Tabla 5. Franjas de tiempo

Franjas de Tiempo
Entre 0 y 1 horas
Entre 1 hora y 2 horas
Entre 2 hora y 4 horas
Entre 4 horas y 24 horas
Entre 24 horas y 48 horas
Entre 48 horas y 72 horas
Más de 72 horas

Fuente: Elaboración Propia

G. Prioridades en la recuperación de la operatividad de la entidad

La estrategia está planteada en recuperar las aplicaciones críticas soportadas en la plataforma tecnológica de la UNP. Los sistemas de información de ubicados en la infraestructura tecnológica de la entidad se recuperarán de acuerdo con la criticidad de ejecución de programas de la UNP.

La UNP realiza copias diarias completas con retención de días y semanas días sobre los servidores que soportan los sistemas Misionales críticos de la Entidad alojados en servidores y Networt. En caso de un incidente, se realiza restauración de la Máquina en el mismo Centro de Datos o en un Centro de Datos diferente según la afectación y disponibilidad de la Nube de Azure.

H. Estrategia de reubicación y sitio de trabajo alternativo.

En el caso de que un desastre inhabilite parcial o totalmente las instalaciones del centro de datos ubicado en el área de infraestructura tecnológica, la estrategia de recuperación se concentrara en habilitar las aplicaciones críticas ubicadas On-Premise en la Unidad Nacional de Protección en un sitio alterno y definido con tecnología de servicios de Nube.

Las estrategias a corto plazo no contemplaran reubicaciones en locaciones físicas que estén planteadas dentro de un programa de recuperación de desastres o de un plan de continuidad de negocios. Lo anterior se hace imposible de establecer debido a que no se tiene capacidad de articulación de acciones dentro de un plan marco donde se comprenda la adecuación de áreas para la instalación de infraestructura On-Premise y la disponibilidad de recursos para la adquisición de equipos para la renovación de la infraestructura tecnológica afectada.

Si se produce una interrupción a largo plazo, establecida por la destrucción definitiva de la estructura física donde está ubicada la infraestructura tecnológica On-Premise de la UNP; la estrategia seguirá planteada a seguir con la implementación de una solución a corto plazo.

El plan de contingencia de la plataforma tecnológica se integrará con el plan maestro de recuperación de desastres de la UNP por medio de la presentación de la estrategia en el escenario creado por la alta dirección para atender la contingencia, el escenario estará representado por el coordinador general del equipo de recuperación.

Identificación de Impacto y tiempos de interrupción permitidos. Las funciones de negocio del AGN se clasifican en:

a) Funciones Críticas:

- Personal para la prestación del servicio de mesa de servicios
- Centro de Cómputo
- Disponibilidad de la infraestructura de los centros de cómputo (Servidores, almacenamiento y conectividad)
- Conectividad
- Disponibilidad de infraestructura de telefonía IP
- Disponibilidad de acceso a Internet
- Disponibilidad de canales de comunicación entre el ESC y los clientes

b) Funciones Esenciales:

- Disponibilidad de las herramientas de gestión de servicios para los grupos solucionadores de los clientes
- Disponibilidad de correo electrónico
- Disponibilidad de Chat, Portales de Servicio

c) Funciones Necesarias:

- Disponibilidad de acceso a Intranet

Basado en estas necesidades de recuperación, los puntos de tiempo máximo para recuperación son:

- Funciones Criticas: <= 4 horas,
- Funciones Esenciales: <= 2 días,
- Funciones Necesarias: <= 4 días

Prioridades de Recuperación

De acuerdo con la clasificación de funciones del AGN y los puntos máximos de recuperación, las

prioridades de recuperación durante el plan de contingencia son:

1. **Prioridad Alta**

- Infraestructura de Red Local
- Canales de comunicación
- Infraestructura de apoyo (Telefonía/telecomunicaciones y aplicaciones)

- Herramientas de Gestión de Servicios y su infraestructura de apoyo (Servidores y Bases de Datos)
- Correo electrónico
- Canal de Internet Local y servidor PROXY.

2. Prioridad Media

- Aplicaciones de negocio

3. Prioridad Baja

Ambientes de prueba y desarrollo.

I. Fases del Plan de Contingencia de la Infraestructura Tecnológica.

Serán las actividades necesarias para la recuperación de la operatividad de las aplicaciones On-Premise de un desastre en las instalaciones de la UNP, las cuales se plantearán en cuatro fases. Estas fases se seguirán secuencialmente en el tiempo.

1. Declaración de desastre:

Esta fase comienza con la ocurrencia del evento de desastre y continúa hasta que se declara oficialmente por parte de la alta dirección el desastre y se toma la decisión de activar los planes de contingencia formulados por cada área.

Las principales actividades que tienen lugar en esta fase incluyen: medidas de respuesta de emergencia, notificación de la gestión, actividades de evaluación de daños y declaración del desastre.

2. Activación del Plan de Contingencia de la Plataforma Tecnológica:

En esta fase, se ponen en vigor del Plan de Contingencia de la Plataforma Tecnológica. Esta fase continúa hasta que se ocupe la instalación alternativa, se normalicen las funciones misionales críticas y se restablezca para los Servidor Público el servicio del sistema informático en las distintas áreas de la UNP. Las principales actividades de esta fase incluyen: notificación y montaje de los equipos de recuperación, implementación de procedimientos provisionales y reubicación en el sitio secundario de instalación/copia de seguridad, y restablecimiento de las comunicaciones de datos.

