PROTOCOLO DE RESPUESTA A INCIDENTES

FACULTAD DE ECONOMÍA Y NEGOCIOS (FEN)

UNIVERSIDAD DE CHILE

Información General del Documento

- **Fecha de Emisión:** 27 de mayo de 2025
- **Versión:** 1.0
- **Páginas:** 1 de 32
- **Autor(es):** Jackson Gonzalez Sanchez - Miguel Avello Moya
- **Revisor(es):** Mario Cuadra Seguel

FACULTAD ECONOMÍA Y NEGOCIOS
UNIVERSIDAD DE CHILE

Contenido

FACULTAD ECONOMÍA Y NEGOCIOS
UNIVERSIDAD DE CHILE

I. Resumen Ejecutivo

- Este documento establece el protocolo institucional para la gestión integral de incidentes tecnológicos que afecten los servicios y sistemas de la Facultad de Economía y Negocios de la Universidad de Chile.

- Su enfoque se basa en prácticas consolidadas de la industria (ITIL, ISO 20000) para asegurar una respuesta oportuna, estructurada y eficaz ante cualquier evento que interrumpa la operación normal de los servicios de TI.

- El protocolo contempla un modelo escalonado de atención, roles claramente definidos, procedimientos detallados de diagnóstico, resolución, comunicación y revisión post-incidente, así como la integración con otros procesos de gestión de servicios.

- Además, incorpora conceptos fundamentales como niveles de severidad, acuerdos de nivel de servicio (SLA), soluciones temporales (workarounds), gestión de la comunicación y mecanismos de mejora continua.

- Con ello, se busca proteger la integridad de los datos, minimizar el impacto sobre la comunidad académica y operativa, y fortalecer la resiliencia tecnológica de la institución.

1. Propósito y Alcance

- **Propósito:** Este protocolo define los procedimientos y responsabilidades para la detección, escalamiento, gestión y resolución de incidentes que afecten los servicios y la infraestructura tecnológica de la facultad. Su objetivo principal es minimizar el impacto de los incidentes, restaurar la operación normal de los servicios lo más rápido posible y prevenir futuras ocurrencias, contribuyendo a la continuidad del negocio y la satisfacción de los usuarios.

- **Alcance:** Este protocolo aplica a todos los usuarios (estudiantes, académicos, personal administrativo), personal técnico y administrativo involucrado en la operación y soporte del ecosistema tecnológico de la facultad. Incluye todos los sistemas, aplicaciones, redes, hardware e infraestructura del Datacenter gestionados por la Unidad de Desarrollo Tecnológico (UDT) de la FEN.

2. DEFINICIONES CLAVE

- **Incidente:** Cualquier evento inesperado que cause una interrupción o degradación en la calidad de un servicio o sistema de la facultad. Se diferencia de una solicitud de servicio, que es una petición rutinaria de información, acceso o soporte. Un incidente se distingue de un problema, que es la causa raíz de uno o más incidentes.
- **Severidad/Prioridad:** Clasificación de un incidente basada en su impacto (cantidad de usuarios afectados, criticidad del servicio) y la urgencia (tiempo de resolución esperado). La severidad determina la prioridad de atención y los SLAs aplicables.
    - **Crítico:** Afecta servicios esenciales (plataformas de enseñanza virtual, correo institucional, sistemas de gestión académica) e interrumpe operaciones clave de toda la Facultad (clases, pagos, inscripciones). Requiere atención inmediata 24/7 y la movilización de todos los recursos necesarios.
    - **Alto:** Afecta servicios importantes (impresoras compartidas, acceso a repositorios de datos) o a un número considerable de usuarios (un departamento completo). Requiere resolución rápida durante el horario laboral y una atención prioritaria.
    - **Medio:** Afecta servicios menores (acceso a una carpeta compartida específica) o a un grupo reducido de usuarios (un aula individual). Requiere atención en un plazo razonable, permitiendo la planificación de las actividades de soporte.
    - **Bajo:** Incidente menor con impacto mínimo o solo a un usuario (reemplazo de periférico, consulta funcional sin urgencia). Puede resolverse en el tiempo disponible, sin afectar la operación normal.

- **SLA (Service Level Agreement - Acuerdo de Nivel de Servicio):** Acuerdos formalizados que definen los tiempos de respuesta y resolución esperados para cada nivel de severidad/prioridad de los incidentes. Estos acuerdos establecen las expectativas de los usuarios y los compromisos del equipo de soporte.

- **Workaround (Solución Temporal):** Una medida provisional que permite restaurar el servicio o mitigar el impacto del incidente mientras se trabaja en la solución definitiva. Los workarounds deben documentarse claramente y comunicarse a los usuarios.

- **RTO (Recovery Time Objective - Objetivo de Tiempo de Recuperación):** El tiempo máximo aceptable en el que un servicio debe ser restaurado después de una interrupción grave. Este objetivo se define en el plan de continuidad del negocio.

- **RPO (Recovery Point Objective - Objetivo de Punto de Recuperación):** La cantidad máxima aceptable de pérdida de datos medida en tiempo. Este objetivo determina la frecuencia de las copias de seguridad.

- **ACR (Análisis de Causa Raíz):** Proceso sistemático para identificar las causas subyacentes de un incidente, más allá de los síntomas.

2.1. Tipos de Incidentes y Categorías Especiales

Los incidentes pueden tener distintas causas y características, por lo que es fundamental categorizarlos adecuadamente para facilitar su análisis, priorización y resolución.

