AIEP
DE LA UNIVERSIDAD ANDRES BELLO

Plan de Respuesta y Mitigación frente a Incidentes de Seguridad Informática.

Nombre del módulo: Trabajo de Aplicación Práctica.

Fecha:14/01/2026

Tabla de contenidos

1. Introducción.

El siguiente documento de Aplicación Práctica para la homologación de la Práctica Profesional de Técnico en Ciberseguridad aborda la creación y ejecución de un Plan de Respuesta y Mitigación frente a Incidentes de Seguridad Informática destinado a la Municipalidad de Cerro Navia.

La elaboración del plan se fundamenta en la evaluación de la infraestructura tecnológica existente en la institución, teniendo en cuenta tanto los sistemas internos como las plataformas externas gestionadas por terceros. Además, está en consonancia con los requisitos académicos establecidos por la asignatura, las mejores prácticas del sector y los estándares internacionales en seguridad de la información.

2. Descripción de la Entidad (Municipalidad de Cerro Navia)

2.1 Contexto Organizacional

La Municipalidad de Cerro Navia es un organismo público que se ocupa de la gestión comunal y la provisión de servicios a los ciudadanos, manejando datos delicados relacionados con residentes, empleados, proveedores y programas sociales.

2.2 Infraestructura Tecnológica

- Computadoras con Windows para los trabajadores municipales
- Servidores locales y soluciones en la nube (correo corporativo, plataformas del gobierno)
- Red LAN y conexión WiFi oficial
- Proveedor de Internet y gestión de la red municipal llevada a cabo por un tercero externo (Mundo)
- Accesos remotos restringidos: solamente una empleada en modalidad de teletrabajo

• Sistemas de terceros gestionados por otras empresas:

- CAS Chile (sistema externo con soporte y administración del proveedor)
- Cero Papel (plataforma externa gestionada por la empresa proveedora)
- Sistemas internos municipales (recursos humanos, finanzas, archivos, servicios administrativos)

2.3 Datos Importantes Administrados

- Datos Importantes Administrados
- Datos Importantes Administrados
- Información personal de personas (Ley 19.628)
- Datos de empleados municipales
- Archivos administrativos y financieros
- Claves de acceso a plataformas institucionales

3. Análisis de Vulnerabilidades y Riesgos

3.1 Vulnerabilidades Identificadas

- Sistemas operativos que aún no han recibido actualizaciones.
- Compartición o reutilización de contraseñas.
- Carencia de división entre diferentes sectores municipales.
- Falta de entrenamientos formales para empleados en temas de ciberseguridad, en particular sobre cómo prevenir phishing, ingeniería social y uso adecuado del correo electrónico.
- Conciencia insuficiente en ciberseguridad entre los empleados.
- Riesgo de exposición de una dirección IP pública asignada a un empleado que trabaja de forma remota, utilizada para acceder al sistema CAS Chile.
- Dependencia de servicios externos (CAS Chile y Cero Papel), lo que restringe el control directo sobre la infraestructura, así como la seguridad y la gestión de posibles incidentes.
- Dependencia de un proveedor externo (Mundo) para la gestión de la red y conexión a Internet.
- Falta de controles adicionales que complementen la seguridad (autenticación multifactor institucional, políticas de acceso uniformes).
- Copias de seguridad sin comprobaciones periódicas documentadas.

3.2 Riesgos Asociados

A continuación, se muestra la tabla de riesgos vinculada a la infraestructura tecnológica del municipio de Cerro Navia, teniendo en cuenta amenazas importantes y su posible efecto en el funcionamiento institucional:

Riesgo	**Impacto**	**Probabilidad**	**Nivel de Riesgo**
Phishing a funcionarios	Alto	Alto	**Crítico**
Fuga de datos personales	Alto	Medio	**Alto**
Malware / Ransomware	Alto	Medio	**Alto**
Caída de sistemas municipales	Alto	Bajo	**Medio**
Accesos indebidos a información sensible	Alto	Medio	**Alto**

4. Normas y Estándares Aplicados

- ISO/IEC 27001 – Sistema de Dirección de Seguridad de la Información
- ISO/IEC 27002 – Medidas de seguridad
- NIST SP 800-61 – Guía para Manejo de Incidentes de Seguridad Informática
- NIST CSF – Estructura de Ciberseguridad
- Mejores prácticas ITIL (gestión de incidentes)

5. Plan de Respuesta ante Incidentes

5.1 Clasificación de Incidentes

- **Incidentes de baja gravedad:** malware limitado, intentos de acceso no exitosos
- **Incidentes de gravedad moderada:** ataques de phishing que logran éxito, interrupción parcial de servicios
- **Incidentes severos:** ransomware, filtración de información, compromiso de servidores.