3. Operaciones alternativas en el sitio:

Esta fase comienza después de que se restablezcan las operaciones de las instalaciones secundarias y continúe hasta que se restablezca la instalación primaria. Las actividades de recuperación primarias durante esta fase son la solución a problemas de acceso de los Servidor Público a las aplicaciones dispuestas en la Nube Azure, disminución a problemas asociados a la transición de la tecnología On-Premise a la de Nube - Azure y los

procedimientos alternativos de acceso a los servidores Públicos a las aplicaciones dispuestas en la Nube Azure (Teletrabajo).

4. Transición al sitio primario:

Esta fase consta de todas y cada una de las actividades necesarias para realizar la transición de nuevo a una ubicación de instalación primaria. Estas dependerán estrictamente de las medidas tomadas por la alta dirección dentro plan marco con la aplicación del plan de continuidad.

J. Estrategias de Backup Aplicaciones Críticas On-premise.

Una buena estrategia de Backup es la mejor defensa contra la perdida de datos. Las tres estrategias comunes de Backup son las siguientes:

- **Backup de Red o Servidor Únicamente:** Se planea respaldar toda la red, o se tienen dispositivos de almacenamiento a ciertos servidores donde los usuarios guardan su información importante.

- **Backup Individual o al Computador Local:** Cada computador necesita un dispositivo de almacenamiento. Cada usuario es responsable por el respaldo de sus datos.

- **Backup del Servidor y Computador:** Cada departamento tiene un dispositivo de almacenamiento y un usuario designado para respaldar toda la información del departamento.

Para el caso de la UNP donde la estructura de la red y la administración es centralizada, se realiza un Backup a los servidores donde se encuentre la información importante tanto de la organización como de los usuarios. La información que no esté sobre los servidores designados y/o que estén en estaciones es responsabilidad de cada servidor Público o del área.

Consideraciones al Plan de Backup

Cuando se desarrolla un plan de Backup se debe tener en cuenta:

- Estar seguro de que se tiene un hardware de respaldo en el caso de que falle un dispositivo de Backup.
- Probar los datos del Backup regularmente para verificar la fiabilidad del procedimiento de Backup y del equipo.
- Incluir una prueba de tensión del hardware de Backup (unidades de almacenamiento, unidades ópticas y controles) y del software (programas de Backup y unidades de dispositivo).

Para el caso de la UNP se cuenta con Networker como herramienta de almacenamiento cada una de las cintas, como también office 365 y Share Point en la nube.

Tipos de Backup

Los Backups se pueden dividir en varios tipos; tanto con la herramienta de Windows o plataformas administradora de la información y nube, como son los siguientes:

- **Un Backup Normal** copia todos los archivos seleccionados y marca cada uno como un Backup normal. Para la restauración solamente y si es necesario del Backup más reciente realizado.

- **Un Backup Incremental**, realiza Backup solamente a los archivos que fueron creados o modificados desde el último Backup normal o incremental. Esta marca solamente los archivos que se les ha realizado Backup. Al utilizar una combinación de Backups normales e increméntales es necesario para la restauración tener el último Backup normal y todo el set de Backups increméntales hasta la fecha.

- **Un Backup Diferencial**, copia los archivos creados o modificados desde el último Backup normal o incremental. Este no marca los archivos como si se le hubiera realizado Backup. Si se tiene una combinación de Backups normales y diferenciales; para la restauración es necesario tener el último Backup normal y el set de Backups diferenciales.

- **Un Backup Copia**, copia todos los archivos seleccionados, pero no marca los archivos como si se le hubiera hecho Backup. Este Backup no afecta otros tipos de Backup.

- Un Backup Diario, copia todos los archivos seleccionados que han sido modificados en el día que se haya realizado el Backup. Los archivos no son marcados.

- **Networker**, trae una característica que permite realizar un Backup a un archivo. Esto es una gran ventaja cuando sobre los servidores no se tienen unidades de cinta; aunque el Backup realizado sigue siendo a cinta. Con la herramienta de Data Protector se posee más flexibilidad con los Backups ya que también se puede enviar a cinta, aunque este maneja agentes para los servidores que se le va a hacer Backup como si fuese de forma local.

Información que se debe respaldar

- De los controladores de dominio se debe realizar copia del estado del sistema para respaldar el directorio activo.
- De los servidores de archivos se deben respaldar las carpetas compartidas y el estado del sistema.
- De los servidores de Exchange se debe hacer copias de las bases de datos de correo y de carpetas públicas.
- Se deben mantener discos de reparación actualizados por cada servidor y almacenados de manera segura.

