Desarrollo de un esquema de Gestión de Riesgos Informáticos en la Universidad Nacional de Río Negro

LUGANI Carlos Fabián, PEÑA Ricardo Luis

Laboratorio de Informática Aplicada, Sede Atlántica, Universidad Nacional de Río Negro
{clugani, rlpena}@unrn.edu.ar

Resumen. La actual gestión de las Tecnologías de la Información y las Comunicaciones requiere que se cumplan con estándares ampliamente aceptados por otros pares, instituciones y la misma organización. Para aplicar cualquier tipo de política, norma o estándar es necesario cumplir antes con ciertas premisas de base, las cuales de no existir, complican el desarrollo de cualquier sistema de gestión. Es común tratar con organizaciones que desean cumplir con un sistema de Gestión de Riesgos, Gestión de Seguridad o incluso Gestión de Calidad que no cuentan con inventarios de sus activos de información, si bien la simple identificación de esos activos es una visión estática. El objetivo de este trabajo es definir un esquema de Gestión de Riesgos Informáticos, y hacer un desarrollo de las primeras etapas de Relevamiento y Clasificación de Activos Informáticos, lo que permitirá una vez implementado, continuar y finalizar con la descripción del esquema completo. Este proceso se diseñó para ser implementado en la Universidad Nacional de Río Negro.

1 Introducción

La actividad principal que se describe es un proceso de gestión de riesgos para los activos informáticos de una organización, como primera definición se destaca que los riesgos están relacionados o asociados con los activos. Se comienza definiendo conceptos clave como son el riesgo, activo informático, integridad, confidencialidad y disponibilidad, enumerando luego las diferentes etapas del proceso de gestión de riesgos y justificando su aplicación. Se describe además, como contenido principal, un esquema de gestión. Mediante este esquema se proporciona una guía de actividades orientadas a facilitar la realización de esta etapa de relevamiento. Por último se enumeran las diferentes normas internacionales que facilitará el cumplimiento de este proceso.

1.1 Riesgos

En la actualidad, las amenazas informáticas han evolucionado de forma abrumadora. Según el informe ESET Security Report 2017 [1] de la compañía ESET Latinoamé-

rica, la infección de malware en las empresas latinoamericanas durante el año 2016 ha alcanzado el 49%, un aumento del 10% con respecto al año anterior. Esta situación demanda la inmediata adopción de medidas de seguridad en las organizaciones, puesto que la ocurrencia de delitos (así como también de accidentes) es más probable cuando se cuenta con activos informáticos vulnerables y con una escasa o nula gestión de los riesgos a los que están expuestos. Sin embargo, sólo el 52% de las empresas de América Latina ha afirmado preocuparse por este aspecto. Además, un escaso 12% afirma haber aplicado alguna solución de seguridad en dispositivos móviles, y un 17% ni siquiera cuenta con un antivirus.

Las áreas de seguridad en las organizaciones encuestadas sólo se aprecian en un 12% de las mismas, lo que explica la creciente necesidad de aplicar controles para reducir o mitigar los riesgos de amenazas que impidan el normal funcionamiento del negocio.

Por lo tanto, podemos afirmar que la gestión de los riesgos ha cobrado una gran relevancia para las organizaciones, hasta el punto de constituir una herramienta fundamental para su desarrollo.

El presente documento tiene como objeto abordar la Gestión de Riesgos desarrollando el relevamiento de los activos informáticos dentro de una organización y su clasificación, analizando las posibles vulnerabilidades (riesgos) que éstos puedan sufrir, así como las posibles alternativas para mitigar tales riesgos.

La información revelada en esta documentación, además, le facilitará a la organización llevar a cabo el cumplimiento de los estándares ISO/IEC 27000, ISO/IEC 31000 e ISO/IEC 22301 para la Seguridad de la Información, Gestión del Riesgo y Gestión de Continuidad del Negocio respectivamente.

1.2 Activos Informáticos

Los activos informáticos –o activos TI- son aquellos recursos (hardware/software) que tiene o explota una organización para el desarrollo de sus actividades de negocio, y que hacen uso de la información concerniente a dicha organización, a través de la tecnología. La información, al estar contenida en estos recursos, es por tanto otro activo informático, de igual (o incluso mayor) importancia que los otros recursos.

Además de estos recursos tecnológicos están los humanos, tales como proveedores y terceros relacionados con los activos TI de la organización.

Por lo tanto, los activos informáticos que se pueden encontrar en una organización recaen en la siguiente **clasificación**:

- Hardware: Servidores, computadoras personales, smartphones, tablets, impresoras, monitores, etc.
- Software: Aplicaciones del negocio, sistemas de gestión empresarial (ERP), sistemas operativos, sistemas de oficina, etc.

- Comunicación: Redes de comunicación, enlaces de fibra óptica, cableado, routers, módem, centrales telefónicas, etc.
- Datos: Bases de datos, Información del personal, claves, manuales de usuario, material de capacitación, documentación de sistemas, etc.
- Proveedores: De servicios y tecnología.
- Terceros (servicios): Aquellos que no son miembros de la organización pero que de alguna manera son responsables o están relacionados con la información de la organización o con los servicios que ésta brinda. Los servicios que estos terceros brindan también son considerados como activos TI.
- Proyectos de TI: como aporte importante a la ciberseguridad en la organización el hecho de calificar a los proyectos de TI como activos informáticos, y analizarlos como tales, teniendo en cuenta los posibles riesgos a los que tales proyectos puedan estar expuestos, como por ejemplo, una mala especificación contractual.
- Información de la organización no contenida en Software: se debe hacer un análisis para identificar aquella información que no está contenida en aplicaciones de la organización pero que es parte de la información que la organización posee para ser tenida en cuenta en este esquema.