5.2 Etapas del Plan de Respuesta

1. Preparación

- Documentación de normas de seguridad
- Entrenamiento a los usuarios
- Instalación de herramientas de vigilancia
- Estrategia de respaldo y restauración

2. Identificación y Evaluación

- Supervisión de registros
- Notificaciones automáticas
- Informes de usuarios
- Evaluación de señales de compromiso (IoC)

3. Contención

- Aislamiento de dispositivos impactados
- Cierre de cuentas en riesgo
- Segmentación temporal de la red

4. Erradicación

- Eliminación de software malicioso
- Implementación de actualizaciones
- Modificación de claves de acceso
- Evaluación de configuraciones

5. Recuperación

- Restauración desde copias de seguridad
- Verificación de servicios
- Vigilancia después del incidente

6. Lecciones Aprendidas

- Informe conclusivo sobre el incidente
- Fortalecimiento de controles
- Revisión del plan

6. Procedimientos de Recuperación y Contingencia

6.1 Sistema de Respaldos Existente

La Municipalidad de Cerro Navia dispone de un sistema de respaldos que ya está en funcionamiento y en uso, gestionado a través de la plataforma Xen Orchestra, que se utiliza para manejar máquinas virtuales y para realizar copias de seguridad del entorno XCP-ng.

Los respaldos se llevan a cabo de manera automática todos los días, siguiendo la regla 3-2-1, lo que garantiza que los sistemas se puedan recuperar y estar disponibles ante problemas de seguridad o fallos operativos.

6.2 Estructura de Servidores de Respaldo

La estrategia de respaldo toma en cuenta la infraestructura de servidores virtuales, distribuidos en estos grupos:

- **xcp-ng1 Principal:** servicios de Apache, bases de datos y el servidor principal de Minio.
- **xcp-ng2 Secundario:** servicios de Apache, bases de datos y el servidor secundario de Minio.
- **xcp-ng3 Servicios:** servidores de almacenamiento de archivos, Firmadoc, LimeSurvey, diversos servidores de Minio, VNC y WebAntigua.
- **xcp-ng4 Gestión:** equilibrador, Directorio Activo (NSDC1), Servidor de Impresiones y servidor de tiempo.
- **xcp-ng5 DNS Principal:** servicios de DNS tanto externos como internos.
- **xcp-ng6 DNS Secundario:** respaldo del servicio de DNS.

Esta estructura facilita la división de funciones, la duplicación de servicios esenciales y un plan de recuperación más efectivo.

6.3 Procesos de Recuperación

- Reinstalación total de máquinas virtuales a través de Xen Orchestra.
- Recuperación mediante snapshots en función de la importancia del servicio.
- Enfoque en sistemas esenciales (DNS, Active Directory, bases de datos, archivos).
- Comprobación de la integridad y operatividad tras la restauración.

6.4 Estrategia de Contingencia

- Colaboración con un proveedor externo (Mundo) en caso de problemas de red.
- Escalamiento interno según la gravedad del servicio afectado.
- Documentación y registro de incidentes y procesos de recuperación efectuados.

7. Normas de Seguridad (CIA)

Confidencialidad

- Restricción de acceso según roles
- Encriptación de datos delicados
- Implementación de autenticación multifactor

Integridad

- Supervisión de modificaciones
- Creación de hash y verificación de archivos
- Registros de auditoría

Disponibilidad

- Sistemas redundantes
- Copias de seguridad
- Vigilancia de servicios esenciales

8. Herramientas Empleadas

- Software antivirus / EDR (Microsoft Defender, Sophos, entre otros).
- SIEM (Wazuh, Splunk, ELK).
- Escáneres de vulnerabilidades (Nessus, OpenVAS).
- Cortafuegos y sistemas de detección/preventivos de intrusiones.
- Herramientas para copias de seguridad.