- Los servidores que manejan sitios y aplicaciones web.
- Las bases de datos de los servidores Oracle y SQL.
- Administración del correo 365 en la nube y el espacio de Share Point
- Sistemas de información

La UNP, tiene con un contrato con la empresa de claro en triara Siberia y este es un data center tier 4 ratifica que el data center ofrece las siguientes garantías:

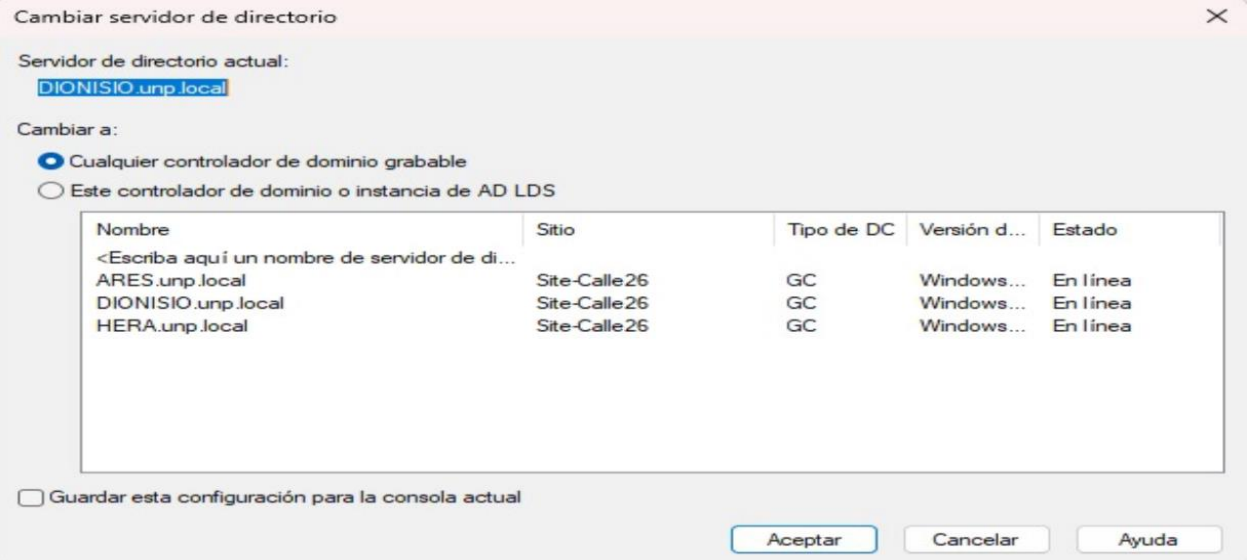
- Que posee una infraestructura robusta, tolerante a fallos.
- Que tiene un alto tiempo de actividad.
- Que es resistencia a desastres y posee diversas protecciones.

Las certificaciones tier creadas por el Uptime Institute para clasificar la fiabilidad de los centros de datos, van desde tier 1 a tier 4, siendo esta última la más completa y actual. Los niveles de disponibilidad de acuerdo con los distintos tier son:

- Tier 1. Disponibilidad garantizada del 99.671 %
- Tier 2. Disponibilidad garantizada del 99.741 %
- Tier 3. Disponibilidad garantizada del 99.982 %
- Tier 4. Disponibilidad garantizada del 99.995 %

Esta característica los convierte en la opción perfecta para los servicios de cloud computing, ya que la alta disponibilidad es el factor más importante. Por ejemplo, al realizar copias de seguridad de una empresa; en un data center tier 4, incrementará la seguridad e integridad de estas, garantizando que puedan ser recuperadas cuando sea necesario.

K. Controladores de dominio



La UNP cuenta con una herramienta Networker de Backups

Respaldo del sistema de archivos del cliente NetWorker.

Los respaldos incrementales del sistema de archivos para un cliente de Windows (por ejemplo, level = incr) parecen respaldar los mismos archivos que no se cambiaron desde el respaldo anterior.

Observaciones:

mminfo -avot -c clientname
muestra el tamaño del respaldo incr casi igual que el respaldo completo.
nsrinfo - V clientname (V en mayúscula)
-V muestra los archivos respaldados y sus respectivas fechas de respaldo y mtime, atime, ctime.

Comprueba nsrinfo para buscar los archivos que se respaldaron en dos o más fechas en las que cada respaldo tiene la misma mtime que la primera fecha de respaldo.

Implica que el archivo no se cambió y que aún se respaldó.

Causa

El comportamiento de NetWorker para el respaldo incremental del sistema de archivos en Windows es el mismo en todas las versiones de NetWorker.

Según la documentación de NetWorker:

En Windows, la hora de modificación/cambio del archivo se refiere a la hora de la última escritura, la hora de creación y el atributo de archivo de archivo de un archivo. Todos estos se utilizan para determinar si se debe respaldar un archivo.

Si se configura el atributo Archive file, el archivo siempre se respaldará, ya que es posible que algunos sistemas de archivos más antiguos no tengan el tiempo de creación de archivos adecuado, a menos que NSR_AVOID_ARCHIVE variable de entorno esté configurada (en un valor distinto de "no").

- Dentro de la plataforma esta configurado la copia de todos los servidores con su parametrización e información que allí eta alojada y se maneja por cintas

  Existen dos categorías de programación

  - **INCREMENTAL:** Se realiza a diario
  - **FULL:** se realiza los fines de semana

Se tiene contemplado realizar las copias de seguridad de toda la infraestructura con las debidas configuraciones de cada uno de los servidores, información controladores como el correo Exchange, página web e intranet y su espacio de share Point, los Backup de nube se realiza y está contemplado para proteger y salvaguardar la información y demás ítems para asegurar la operación.