A continuación, se detallan los tipos más frecuentes de incidentes tecnológicos según su naturaleza, con énfasis en aquellos que requieren tratamiento especializado.

a) Incidentes de Seguridad de la Información

- Este tipo de incidentes compromete directamente la confidencialidad, integridad o disponibilidad de la información institucional. Requieren un tratamiento urgente y específico, dada su potencial criticidad y el impacto legal y reputacional que pueden acarrear.
  - **Ejemplos:**
    - Acceso no autorizado a sistemas, bases de datos o cuentas de usuario (incluyendo cuentas privilegiadas).
    - Propagación de malware, ransomware o troyanos (incluyendo ataques de

cryptojacking).
- Fuga, pérdida o manipulación no autorizada de datos sensibles (incluyendo datos personales y propiedad intelectual).
- Suplantación de identidad (phishing dirigido a personal o estudiantes, ataques BEC).
- Exposición accidental de información confidencial (por ejemplo, configuración incorrecta de permisos).
- Ataques de denegación de servicio (DoS/DDoS) que interrumpen la disponibilidad de servicios críticos.
- Ataques de intermediario (MitM) que interceptan y modifican la comunicación entre sistemas.
- Vulnerabilidades de seguridad no parcheadas que son explotadas.

- **Tratamiento específico:**
  - Priorización crítica inmediata y asignación de un equipo de respuesta especializado.
  - Escalamiento a los niveles superiores de soporte y seguridad institucional (Oficial de Seguridad de la Información, Comité de Ciberseguridad de la U. de Chile), según el protocolo de la Universidad.
  - Activación de procedimientos de contención (aislamiento de sistemas afectados, cambio de contraseñas) y análisis forense (preservación de evidencia digital, análisis de logs).
  - Notificación obligatoria a la Agencia de Protección de Datos Personales (si hay fuga de datos personales) y a otras autoridades competentes, según la legislación vigente.
  - Comunicación transparente y oportuna a los usuarios afectados, según el protocolo de comunicación de incidentes de seguridad.
  - Registro detallado del incidente en el sistema de gestión (Jira u otro), incluyendo todos los hallazgos del análisis forense y las acciones tomadas.

b) Incidentes de Infraestructura de Cómputo

- Corresponden a eventos que afectan la operación de los servidores, almacenamiento o componentes físicos del datacenter. Estos incidentes pueden

causar interrupciones significativas en los servicios y requieren un diagnóstico y una resolución rápidos.

- **Ejemplos:**
  - Falla de discos duros, controladoras RAID o unidades de respaldo (incluyendo la pérdida de datos).
  - Interrupciones en servicios virtualizados (hipervisores, clusters, máquinas virtuales).
  - Problemas con el rendimiento de almacenamiento compartido o redes SAN (latencia, congestión).
  - Reinicios inesperados, errores de energía o fallos de hardware de servidores (CPU, memoria, fuente de alimentación).
  - Problemas con la infraestructura de red del datacenter (switches, cables).
  - Fallas en el sistema de alimentación ininterrumpida (UPS).

Tratamiento específico:

- Diagnóstico inmediato por Nivel 2 (plataforma/sistemas) o Nivel 3 si se requiere contacto con DELL u otros proveedores.
- Verificación del alcance e impacto del incidente: identificar si afecta a servicios productivos, sistemas académicos, backup o servicios críticos.
- Activación de soluciones alternativas si corresponde (failover, recuperación desde respaldo, uso de nodos redundantes, redirección de tráfico).
- Coordinación con soporte de fabricante si el incidente es físico o requiere intervención en garantía (hardware, firmware, reemplazo de partes).
- Recopilación y análisis de logs, errores de sistema y otra evidencia técnica relevante para la identificación de la causa raíz.
- Actualización detallada del ticket con todos los hallazgos y acciones tomadas.
- Comunicación proactiva y oportuna a los usuarios afectados, especialmente si hay una interrupción visible o prolongada.
- Documentación post-incidente completa para el análisis de causa raíz (si aplica) y la implementación de acciones preventivas.

c) Incidentes de Conectividad y Red

Relacionados con las capas 1 a 3 del modelo OSI (física, enlace de datos y red), estos incidentes afectan el acceso o el rendimiento de los servicios tecnológicos.

- **Ejemplos:**
  - Corte o daño en enlaces de fibra o cobre (internos o externos).
  - Falla de switches, routers, firewalls o balanceadores de carga.
  - Asignación incorrecta de direcciones IP/DHCP o problemas con el servicio DNS.
  - Saturación de enlaces WAN o enlaces redundantes caídos (problemas de ancho de banda).
  - Errores de configuración de VLANs, ACLs o rutas estáticas.
  - Problemas con la conectividad inalámbrica (Wi-Fi).
  - Ataques de denegación de servicio (DoS/DDoS) a la red.

Tratamiento específico:

- Diagnóstico inmediato de la capa OSI afectada (física, enlace, red) para aislar el problema.
- Verificación física y lógica de la infraestructura de red (estado de puertos, enlaces redundantes, STP, configuración de VLANs, ACLs, rutas estáticas, logs de switches/routers).
- Uso de herramientas de diagnóstico de red (ping, traceroute, sniffer) para identificar la causa del problema.
- Escalamiento a soporte de comunicaciones (Nivel 2/3) o al proveedor de servicios de internet (ISP) si hay fallo en la infraestructura externa o se requiere soporte especializado.
- Aislamiento de la zona afectada para minimizar el impacto en otros servicios (uso de backup link, rutas alternativas, desactivación temporal de servicios no esenciales).
- Aplicación de configuraciones temporales (ej., rutas manuales, activación de uplink secundario, cambio de VLAN) para restaurar la conectividad lo antes posible.
- Registro detallado del evento, topología afectada, equipos involucrados, configuraciones aplicadas y solución implementada.