9. Archivos e Informes

- Anotación de sucesos
- Registro de actividades
- Reportes técnicos y de gestión
- Revisión de normas internas

10. Trabajo en Equipo y Comunicación

En la actualidad, la Municipalidad de Cerro Navia no dispone de un esquema formal para el trabajo conjunto en temas de ciberseguridad, ni ha definido un CSIRT interno, ni ha establecido roles específicos, ni tiene procedimientos documentados para la comunicación y el manejo de incidentes de seguridad.

La administración de los temas tecnológicos y de seguridad se rige principalmente por la Política del Área Informática, que proporciona directrices generales, pero no incluye de manera específica:

- Roles establecidos para la atención de incidentes relacionados con ciberseguridad.
- Canales formales para reportar eventos de seguridad.
- Procedimientos para la escalación de incidentes.
- Coordinación organizada entre las áreas de TI, legal y la alta dirección en situaciones de seguridad de la información.

Esta situación significa que la respuesta ante incidentes de ciberseguridad se basa en reacciones espontáneas en lugar de un proceso previamente definido, lo que podría afectar los tiempos de respuesta, la adecuada notificación y la gestión global de los riesgos relacionados con la seguridad de la información.

11. Uso Responsable y Ético de la Información

- Cumplimiento de la **Ley N°19.628 sobre Protección de datos personales.**
- Principio de mínima información necesaria.
- Uso responsable de sistemas municipales.
- Confidencialidad de la información ciudadana.
- Concientización y capacitación continua a funcionarios.

11.1 Conciencia y Formación en Ciberseguridad (Requisito Normativo)

Según la Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información (Ley N° 21.663), las entidades del sector público están obligadas a implementar medidas organizativas que se centren en la prevención, identificación y respuesta ante incidentes de ciberseguridad, abarcando tanto controles técnicos como aquellos relacionados con el aspecto humano y organizacional.

De igual forma, la Política de Seguridad de la Información y Protección de Datos de la Municipalidad de Cerro Navia establece la necesidad de fomentar la divulgación de la política, así como la formación y concienciación de los empleados y el personal externo que accede a los activos de información institucionales, reconociendo la importancia del factor humano en la salvaguarda de la información.

En el ámbito de estándares internacionales, esta exigencia se alinea con las siguientes normas y buenas prácticas del sector:

- ISO/IEC 27001: Control A. 6 – Conciencia, educación y formación en seguridad de la información.
- ISO/IEC 27002: Controles relacionados con el comportamiento seguro de los usuarios y la mitigación de riesgos vinculados a fallos humanos.
- ISO/IEC 27035: Gestión de incidentes de seguridad de la información, que establece que los usuarios deben ser capaces de identificar y reportar incidencias de manera oportuna.
- NIST Cybersecurity Framework (CSF): Función Protect, categoría Conciencia y Formación (PR. AT).

En este marco, la concienciación en ciberseguridad no es una opción, sino un requisito normativo y organizacional, destinado a disminuir riesgos como el phishing, la ingeniería social, el mal uso del correo institucional y la gestión inadecuada de credenciales de acceso.

En la actualidad, no se observan iniciativas formales y sistemáticas de capacitación sobre estos temas dentro de la organización, lo que representa una falta de implementación en relación con la normativa legal, los estándares internacionales y la política interna vigente.

Como referencia para el cumplimiento, estas acciones deberían incluir, al menos:

Detección de correos electrónicos maliciosos (phishing).

Prevención de ataques de ingeniería social.

Mejores prácticas en el uso del correo institucional y la gestión de contraseñas.

Procedimientos para la notificación oportuna de incidentes de seguridad de la información.

Este análisis se lleva a cabo con objetivos académicos, en el contexto de la convalidación de la práctica profesional, sin implicar la implementación directa de campañas ni cambios en los sistemas productivos existentes.

11.2 Recomendación Futura (No Obligatoria).

Como mejora futura y sin carácter obligatorio, se recomienda la implementación gradual de campañas de concientización en ciberseguridad dirigidas a los funcionarios municipales, enfocadas principalmente en:

- Identificación de correos electrónicos maliciosos (phishing).
- Prevención de ingeniería social.
- Buenas prácticas en el uso del correo institucional y contraseñas.
- Reporte oportuno de incidentes de seguridad.

Estas campañas podrían realizarse mediante charlas breves, material informativo digital o cápsulas educativas, sin requerir intervenciones técnicas sobre los sistemas productivos ni plataformas externas administradas por terceros. Su objetivo es reducir el riesgo humano y fortalecer la cultura de seguridad de la información dentro de la organización.