Esquema de Custodia de Backups

La UNP cuenta con la custodia de medios magnéticos (cintas magnéticas, discos, cartuchos, disquetes) en un lugar seguro fuera de la entidad con condiciones ambientales controladas, sistemas automáticos de extinción de incendios y acceso restringido, como medida preventiva en caso de un desastre o perdida involuntaria de los archivos vitales.

L. Aspectos de Seguridad

Dentro de los sistemas de seguridad física implementados se tiene:

Tabla 6: Seguridad Física a Instalaciones

Item	Responsable
Cámaras de Televisión	Secretaria general - empresa de vigilancia
Contactos Magnéticos	Secretaria general - empresa de vigilancia
Carnetización	Subdirección de Talento humano
Sistemas de Detección de Incendios	Secretaria general - Grupo de Gestión Administrativa
Control de Roedores	Subdirección de TH- Grupo de Gestión Administrativa
Circuito cerrado de televisión	Secretaria general - empresa de vigilancia
Prevención, detección y control de Energía.	Subdirección de TH - Medio ambiente

Item	Responsable
Planta Eléctrica de Emergencia	Secretaria general - Grupo de Gestión Administrativa
Sistemas de UPS	Secretaria general - Grupo de Gestión Administrativa
Mantenimiento y soporte de cableado estructurado	Grupo de Gestión A Grupo de Gestión Administrativa administrativa - Grupo de gestión de las tecnologías

Fuente: Elaboración propia

Administración de Bases de datos

Bases de Datos SQL

Tabla 6: Bases de Datos SQL

Servidor Evanthe y Demetrio Instancia EDDA Bases de datos de producción				
ID de la BD	**Nombre de la Base de Datos**	**Tamaño de la Base**	**Unidad de Medida**	**Fecha de Creación**
1	master	7,00	MB	Apr 8 2003
2	tempdb	281.448,94	MB	Aug 22 2024
3	model	3,13	MB	Apr 8 2003
4	msdb	91,69	MB	Apr 30 2016
5	SIGOB	4.534.967,19	MB	Jul 1 2017
6	App_sigob	17,00	MB	Jul 1 2017
7	PQRS_Web	188,49	MB	Jul 1 2017
8	Control_y_Registro	152,00	MB	Jul 1 2017
9	DDHH_OLTP	356,69	MB	Jul 1 2017
10	Indicadores	86,00	MB	Jul 1 2017
11	Notificaciones	81,38	MB	Jul 1 2017
12	Solicitudes_Web	55,44	MB	Jul 1 2017
13	Indicadores_Prueba	21,00	MB	Jul 1 2017
14	SER_Web	75,81	MB	Aug 22 2017
16	PH_Events	99,13	MB	Jul 15 2022
17	MIPG_PROD	4,00	MB	Dec 14 2022
18	suiteveyf	1.299,13	MB	Dec 15 2022
19	suiteve	595,13	MB	Dec 15 2022

Servidor Evanthe y Demetrio Instancia EDDA Bases de datos de producción				
ID de la BD	**Nombre de la Base de Datos**	**Tamaño de la Base**	**Unidad de Medida**	**Fecha de Creación**
Servidor Evanthe y Demetrio Instancia MILO SharePoint				
ID de la BD	**Nombre de la Base de Datos**	**Tamaño de la Base**	**Unidad de Medida**	**Fecha de Creacion**
1	master	7,88	MB	Apr 8 2003
2	tempdb	2.738,88	MB	Aug 22 2024
3	model	8,50	MB	Apr 8 2003
4	msdb	85,75	MB	Apr 30 2016
5	SharePoint_Config	1.951,13	MB	Sep 27 2017
6	SharePoint_AdminContent_a34e03a4-5812-499d-b898-0c63b826b14a	2.191,81	MB	Sep 27 2017
7	WSS_Content_Intranet	30.968,25	MB	Oct 19 2017
8	Secure_Store_Service_DB_16808c0028d44ab3afe499246ec68c73	16,00	MB	Sep 28 2017
9	StateService_c6c8a7dddd944ba0afc7f699359a1c9c	16,00	MB	Sep 28 2017
10	Profile DB	199,56	MB	Oct 3 2017
11	WSS_Logging	13.405,25	MB	Sep 28 2017
12	Bdc_Service_DB_7de0f1a8833e460fb643c3735a1e599d	16,00	MB	Sep 28 2017
13	Managed Metadata Service	19,68	MB	Oct 2 2017
14	Sync_3e6d5dff-2ab2-4b78-a1c2-b4a576667c79 DB	8,50	MB	Oct 3 2017
15	Social DB	40,50	MB	Oct 3 2017
16	WSS_Content_ArcGis	193,56	MB	Jul 24 2018
17	WSS_Content_unpweb	15.436,87	MB	Oct 19 2017
18	AppManagementServiceApplication	8,50	MB	Oct 18 2017