- Evaluación del impacto en servicios dependientes (correo, DNS, acceso a internet, plataformas académicas, sistemas de autenticación).

d) Incidentes en Sistemas de Climatización y Contra Incendios

- Estos incidentes afectan la seguridad física y operativa del datacenter y requieren una respuesta rápida y coordinada para evitar interrupciones mayores y daños a la infraestructura tecnológica.

  - **Ejemplos:**
    - Fuga de gas refrigerante o fallas en los aires acondicionados del datacenter (incluyendo la pérdida de redundancia).
    - Temperaturas fuera de rango aceptable para los servidores (altas o bajas temperaturas).
    - Activación accidental o real del sistema de supresión por gas (NOVEC 1230 u otros).
    - Fallas en estrobos, sensores térmicos o presurización del sistema de supresión de incendios.
    - Alarmas de humo, calor o presión no respondidas o mal gestionadas.
    - Cortes de energía prolongados o fluctuaciones en el suministro eléctrico.

  - **Tratamiento específico:**
    - Alerta inmediata al proveedor de infraestructura (Netics SPA) y al personal de seguridad de la facultad, según el protocolo de contrato y los planes de emergencia.
    - Verificación de las condiciones de riesgo y su gravedad: temperatura crítica, fuga de gas, activación de alarma o sistema NOVEC, presencia de humo o fuego.
    - Evaluación del impacto potencial en los servicios y sistemas críticos.
    - Ejecución de contingencias físicas si aplica:
      - Cierre controlado de equipos para evitar daños por calor o falta de energía (siguiendo un procedimiento predefinido).
      - Traslado de servicios a un clúster activo fuera del datacenter (si está disponible y es viable).
      - Evacuación del personal del datacenter según el plan de emergencia.

- Coordinación directa y constante con Nivel 3 (Jefe de Desarrollo Tecnológico) y la Dirección Económica y Administrativa para la toma de decisiones de riesgo operativo y la asignación de recursos.
- Supervisión de las acciones del proveedor y garantía de que se cumplen los SLAs.
- Registro detallado del evento, las acciones del proveedor, el reemplazo de componentes, las pruebas de verificación funcional y el tiempo de inactividad de los servicios.
- Informe técnico obligatorio y detallado por parte del proveedor y análisis posterior (Post-Mortem) para identificar la causa raíz y prevenir recurrencias.

e) Otros Incidentes Operativos o Funcionales

- Relacionados con fallas en el uso de plataformas, software institucional, o interacción del usuario final con los sistemas. Estos incidentes suelen ser menos críticos, pero más frecuentes y pueden afectar la productividad de los usuarios.

  - **Ejemplos:**
    - Error en la autenticación de usuarios o problemas con servicios de directorio Cuenta FEN y Google.
    - Caídas o mal funcionamiento de servicios web, correo electrónico, plataformas académicas (Docencia Web, Canvas, Registro Curricular, SAD) o aplicaciones específicas.
    - Fallos de impresión, escaneo o acceso a carpetas compartidas.
    - Problemas en backups programados o restauraciones fallidas (errores de configuración, medios dañados).
    - Errores en la ejecución de scripts o procesos automatizados.
    - Problemas de rendimiento en aplicaciones (lentitud, congelamientos).

  - **Tratamiento específico:**
    - Registro inicial y análisis en Nivel 1 o Nivel 2 según la complejidad del incidente y la información disponible.
    - Aplicación de soluciones comunes documentadas en la base de conocimientos o en las guías de solución de problemas (ej., errores de login, bloqueo de cuentas, configuración de impresoras).

- Soporte remoto o presencial al usuario según la criticidad del incidente y el contexto (ej., sala de clases vs. oficina).
- Recopilación de información adicional del usuario (pasos para reproducir el error, mensajes de error, etc.).
- Escalamiento a Nivel 2 o Nivel 3 si el incidente requiere un análisis más profundo, la intervención de un especialista o la modificación de la configuración del sistema.
- Documentación detallada de la solución aplicada y, si no existía, actualización o creación de un nuevo artículo en la base de conocimientos para futuras referencias.
- Verificación de la recurrencia del incidente: si el incidente es repetitivo o afecta a varios usuarios, escalarlo como problema para un análisis de causa raíz y una solución a largo plazo.
- Comunicación empática y clara con el usuario final, proporcionando actualizaciones oportunas y gestionando las expectativas de atención y resolución.

3. Roles y Responsabilidades

- **Reportador de Incidente:** Cualquier usuario o miembro del personal que detecte una anomalía en un servicio o sistema.
    - *Responsabilidad:* Notificar el incidente a través del canal de comunicación establecido, proporcionando la mayor cantidad de detalles posible soporte.tecnologia@fen.uchile.cl.

- **Nivel 1 (Soporte de Primera Línea / Mesa de Ayuda):** Pablo Hormazabal, Antonio Araya Umaña
    - *Contacto:* Pablo Hormazabal (pormazabal@fen.uchile.cl, Tel: +56 985969355), Antonio Araya Umaña (aarayau@fen.uchile.cl, Tel: +56 950181848)
    - *Responsabilidades:*
        - Detección inicial, registro y clasificación del incidente en el sistema de tickets (Jira Service Desk).
        - Evaluación preliminar del incidente, incluyendo la recopilación de información adicional del reportador y la determinación del alcance e impacto inicial.
        - Intentar la resolución de problemas conocidos y de baja complejidad utilizando la base de conocimientos y las herramientas de diagnóstico disponibles.
        - Escalamiento del incidente al Nivel 2 o Nivel 3 según la clasificación de severidad/prioridad y el tipo de incidente, proporcionando toda la información relevante y el historial del ticket.
        - Comunicación inicial y actualizaciones básicas con el reportador del incidente, gestionando sus expectativas.