12. Implementación Práctica y Validación de Práctica Profesional

Declaración académica: Este esquema se elabora con propósitos académicos para validar la práctica profesional, sin interferir ni modificar sistemas productivos o plataformas externas gestionadas por terceros.

12.1 Función del Estudiante en la Implementación Práctica

El estudiante actúa como Técnico en Ciberseguridad, involucrándose de manera activa en actividades de análisis, implementación y creación de documentos sobre controles de seguridad, replicando un entorno laboral auténtico. Las actividades realizadas abarcan:

• Detección de vulnerabilidades en redes y sistemas.

• Asistencia en la implementación de medidas de seguridad.

• Realización de procedimientos para la respuesta a incidentes.

• Manejo de herramientas técnicas de ciberseguridad.

• Creación de documentación técnica y elaboración de informes.

12.2 Actividades Prácticas Realizadas

Durante la etapa de aplicación práctica se llevaron a cabo las siguientes tareas:

1. Recolección de datos sobre la infraestructura tecnológica.
2. Evaluación de riesgos y áreas vulnerables.
3. Elaboración y registro del Plan de Respuesta a Incidentes.
4. Ejercicios de simulación de incidentes (phishing, malware, accesos no autorizados).
5. Implementación de procedimientos de contención y recuperación tanto en formato documental como metodológico.
6. Creación de informes técnicos junto con recomendaciones.

12.2.1 Duración de la Aplicación Práctica

Esta práctica profesional se concreta a través del presente documento de aplicación práctica, que reúne las tareas, análisis y procedimientos realizados a lo largo del periodo formativo del estudiante.

La institución no especifica un número determinado de horas de asistencia ni requiere la validación por medio de la firma de un supervisor, considerando este informe como pruebas suficientes de la práctica profesional, de acuerdo con las directrices académicas proporcionadas.

12.3 Pruebas de Aprendizaje

Las pruebas vinculadas a esta práctica incluyen:

• Documento del Plan de Respuesta y Mitigación para Incidentes.

• Matriz de amenazas y debilidades.

• Registros de incidentes ficticios.

• Informes técnicos sobre el análisis y las acciones realizadas.

• Documentación de normas y procedimientos.

12.4 Habilidades Técnicas Presentadas

• Manejo básico de incidentes relacionados con ciberseguridad.

• Implementación de normas de seguridad de la información.

• Manejo de herramientas de vigilancia y protección.

• Análisis técnico y generación de documentación profesional.

12.5 Habilidades Transversales y de Valor para el Empleo

• Colaboración en equipos de tecnología de la información.

• Comunicación clara con usuarios y grupos técnicos.

• Compromiso y ética en el ámbito laboral.

• Planificación y manejo del tiempo.

13. Conclusión

Esta aplicación práctica muestra que el alumno posee las habilidades tanto técnicas como transversales requeridas para actuar como Técnico en Ciberseguridad, alcanzando los propósitos educativos de la práctica profesional.

La creación de este Plan de Respuesta y Mitigación ante Incidentes confirma la habilidad del estudiante para poner en práctica sus conocimientos teóricos en situaciones reales, en sintonía con las demandas del mercado laboral contemporáneo y los estándares de calidad de la industria.

El diseño de este plan facilitó la implementación práctica de lo aprendido en la capacitación técnica en ciberseguridad, teniendo en cuenta las condiciones reales de una entidad pública, sus restricciones y sus dependencias externas, además de ajustar el análisis a la legislación actual y a las mejores prácticas del sector. Todo esto se enmarca en una experiencia educativa enfocada en la empleabilidad y en el ejercicio responsable de la profesión.

14. Referencias

Gobierno de Chile. (2024). *Ley N° 21.663: Ley marco de ciberseguridad e infraestructura crítica de la información*. Biblioteca del Congreso Nacional de Chile.

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

International Organization for Standardization. (2022). *ISO/IEC 27002: Information security, cybersecurity and privacy protection — Information security controls*. ISO.

International Organization for Standardization. (2016). *ISO/IEC 27035: Information security incident management*. ISO.

National Institute of Standards and Technology. (2012). *Computer security incident handling guide (Special Publication 800-61 Rev. 2)*. U.S. Department of Commerce.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. NIST.