Servidor Evanthe y Demetrio Instancia EDDA Bases de datos de producción				
ID de la BD	**Nombre de la Base de Datos**	**Tamaño de la Base**	**Unidad de Medida**	**Fecha de Creación**
19	WSS_Content_Prueba	151,31	MB	Oct 18 2017
20	WSS_Content_mysite	134,94	MB	Oct 18 2017
21	CouldSearchApplication	183,06	MB	Oct 20 2017
22	CouldSearchApplication_CrawlStore	1.854,06	MB	Oct 20 2017
23	CouldSearchApplication_AnalyticsReportingStore	8,50	MB	Oct 20 2017
24	CouldSearchApplication_LinksStore	166,25	MB	Oct 20 2017
25	SPSubscriptionSettingsService_DB	8,50	MB	Jul 24 2018
Servidor NIKE Instancia LOKI				
ID de la BD	**Nombre de la Base de Datos**	**Tamaño de la Base**	**Unidad de Medida**	**Fecha de Creación**
1	master	5,25	MB	Apr 8 2003
2	tempdb	40,00	MB	Aug 9 2024
3	model	16,00	MB	Apr 8 2003
4	msdb	16,56	MB	Oct 8 2022
5	DBS_FUSAR	336,00	MB	Aug 12 2024

Bases de datos MySQL

Servidor HELL 2				
ID de la BD	**Nombre de la Base de Datos**	**Tamaño de la Base**	**Unidad de Medida**	**Fecha de Creacion**
1	SER - ISAACK	23.612,00	MB	Apr 8 2003

Fuente: Elaboración Propia

6.2 Equipo de Recuperación

A. Propósito y objetivo

Esta sección del plan identifica quién participará en el proceso de recuperación de las aplicaciones críticas de la entidad dentro del plan de contingencia. El equipo de ingenieros está organizado en un solo equipo, con un líder de equipo. Cada Servidor Público está asignado a una responsabilidad específica dentro del equipo para llevar a cabo tareas según sea necesario.

B. Descripciones del equipo de recuperación

El equipo de Ingeniería de TI de la UNP a cargo de la ejecución del plan es el siguiente:

Tabla 7: Equipo de Recuperación

ROL	Tipo de Contratación	Perfil	Descripción funcional
Infraestructura	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura –servidores-	Planta	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura- AD	planta	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura - Firewall	planta/Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura- data center	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura- redes	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura-centros de cableado	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura-seguridad	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura-Backups	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación

ROL	Tipo de Contratación	Perfil	Descripción funcional
Infraestructura-vulnerabilidades	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Infraestructura- correo electrónico 365	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Mesa de servicios-servicios - plataforma	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Mesa de servicios-servicios tecnológicos	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Página web	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos como presupuestales y herramientas para realizar la operación de recuperación
Desarrollo inhouse	contratista	sociólogo	Disponer de los recursos humanos y de los dueños de la información para que realicen la verificación de esta
Desarrollos terceros	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos y de los dueños de la información para que realicen la verificación de esta
Servicios Opas	Contratista	Ingeniero de sistemas	Disponer de los recursos humanos y de los dueños de la información para que realicen la verificación de esta
Desastres naturales	Contratista	Ingeniero de sistemas	Disponer de las áreas y de todo el personal para colaborar con la contingencia

Fuente: Elaboración Propia

C. Asignaciones de roles dentro del equipo de recuperación

Esta sección identifica los roles del equipo y las responsabilidades específicas que se han asignado a cada miembro del equipo de recuperación.

Tabla 8: Responsabilidades de Contingencia Equipo de Recuperación

Rol	Responsabilidades en la contingencia
Administrador Servicos de Nube - Azure	Disponer de los recursos de TI necesarios en la Nube, para el traslado de Aplicaciones y Base de Datos On-premise a la Nube.
Administrador de Servidores y Almacenamiento	Verificar que los recursos de TI en la Nube sean suficientes y acordes a los requerimientos técnicos para que las aplicaciones, bases de datos y repositorios estén disponibles y accesibles.

Rol	Responsabilidades en la contingencia
Administrador de Bases de Datos	Proceder con el restablecimiento de Bases de Datos en la Nube con el ultimo Back Up disponible y realizar su administración.
Administrador Mesa de servicios	Administrador de la plataforma Ivanti de mesa de servicios
Administrador Sitios Web, Videoconferencias,	Proceder con el restablecimiento de las aplicaciones y sitios web en la Nube con el ultimo Back Up disponible y realizar su administración.
Administrador plataforma office 365	Garantizar la disponibilidad de las cuentas de correo y su administración.
Sistemas de información	Responsable de verificar las restauraciones de la información de los sistemas de información

Fuente : Elaboración propia

D. Ubicación dentro de la UNP del equipo de recuperación

Esta sección identifica la ubicación física de los servidores Públicos encargados del proceso de recuperación dentro de la UNP.

E. Responsabilidades del equipo de recuperación

ROL general del equipo de recuperación

En caso de desastre, el Coordinador del equipo de recuperación es responsable de garantizar que las siguientes actividades se cumplan con éxito

- Trabaja con el equipo de gestión de emergencias de Talento Humano para declarar oficialmente un desastre e iniciar el proceso de implementación del Plan de Contingencia de la Plataforma Tecnológica, con el fin de recuperar la funcionalidad de las aplicaciones críticas Misionales y no Misionales de la UNP en un sitio alternativo.
- Alertar a la alta gerencia de la UNP que se ha declarado un desastre.
- Monitorear diariamente el progreso del equipo encargado de la implementación del Protocolo de Contingencia de la Plataforma Tecnológica.
- Elaborar informes del estado de recuperación de las aplicaciones Misionales y No Misionales a la Dirección General.
- Comunicar las instrucciones recibidas de la Dirección General al equipo implementador del Plan de Contingencia de la plataforma tecnológica.
- Brindar apoyo y orientación continuo al equipo de ingenieros encargados de la implantación Protocolo de Contingencia de la plataforma tecnológica.
- Revisar la disponibilidad del equipo y recomendar asignaciones alternativas, si es necesario.