- **Nivel 2 (Soporte Especializado / Técnico):** Miguel Avello Moya, Jackson Gonzalez Sanchez

    - *Contacto:* Miguel Avello Moya (mavellom@fen.uchile.cl, Tel: +56 957198965), Jackson Gonzalez Sanchez (jacgonzale@fen.uchile.cl, Tel: +56 987688998)
    - *Responsabilidades:*
        - Análisis profundo y diagnóstico del incidente, utilizando herramientas de diagnóstico avanzadas y conocimientos especializados.
        - Implementación de soluciones definitivas (correcciones, parches) y/o soluciones temporales (workarounds) para restaurar el servicio.
        - Coordinación con proveedores externos (ej., software específico, hardware) si es necesario para obtener soporte o escalamiento adicional.
        - Actualización detallada del ticket con el progreso de la investigación, los pasos seguidos, las soluciones aplicadas y cualquier otra información relevante.
        - Comunicación proactiva con el Nivel 1 sobre el estado del incidente y las acciones tomadas.
        - Escalamiento al Nivel 3 si la resolución supera sus capacidades técnicas, requiere decisiones de alto nivel o implica un impacto significativo en la infraestructura.

- **Nivel 3 (Soporte de Infraestructura / Liderazgo Técnico / Dirección):**

    - **Jefe de Desarrollo Tecnológico:** [Mario Cuadra Seguel]
        - *Contacto:* [mcuadra@fen.uchile.cl, +56935244717]
        - *Responsabilidades:*
            - Liderazgo técnico en la resolución de incidentes complejos y estratégicos, proporcionando dirección y experiencia.
            - Desarrollo e implementación de soluciones a largo plazo para prevenir la recurrencia de incidentes y mejorar la estabilidad de los sistemas.

- Supervisión de la estrategia tecnológica post-incidente, incluyendo la evaluación de la necesidad de inversiones en infraestructura o cambios en los procesos.
- Coordinación general de las comunicaciones del incidente, especialmente en incidentes críticos.

- **Director Financiero:** [Pedro Carrizo]
  - *Contacto:* [pcarrizo@fen.uchile.cl, +56985297027]
  - *Responsabilidades:*
    - Evaluar el impacto financiero de incidentes críticos, especialmente aquellos que afectan la continuidad de las operaciones de la facultad.
    - Autorizar la asignación de recursos extraordinarios (personal, hardware, software) necesarios para la resolución del incidente y la recuperación de los servicios.
    - Participar en la toma de decisiones estratégicas que afecten la continuidad del negocio y la inversión en TI, considerando el equilibrio entre el costo de la resolución y el impacto del incidente.

- **Equipo Técnico de DELL (Proveedor de Infraestructura de Datacenter):**
  - *Contacto:* [Danisa Saldivia, +56977491877 o Mesa de Ayuda de DELL para la Facultad, Teléfono de Soporte Crítico]
  - *Responsabilidades:*
    - Soporte y resolución de incidentes relacionados con la infraestructura física y lógica del datacenter (servidores, almacenamiento, networking a nivel de hardware DELL) bajo contrato de servicio y los SLAs establecidos.
    - Escalamiento interno dentro de DELL si el incidente requiere experiencia especializada o la intervención de un nivel superior de soporte.
    - Comunicación proactiva y oportuna con el Nivel 2 y el Nivel 3 de la FEN sobre el progreso de la resolución.

- **Tline (Partner Especialista en Infraestructura y Seguridad):**
  - *Contacto:* [Monica Cardenas de Tline para la Facultad, +56985282648]
  - *Responsabilidades:*
    - Soporte técnico especializado en soluciones y tecnologías específicas de las que Tline es partner (software empresarial, soluciones de ciberseguridad, infraestructura avanzada, servicios gestionados).
    - Asesoramiento y orientación en la resolución de incidentes complejos relacionados con su área de especialización.
    - Transferencia de conocimiento al personal de la FEN para mejorar la capacidad de resolución interna.

- **Sistema contra Incendio:**
  - Contacto: Proveedor Netics SPA - Ingeniero Responsable: Francisco Marquez +56 9 7983 9342
  - Responsabilidades:
    - Asegurar la operatividad continua y segura del sistema de supresión de incendios del Data Center, ejecutando mantenciones preventivas y correctivas según las especificaciones técnicas y normativas vigentes.
    - Actuar de manera inmediata ante cualquier incidente para diagnosticar, corregir y restablecer el funcionamiento del sistema, incluyendo la reposición de componentes críticos como filtros, luces estroboscópicas con sirena y cilindros de gas, cuando corresponda.
    - Realizar pruebas de funcionamiento del sistema, documentar las acciones realizadas, registrar anomalías y emitir informes técnicos detallados.

- **Sistema Aire acondicionado:**
  - Contacto: Proveedor Netics SPA - Ingeniero Responsable: Francisco Marquez +56 9 7983 9342
  - Responsabilidades:

- Ejecutar labores de mantenimiento correctivo ante fallas en el sistema de climatización del Data Center, incluyendo el diagnóstico técnico y el reemplazo de componentes que presenten deterioro o pérdida de funcionalidad.
- Realizar intervenciones inmediatas ante incidentes relacionados con fugas o fatiga en las tuberías internas, incluyendo trabajos de soldadura para asegurar la continuidad operativa del sistema.
- Gestionar completamente el refrigerante, lo que implica la carga o recarga del gas necesario para mantener condiciones óptimas de enfriamiento.
- Frente a cualquier evento que afecte la estabilidad térmica del Data Center, el proveedor deberá activar protocolos de respuesta rápida, ejecutar acciones correctivas eficaces y minimizar el impacto sobre la infraestructura tecnológica crítica, todo ello dentro de los plazos definidos en los acuerdos de nivel de servicio.