- Trabajar con la Dirección General de la UNP para que se autorice el uso del sitio de recuperación alternativo seleccionado para volver a implementar aplicaciones críticas misionales y no Misionales de la UNP.
- Revisar e informar los cronogramas de procesamiento críticos y el progreso del trabajo atrasado.

Administrador Servicios de Nube -Azure

- Disponer de los recursos de TI necesarios en la Nube, para el traslado de Aplicaciones y Base de Datos On-premise a la Nube - Azure.
- Implementar la arquitectura de solución apropiada y definida para las aplicaciones misionales y no misionales que se requieran subir a la Nube de Azure.
- Garantizar la operabilidad de las aplicaciones misionales y no misionales en la Nube – azure
- Dar soporte desde el punto de vista técnico a los usuarios finales en el cómo y cuándo se podrá acceder a las aplicaciones misionales críticas.
- Generar cronograma junto con la coordinación general del equipo de recuperación y el administrador de servidores para el proceso de recuperación de las aplicaciones misionales y no misionales de la entidad.

Administrador de Servidores

- Ser el respaldo de la líder del equipo de recuperación, asumiendo las funciones dentro del plan de contingencia, si solo si se llegara a no contar con su presidencia.
- Coordinar con el administrador de la Nube de Azure, la disponibilidad y la puesta en marcha los nuevos servidores, esto de acuerdo con la necesidad y priorización de las aplicaciones misionales y no misionales On-primise que se requieran migrar a la Nube – Azure.
- Disponer los últimos Back ups realizados de acuerdo con la política de back ups de la UNP. Además, deberá coordinar con el administrador de la Nube - Azure, la prioridad de la generación de back ups y ajustar la política de back ups institucional a la desarrollada con los servicios en la Nube de Azure.
- Verificar que la configuración hardware de los servidores estén acorde a las necesidades de las aplicaciones misionales y no misionales que se requieran desplegar en la Nube - Azure, hallar posibles incompatibilidades con determinadas versiones de software que tenga que ser actualizado.
- Verificar que los recursos de TI en la Nube sean suficientes y acordes a los requerimientos técnicos para que las aplicaciones, bases de datos y repositorios estén disponibles y accesibles.

Administrador de Bases de Datos Principal

- Proceder con el restablecimiento de Bases de Datos en la Nube con el ultimo Back Up disponible y realizar su administración.

- Establecer con la coordinación y con el equipo de recuperación, los procedimientos para la recuperación de las bases de datos de las aplicaciones misionales y no misionales que se encuentran On-premise y que se requieran subir de acuerdo a la prioridad a la Nube Nube de Azure.
- Realizar monitoreo a las bases de datos con el fin mantener la accesibilidad a la base de datos desde la Nube – Azure y Garantizar que sea segura.
- Monitorear el desempeño de las bases de datos en la Nube – Azure, con el fin de garantizar que esté manejando los parámetros adecuadamente y que el brinde respuestas rápidas a los usuarios.
- Disponer en la migración de los últimos Back Ups de Bases de Datos disponibles y generados de acuerdo con la política de Back Ups de la UNP.
- Verificar que las políticas de administración de Base de Datos en la Nube estén ajustadas armonizadas de acuerdo con las necesidades de la entidad.
- Planificar y conservar un sistema de respaldo de las bases de datos migradas a la Nube – Azure.
- Servir de Back Up del Administrador de Bases de Datos Principal.
- Proceder con el restablecimiento de Bases de Datos en la Nube con el ultimo Back Up disponible y realizar su administración.
- Establecer con la coordinación y con el equipo de recuperación, los procedimientos para la recuperación de las bases de datos de las aplicaciones misionales y no misionales que se encuentran On-premise y que se requieran subir de acuerdo con la prioridad en la Nube Nube de Azure.
- Realizar monitoreo a las bases de datos con el fin mantener la accesibilidad a la base de datos desde la Nube – Azure y Garantizar que sea segura.
- Monitorear el desempeño de las bases de datos en la Nube – Azure, con el fin de garantizar que esté manejando los parámetros adecuadamente y que el brinde respuestas rápidas a los usuarios.
- Disponer en la migración de los últimos Back Ups de Bases de Datos disponibles y generados de acuerdo con la política de Back Ups de la UNP.
- Verificar que las políticas de administración de Base de Datos en la Nube estén ajustadas armonizadas de acuerdo a las necesidades de la entidad.
- Planificar y conservar un sistema de respaldo de las bases de datos migradas a la Nube – Azure.

Administrador de Aplicaciones

- Proceder con el restablecimiento de aplicaciones web en la nube con el ultimo Back Up disponible y realizar su administración.
- Establecer con la coordinación y con el equipo de recuperación, los procedimientos para la recuperación de las aplicaciones misionales y no misionales que se encuentran On-premise y que se requieran subir de acuerdo con la prioridad a la Nube de Azure.
- Realizar monitoreo de las aplicaciones web con el fin mantener su accesibilidad desde la Nube – Azure y Garantizar que sea segura.