- **Coordinador de Comunicaciones: Jefe de Desarrollo Tecnológico en conjunto con la Unidad de Comunicaciones y Recursos Humanos.**
    - *Contactos:* [mcuadra@fen.uchile.cl, Jefe de Desarrollo Tecnológico, Correo/Contacto Principal de la Unidad de Comunicaciones, Correo/Contacto Principal de Recursos Humanos]
    - *Responsabilidades:*
        - Gestionar y coordinar todas las **comunicaciones internas y externas** durante incidentes, especialmente los críticos.
        - Elaborar **comunicados de estado** para usuarios, directivos y, si es necesario, stakeholders externos.
        - Asegurar que la información sea **oportuna, precisa y adecuada** para cada audiencia.
        - Manejo de la comunicación con el personal afectado (por ejemplo, por interrupciones de servicio o cambios en horarios).

4. Flujo del Protocolo de Respuesta a Incidentes

4.1. Detección y Reporte de Incidentes

- **Proceso:** Un usuario, un sistema de monitoreo o cualquier miembro del personal detecta una anomalía o interrupción de servicio.
- **Canal de Reporte:** El incidente se reporta a través de la **plataforma de chat centralizada** [FEN-IT/Operaciones Whatsapp, Meet , Jira].
- **Generación de Ticket:** Una vez reportado, el sistema automáticamente **genera un ticket de seguimiento** en la herramienta [Jira Service Desk], asignándole un identificador único.
- **Información Requerida:** El reportador debe proporcionar la siguiente información mínima:
    - Descripción clara y concisa del problema.
    - Impacto percibido (ej. "No puedo acceder al sistema X", "El servidor Y no responde").
    - Capturas de pantalla o mensajes de error, si aplica.
    - Hora aproximada de inicio del incidente.
    - Usuarios afectados (si se conoce).

4.2. Escalación y Evaluación Inicial (Nivel 1)

- **Responsables:** Pablo Hormazabal y Antonio Araya Umaña.
- **Acciones:**
    - **Revisión inmediata del ticket** y la información proporcionada.
    - **Comunicación inicial** con el reportador para recabar más detalles si es necesario.
    - **Clasificación del Incidente:**
        - **Tipo de Incidente:** (Ej. Fallo de red, problema de software, seguridad, hardware, acceso).
        - **Severidad/Prioridad:** Determinación de si es Crítico, Alto, Medio o Bajo, basado en el impacto en los servicios y usuarios.
    - **Determinación del Alcance:** Identificar los sistemas, servicios y cantidad de usuarios potencialmente afectados.

- **Intentos de Resolución de Primera Línea:** Aplicar soluciones de primera línea o de conocimiento preexistente para problemas comunes.
- **Escalamiento:** Si el incidente no puede ser resuelto por Nivel 1 o su severidad lo requiere (Crítico, Alto), se escala al Nivel 2 o Nivel 3, proporcionando toda la información relevante y el historial del ticket.

4.3. Análisis y Diagnóstico (Nivel 2 y Nivel 3)

- **Responsables:** Nivel 2 o Nivel 3, según el nivel de escalamiento y la naturaleza del incidente.
- **Acciones:**
  - **Confirmación de Incidente:** Verificación y replicación del problema.
  - **Análisis Causa Raíz (ACR):** Identificación de la causa subyacente del incidente, no solo de los síntomas.
  - **Investigación Profunda:** Recopilación de logs, métricas de rendimiento, configuraciones de sistema, y cualquier otra información técnica relevante.
  - **Coordinación con Proveedores:** Si el incidente involucra servicios externos o infraestructura gestionada por DELL o Tline, se activan los canales de soporte correspondientes y se colabora en el diagnóstico.
  - **Determinación de Solución:** Planificación y diseño de la acción correctiva o el workaround.

4.4. Resolución e Implementación

- **Responsables:** Nivel 2 o Nivel 3 (incluyendo DELL/Tline si aplica).
- **Acciones:**
  - Desarrollo e **implementación de la solución** o workaround planificado.
  - **Pruebas exhaustivas** para verificar que el incidente ha sido resuelto y que los servicios afectados operan con normalidad.
  - **Documentación de la solución** aplicada y de los pasos realizados en el ticket del incidente.

4.5. Comunicación del Incidente

- **Responsables:** Coordinador de Comunicaciones (Jefe de Desarrollo Tecnológico, Unidad de Comunicaciones y Recursos Humanos).
- **Acciones:**
    - **Interna:**
        - Actualizaciones regulares a los equipos de Nivel 1 y Nivel 2 sobre el progreso y estado de la resolución.
        - Información oportuna a la dirección de la facultad sobre incidentes críticos.
    - **Externa (a usuarios y stakeholders):**
        - Envío de **notificaciones sobre el estado del incidente** (inicio, progreso, restauración de servicio) a través de canales definidos (ej. correo electrónico masivo, intranet, banner en el sitio web de la facultad).
        - Las comunicaciones deben ser claras, concisas y gestionar las expectativas de los usuarios.
        - [Se recomienda usar plantillas de comunicación predefinidas para agilizar el proceso, ver Anexo C].

4.6. Cierre del Incidente

- **Responsables:** Nivel 1 o el equipo que resolvió el incidente.
- **Acciones:**
    - **Verificación final** con el reportador/usuario de que el servicio ha sido completamente restaurado a su estado normal.
    - **Documentación completa de la resolución** y la causa raíz (si se identificó) en el ticket.
    - **Clasificación del incidente** como "Resuelto" y luego "Cerrado" en el sistema de tickets.
    - Asegurarse de que todos los pasos del protocolo se hayan seguido.

4.7. Post-Incidente (Revisión y Lecciones Aprendidas)

- **Responsables:** Equipo involucrado en el incidente (Nivel 2, Nivel 3, Gerencia de TI).
- **Acciones:**
    - Para **incidentes críticos o recurrentes**, realizar un **análisis post-incidente (Post-Mortem)** en un plazo definido.
    - Identificar **lecciones aprendidas** y **oportunidades de mejora** en procesos, herramientas, capacitación del personal y arquitectura de sistemas.
    - Implementar **acciones preventivas o correctivas** a largo plazo para evitar futuras reincidencias del mismo tipo de incidente.
    - **Actualizar la base de conocimientos** con la nueva información, soluciones y workarounds para futuras referencias.
    - Revisar y ajustar los SLAs si es necesario.

5. Anexos

- **Anexo A: Matriz de Clasificación de Incidentes**
  - Tabla que detalla los criterios para definir la severidad (Crítico, Alto, Medio, Bajo) en función del impacto en el negocio y la urgencia de la resolución.

Severidad	Impacto	Urgencia	Ejemplos	Tiempo de respuesta
Crítico	Interrumpe servicios esenciales de forma total. Afecta operaciones clave de toda la Facultad.	Inmediata. Afecta clases, procesos administrativos o datos sensibles.	- Caída total de red o correo institucional. - Servidores críticos fuera de servicio. - Fuga de datos o ransomware.	15 minutos (atención) 2 horas (resolución temporal)
Alto	Afecta servicios relevantes o a un número considerable de usuarios.	Alta. Necesita intervención durante el día.	- Caída de impresoras compartidas. - Problemas masivos de acceso al sistema académico.	1 hora (atención) 4 horas (resolución temporal)
Medio	Impacto moderado. Servicios secundarios o grupos pequeños.	Moderada. Puede esperar una ventana de resolución estándar.	- Usuario no puede acceder a su cuenta. - Problemas en conexión de aula individual.	4 horas (atención) 1 día (resolución)
Bajo	Impacto mínimo. Afecta a un solo usuario o función no crítica.	Baja. Puede resolverse según disponibilidad.	- Reemplazo de periférico. - Consulta funcional o solicitud sin urgencia.	1 día (atención) 3 días (resolución)

- **Anexo B: Lista de Contactos de Emergencia**
    - Números de contacto fuera de horario de todos los niveles, incluyendo proveedores externos clave (Dell, Tline, etc.).

Nombre / Cargo	Rol	Correo	Teléfono directo / celular
Roberto Inostroza	Nivel 2 / Gestión técnica	rinostroza@fen.uchile.cl	Tel. +56 9 9844 0384
Jackson Gonzalez Sanchez	Nivel 2 / Gestión técnica	jacgonzale@fen.uchile.cl	Tel. +56 9 87688998
Miguel Avello Moya	Nivel 2 / Soporte técnico	mavellom@fen.uchile.cl	Tel. +56 9 57198965
Mario Cuadra Seguel	Nivel 3 / Jefe Desarrollo Tecnológico	mcuadra@fen.uchile.cl	Tel. +56 9 35244717
Pedro Carrizo	Nivel 3 / Director Financiero	pcarrizo@fen.uchile.cl	Tel. +56 9 85297027
Pablo Hormazabal	Nivel 1 / Mesa de Ayuda	pormazabal@fen.uchile.cl	Tel. +56 9 85969355
Antonio Araya Umaña	Nivel 1 / Mesa de Ayuda	aarayau@fen.uchile.cl	Tel. +56 9 50181848
Danisa Saldivia (DELL)	Soporte datacenter hardware	danisa.saldivia@dell.com	Tel. +56 9 77491877
Mónica Cárdenas (Tline)	Soporte seguridad e infraestructura	mcardenas@tline.cl	Tel. +56 9 85282648
Francisco Márquez (Netics)	Climatización y supresión incendios	fmarquez@netics.cl	Tel. +56 9 79839342

- **Anexo C: Lista de Contactos de OSI – ANCI.**

Nombre / Cargo	Rol	Correo	Teléfono directo / celular
Cristopher Follin	Oficial de Seguridad de la Información (VTI)	christopher.follin@uchile.cl	+56985073331
Monitoreo OSI	Monitoreo (VTI	monitoreo.osi@uchile.cl	+56985073331
Benjamin Iturra	ANCI - Lead		+56959193114
Manuel Varela	ANCI – Analista		+56931347693
Cesar Lopez	ANCI – Analista		+56931347693
Eduardo Rivera	ANCI – Analista	eriveros@interior.gob.cl	+56982171920

Ley 21663

LEY MARCO DE CIBERSEGURIDAD
MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA
Publicación: 08-ABR-2024 | Promulgación: 26-MAR-2024
Versión: Última Versión De : 01-MAR-2025
Url Corta: https://bcn.cl/ZuSFox

Párrafo 2°
Obligaciones de ciberseguridad

Artículo 7°. Deberes generales. Las instituciones obligadas por la presente ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

El cumplimiento de estas obligaciones exige la debida implementación de los protocolos y estándares establecidos por la Agencia, así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva. El objeto de estos protocolos y estándares será la prevención y gestión de los riesgos asociados a la ciberseguridad, así como la contención y mitigación del impacto que los incidentes puedan tener sobre la continuidad operacional del servicio prestado o la confidencialidad y la integridad de la información o de las redes o sistemas informáticos, de conformidad con lo prescrito
en la presente ley.