- Monitorear el desempeño de las aplicaciones web en la Nube – Azure, con el fin de garantizar que esté manejando los parámetros adecuados y que les brinde respuestas rápidas a los usuarios.
- Disponer en la migración de los últimos Back Ups de las aplicaciones web disponibles y generados de acuerdo con la política de Back Ups de la UNP.
- Verificar que las políticas de administración de aplicaciones web en la Nube estén ajustadas y armonizadas de acuerdo con las necesidades de la entidad.
- Planificar y conservar un sistema de respaldo de las aplicaciones web migradas a la Nube – Azure.

Administrador de Plataforma office 365

- Establecer con la coordinación y con el equipo de recuperación, los procedimientos para que se mantengan funcionales las cuentas de correo electrónico y el directorio activo en la Nube.
- Garantizar desde la administración de la plataforma de servicios de Office 365 que los servicios estén arriba y accesibles para los usuarios.
- Verificar el cumplimiento de los acuerdos de nivel servio por parte de Microsft, esto se aplicará en caso de que el desastre llegue afectar los servicios de Office 365.
- Realizar la administración de los servicios de réplica de directorio Activo a la Nube de Office 365 y su correcto funcionamiento una vez se declare inaccesibles los servicios On-Premise.

Administrador plataforma de mesa de servicios

- Realizar los procesos de restauración de la plataforma de Ivanti- mesa de servicios
- Realizar la revisión de todos los servicios parametrizados en la plataforma se encuentran funcionando.
- Garantizar los respectivos Backup
- Revisión periódica de los perfiles quienes manejan la plataforma
- Brindar continuidad con el manejo de mesa de servicios

Tabla 9: Fases de Activación de Protocolo de Contingencia

Desastre tecnológico
Responsable el jefe de la oficina asesora de planeación
Responsable técnico: Coordinador del GGT
FASE 1 Diagnostico
Sistemas de telecomunicaciones ✓ Router de acceso a Internet ✓ Canal de acceso a servicios de Internet ✓ Switches de core y switches de piso ✓ Equipos de seguridad perimetral como firewall y concentrador de VPN ✓ Servicios de mensajería electrónica Teames y sistema colaborativo Office 365 Servidores que soportan sistemas de información institucionales ✓ Pagina WEN Institucional ✓ Sitio de la Intranet institucional ✓ Sistema de Información Internos administrativos y misionales ✓ Sistema de información SIGEP

- ✓ Sistema de información SUIT
- ✓ Sistema de información FURAG
- ✓ Sistema Integrado de Planeación y Gestión
- ✓ Portal gov.co
- ✓ Sistema financiero SIIF

Reporte de incidentes a el centro cibernético policial, centro de respuesta a incidentes informático del Min Defensa o el Min TIC se determina la ocurrencia de emergencias que
suspenderán la prestación de servicios informáticos de la Entidad como:

- ✓ Ataques cibernéticos como denegación de servicios
- ✓ Secuestro de la información institucional por ataque de software malicioso (ransomware)
- ✓ Falla total de los subsistemas de energía o aire acondicionado del centro de computo
- ✓ Falla eléctrica por voltaje severamente reducido, depresiones, picos y sobre voltajes
- ✓ Caída total del servicio de acceso a Internet o red local institucional
- ✓ Caída de canales de comunicación principales a cargo de los proveedores de acceso a Internet que alteren y/o interrumpan el normal funcionamiento de los equipos que se utiliza para los procesos misionales.
- ✓ Fuego o inundación del centro de datos que obliga al apagado de todo el centro de datos
- ✓ Falla total del sistema de almacenamiento masivo de datos compartidos
- ✓ Falla total del sistema de virtualización de servidores
- ✓ Indisponibilidad total de bases de datos por corrupción de datos

Pérdida acceso a sistemas críticos por finalización de licencia de uso manipulación incorrecta de sistemas informáticos debido a:

- ✓ Actividad errónea de administración de base de datos, corrupción de la base de datos, acceso indebido a la base de datos para modificarla, errores en puesta en producción / regresión con impacto en base de datos y errores en generación y restauración de respaldos que conlleven a la pérdida total o parcial de los servicios

- ✓ Por problemas y exposiciones s en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación de usuarios externos al pedir cambio de clave, ataques externo s para obtención/modificación indebida de información

Los profesionales responsables de la administración de los sistemas afectados realizan un diagnóstico sobre el incidente, teniendo en cuenta:

- ✓ Naturaleza e impacto del incidente.
- ✓ Estrategias definidas en el Plan de Recuperación ante desastres aplicables u otras soluciones potenciales definidas por la base de conocimientos de la mesa de servicio.
- ✓ Tiempo estimado de solución del incidente.