Para efectos de emitir las medidas de seguridad a que se refiere el inciso primero, la Agencia deberá observar lo prescrito en el artículo 25, según corresponda. Dichos protocolos y estándares deberán someterse a consulta pública, en la misma forma y plazo señalados en el inciso tercero del artículo 6°. La medida deberá publicarse junto con el informe en que se justifique el rechazo o modificación de las observaciones que correspondan.
La Agencia deberá establecer medidas de seguridad diferenciadas según el tipo de organización de que se trate, teniendo especialmente en consideración las características y posibilidades de las pequeñas y medianas empresas definidas por la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño.

Artículo 8°. Deberes específicos de los operadores de importancia vital. Todos los operadores de importancia vital deberán:

a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de

las redes, sistemas informáticos y datos, y la continuidad operacional del servicio.

Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de revisiones periódicas por parte de los sujetos obligados, con una frecuencia mínima de dos años.

Con todo, la Agencia podrá instruir a uno o más operadores de importancia vital, fundadamente y por motivos sobrevinientes graves, la certificación de sus planes de continuidad operacional o ciberseguridad en un plazo menor al indicado en el párrafo precedente; sin embargo, la Agencia sólo podrá ejercer esta facultad, respecto de cada operador de importancia vital, siempre que la certificación tenga, al menos, un año de vigencia.
d) Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Nacional, en la forma que determine el reglamento.

e) Adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario.

f) Contar con las certificaciones que señala el artículo 28.

g) Informar a los potenciales afectados, en la medida que puedan identificarse y cuando así lo requiera la Agencia, sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

h) Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.

i) Designar un delegado de ciberseguridad, quien actuará como contraparte de la Agencia e informará a la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado o a los directores, gerentes, administradores o ejecutivos principales, según lo definan las instituciones privadas.

Artículo 9°. Deber de reportar. Todas las instituciones públicas y privadas señaladas en el artículo 4° tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27, tan pronto les sea posible y conforme al siguiente esquema:

a) Dentro del plazo máximo de **tres horas** contado desde que se tiene conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad que pueda tener impactos significativos, se deberá enviar una alerta temprana sobre la ocurrencia del evento.

b) Dentro del plazo máximo de **setenta y dos horas**, una actualización de la información contemplada en la letra a), que incluya una evaluación inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles.

Sin embargo, en caso de que la institución afectada fuera un operador de importancia vital y éste viera afectada la prestación de sus servicios esenciales a causa del incidente, la actualización de la información deberá entregarse al CSIRT Nacional en el plazo máximo de **veinticuatro horas** contado desde que haya tenido conocimiento del incidente.

c) Dentro del plazo máximo de **quince días corridos** contado desde el envío de la alerta temprana contemplada en la letra a), un informe final en el que se recojan, al menos, los siguientes elementos:

i. Una descripción detallada del incidente, incluyendo su gravedad e impacto.
ii. El tipo de amenaza o causa principal que probablemente haya causado el incidente.
iii. Las medidas de mitigación aplicadas y en curso.
iv. Si procede, las repercusiones transfronterizas del incidente.

d) En el caso de que el incidente siga en curso con posterioridad a la presentación del informe contemplado en el literal c), éste se reemplazará por un informe sobre la situación en ese momento. El informe final deberá ser presentado en el plazo de quince días corridos contado desde que se haya gestionado el incidente.

Sin perjuicio de lo anterior, tanto el CSIRT Nacional como la autoridad Sectorial competente, podrán requerir las actualizaciones pertinentes sobre la situación.

Los operadores de importancia vital deberán, además, informar al CSIRT Nacional su plan de acción, tan pronto lo hubieren adoptado. El plazo para la adopción de un plan de acción en ningún caso podrá ser superior a siete días corridos contados desde que se tuvo conocimiento de la ocurrencia del incidente.

En el caso de los organismos del Estado, para el cumplimiento del deber

establecido en este artículo, los jefes de servicio deberán exigir a los proveedores de servicios de tecnologías de la información que compartan la información sobre vulnerabilidades e incidentes que puedan afectar a las redes y sistemas informáticos de los organismos del Estado, y siempre que tenga por objeto prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o reforzar el nivel de ciberseguridad y garantizar, a su vez, que se respete la posible naturaleza delicada de la información compartida. Con el objeto de cumplir con lo anterior, los contratos de prestación de servicios no podrán contener ninguna cláusula que pueda restringir o dificultar de cualquier modo la comunicación de información sobre amenazas por parte del prestador de servicios, siempre y cuando con ello no se comprometa la seguridad y protección de datos, incluida la confidencialidad y protección de la propiedad intelectual.

La Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo. En caso de existir la obligación de notificar a más de una autoridad, la Agencia en conjunto con las autoridades involucradas, y conforme lo dispuesto en el artículo 24, procurará poner a disposición de los obligados un sistema de ventanilla única que permita notificarlas simultáneamente.

Un reglamento expedido por el Ministerio encargado de la seguridad pública regulará el contenido de las diversas clases de reportes señalados en este artículo.

- **Anexo D: Plantillas de Comunicación**
    - Ejemplos de correos electrónicos o mensajes para notificar a usuarios sobre el inicio, progreso y resolución de incidentes.

a) Comunicación Inicial del Incidente (Notificación)

Estimados usuarios,
Informamos que desde las [hora] se ha detectado una interrupción en el servicio [nombre del servicio]. Nuestro equipo técnico ya está trabajando para identificar la causa y restablecer la operación lo antes posible.

Agradecemos su comprensión. Se enviarán actualizaciones oportunamente.

Atentamente,
Equipo de Soporte FEN

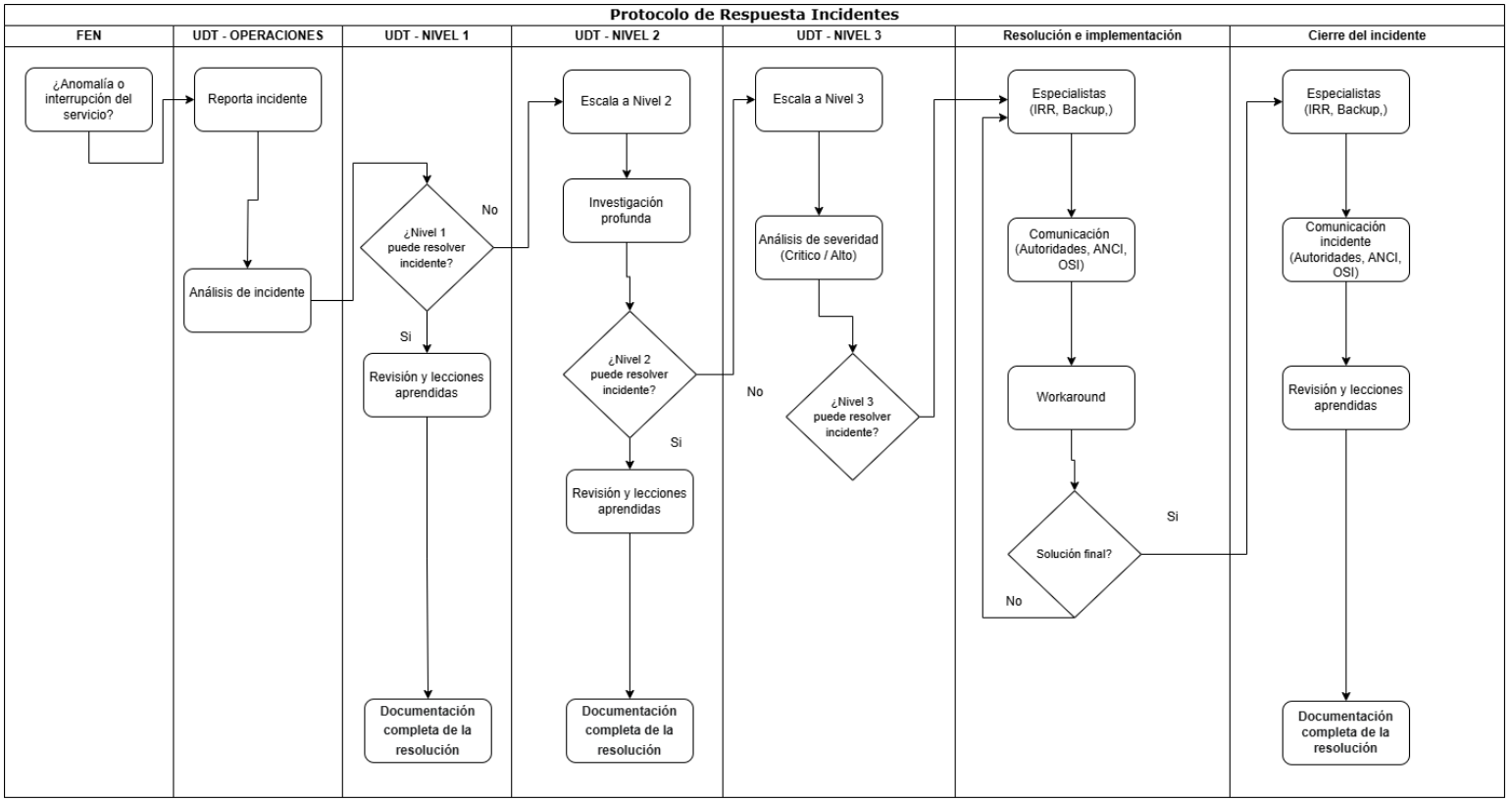
b) Actualización de Progreso

Estimados,
Les informamos que el incidente detectado en [nombre del servicio] continúa en análisis. Se ha identificado [breve resumen de causa probable o área técnica afectada].

Continuamos trabajando junto a nuestro equipo técnico / proveedor para restablecer el servicio. Próxima actualización estimada: [hora o fecha].

Atte.,
Equipo de Soporte FEN

- **Anexo E: Diagrama de Flujo del Protocolo de Incidentes**
  - Representación visual simplificada del flujo de trabajo de respuesta a incidentes.



6. Historial de Revisiones del Documento

Versión	Fecha	Descripción del Cambio	Autor
1.0	27/05/2025	Creación inicial del documento.	[Mario Cuadra Seguel]
1.1	28/05/2025	Incorporación de Dell, Tline, Jefe de Desarrollo Tecnológico y Director Financiero en Nivel 3.	[Mario Cuadra Seguel]
1.2	28/05/2025	Definición de Coordinador de Comunicaciones como rol conjunto (Jefe Desarrollo Tecnológico, Unidad Comunicaciones, RRHH).	[Mario Cuadra Seguel]

FACULTAD ECONOMÍA Y NEGOCIOS
UNIVERSIDAD DE CHILE

APROBADO POR : Pedro Carrizo Polanco
CARGO : Director Económico y Administrativo
DIRECCIÓN : Dirección Económica y Administrativa

Pedro Antonio Carrizo Polanco

Firmado digitalmente por Pedro Antonio Carrizo Polanco