De acuerdo con la política y procedimientos y contratos con terceros de soporte para los diferentes sistemas de información y plataformas informáticas, del Grupo de Gestión de las Tecnologías aplica las acciones de remediación para resolver la contingencia, si el evento no se ha resuelto de acuerdo con el siguiente tiempo máximo tolerable de caída, el jefe de la oficina asesora de Planeación confirmará la situación de alerta por falla de infraestructura tecnológica o ataque informático y mediante un oficio formal y notifica al equipo de internos para gestionar la necesidad de activar el proceso de recuperación que se contempla en el BIA

FASE 2 Activación

- Sistemas y servicios afectados
- Resultados del diagnóstico sobre los sistemas afectados

- Acciones de recuperación realizadas hasta el momento
- Tiempo estimado para el restablecimiento de los servicios afectados
- Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles

❖ Recomendación de activar el protocolo de continuidad institucional e iniciar la ejecución de las estrategias de recuperación ante desastres de tecnología.

1. El Equipo de Gestión de Emergencias evalúa la información y decide si se debe activar el protocolo de continuidad y plan de operación alterno de cada una de las dependencias.
2. Si se aprueba la ejecución del protocolo de continuidad del negocio de operación alterno por desastre tecnológico, se comunica al jefe de la Oficina Asesora de Información que se debe notificar a los jefes de dependencia la necesidad de aplicar sus respectivos planes de operación alterno por crisis de infraestructura tecnológica.
3. El equipo del grupo de gestión de las tecnologías define el mensaje oficial de respuesta que se comunicará a los grupos de valor que incluye:

✓ Centro de respuesta a incidentes informáticos de Gobierno -Csirtgob csirtgob@mintic.gov.co
✓ Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT contacto@colcert.gov.co

Servidores Públicos y contratistas de la UNP a través de los medios de comunicación estipulados en la UNP. define:

- ✓ ¿Qué información concreta se tiene sobre la crisis (incidente presentado, diagnóstico,
- ✓ tiempo de solución)?
- ✓ ¿Qué información está en proceso de verificación e investigación?
- ✓ ¿Qué información válida se puede realizar en el formato de incidentes mayores?
- ✓ ¿Qué información se debe manejar al interior de la entidad?

Fase 3: Resolución del incidente

Cuando se realice el restablecimiento de los sistemas informáticos afectados El Jefe de la Oficina asesora de la Información, notifica:

✓ El correcto funcionamiento de los sistemas informáticos, el orden de restablecimiento de los servicios definido en el análisis de impacto al negocio BIA, para lo cual Comunica

- Reanudación de procesos
- disponibilidad de servicios TIC requerido por cada proceso,
- Reanudar las actividades normales de cada día

✓ Se notifica nueva nuevamente a los entes de emergencia del gobierno nacional la resolución del incidente

- Centro de respuesta a incidentes informáticos de Gobierno Csirtgob csirtgob@mintic.gov.co
- Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT contacto@colcert.gov.co

Al finalizar se dejan las evidencias en el repositorio para tener la salvaguarda para presentar en otros informes o auditorias que lo requieran

Fuente: Elaboración Propia

7. VIGENCIA

Las políticas descritas en este documento regirán a partir de la fecha de aprobación y publicación de estas.

8. DOCUMENTOS RELACIONADOS

- GTE-MA-02 Manual de políticas Específicas de seguridad y privacidad de la información
- GTE-PL-01 Plan de Mantenimiento de la Infraestructura Tecnológica
- GTE-PL-02 Plan de seguridad y privacidad de la información
- GTE-PL-03 Plan de tratamiento de riesgos de seguridad y privacidad de la información
- GTE-PR-41 Procedimiento Gestión de copia de seguridad, resguardo y restauración
- GTE-FT-05 Informe de Estado y Gestión
- GTE-FT-46 Declaración Aplicabilidad-SOA
- GTE-FT-50 Análisis de Impacto de Negocios-BIA
- GTE-FT-51 Formato de copias de seguridad y restauración

9. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del documento con el propósito de establecer criterios específicos en caso de que se presenten interrupciones en los servicios de operación respecto a la seguridad y privacidad de la información de la UNP.	29/11/2024	01

10. BIBLIOGRAFÍA

- ICONTEC. Norma Técnica Colombiana NTC-ISO 9000. Colombia. 2015. Segunda actualización.
- ICONTEC. Norma Técnica Colombiana NTC-ISO 27001. Colombia. 2013. Segunda edición.
- ICONTEC, NTC-ISO-IEC 27001, 2022 Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC.
- ISO. Términos y Definiciones. En: Gestión de la seguridad de la información (Fundamentos y vocabulario). 2006. (POLÍTICA ISO/IEC 27000).
- Guía para la Gestión y Clasificación de Activos de Información. Seguridad y Privacidad de la Información. [En Línea] Bogotá, D.C. [Citado el 13 julio de 2017]. Disponible en Internet: <URL: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf >
- Manual de Seguridad y Privacidad de la Información. Seguridad y Privacidad de la Información. [En Línea] Bogotá, D.C. [Citado el 13 julio de 2017]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Manual_de_Seguridad_Privacidad.pdf >

- POLÍTICA TÉCNICA COLOMBIANA MTC-ISO 31000, página 9. [En Línea] Bogotá, D.C.: [Citado el 9 de abril del 2018]. Disponible en Internet: <URL: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf >

11. ANEXOS

- Anexo 1. Declaración de Aplicabilidad – agosto de 2024
- Anexo 2. INFORME ANALISIS DE IMPACTO DE NEGOCIOS – BIA - UNP