1.3 ¿Por qué gestionar los riesgos en los activos TI?

De acuerdo a ISO (International Organization for Standarization) el riesgo es definido en la Guía ISO/IEC 73 como “la combinación de la probabilidad de un suceso y sus consecuencias”. [2]

Por lo tanto, el hecho de conocer los riesgos que puedan sufrir estos activos y las posibles formas de mitigarlos, constituye una herramienta imprescindible para cualquier organización, puesto que le permite tener un mayor control de la información que ésta maneja, y la certeza de que tal información está protegida. Podemos afirmar entonces que esta actividad de relevamiento y análisis ayuda a un mejor funcionamiento de la organización, reduciendo el costo que implica la detección de un fallo de seguridad sin estar preparados o informados para tal eventualidad.

2 Gestión de Riesgos

Es importante reconocer que la información está sujeta a riesgos o amenazas que afectan su integridad, disponibilidad y confidencialidad.

La información es íntegra cuando se mantiene exacta y completa, es confidencial porque no se pone a disposición ni se revela a individuos, entidades o procesos no

autorizados; y debe estar disponible para su acceso y utilización por parte de aquellas personas o entidades autorizadas a ello cuando éstas lo requieran.

El no cumplimiento de estas propiedades afecta de forma negativa a los procesos y objetivos de la organización, por lo que los riesgos de que se dé esta situación son inaceptables. Para esto, se diseñan e implementan controles creados para reducir, contrarrestar o anular los riesgos o amenazas.

Una correcta administración de riesgos de información y de los recursos que se utilizan para procesarla, debe definir los activos involucrados y los riesgos a los que éstos se ven expuestos. Según el tipo de control que se establezca para tratar estos riesgos, los mismos se verán afectados en forma diferente.

2.1 El proceso de gestión de riesgos [3] [4]

Se definen las siguientes etapas para la gestión de riesgos:

- Planificación: cómo realizar las actividades de gestión de los riesgos para un proyecto
- Identificación: determinar los riesgos que pueden afectar el proyecto y se documentan sus características
- Análisis cualitativo: evaluar los riesgos en términos de impacto y probabilidad de ocurrencia y priorizar
- Análisis cuantitativo: analizar en forma numérica el impacto de los riesgos en los objetivos de la organización. Asignar un valor numérico al análisis de los riesgos
- Respuesta a los riesgos: desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas identificadas anteriormente
- Monitoreo y control: llevar a cabo planes y acciones para el seguimiento de los riesgos identificados y las acciones de respuesta a esos riesgos. Identificar nuevos riesgos y evaluar la efectividad del proceso

Este proceso se repite de forma continua, como se muestra en la imagen a continuación y cumpliendo con los estándares de calidad de retroalimentación del proceso:

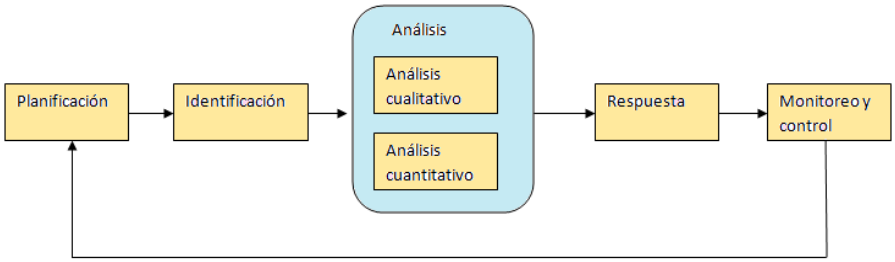

Figura 1. Proceso de gestión de riesgos.

El modelo de relevamiento que se describe en este documento consta de las siguientes características a evaluar para cada activo identificado:

- Tipo: Si es un activo de software, hardware, datos, etc. (de acuerdo con **clasificación**).
- Ubicación: donde se encuentra tal activo.
- Propietario: A quién pertenece el activo.
- Responsable: Quién (o quienes) figura como responsable de la gestión del activo, en este caso el Propietario deberá reconocer que para temas administrativos el Responsable es la persona que se encarga de la gestión diaria del activo.
- Versión: En qué versión se encuentra actualmente el activo.
- Descripción: Breve descripción del activo.
- Estado: Si está en uso o no.
- Relación con otros activos: Si el activo funciona de forma aislada (inusual) o con qué otros activos se relaciona. Esto es especialmente importante para detectar la existencia de otros activos y su relación.
- Tecnología: Con que herramientas tecnológicas fue hecho o se relaciona el activo.
- Responsable del área de sistemas: Quién se responsabiliza del área de Sistemas.
- Confidencialidad: Qué tan confidencial es el activo. De acuerdo a una definición básica de activos de la organización como: Información Pública, Privada y Confidencial.
- Sensibilidad: El grado de sensibilidad del recurso según la información que maneja.

Luego de haber identificado los recursos informáticos de los que dispone la organización, se deben identificar y analizar los riesgos asociados a cada recurso.

Los riesgos que pueden ocurrir dependen de los activos específicos por lo que no es posible establecer todos los riesgos de seguridad de forma esquemática y completa

sin haber realizado un relevamiento detallado. Una vez identificados los posibles riesgos de los activos, se evalúa la probabilidad de ocurrencia y el impacto de estos riesgos en caso de ocurrir.

Los pasos para evaluar los riesgos son los siguientes:

a- Analizar la probabilidad de ocurrencia del riesgo, cuantificándola con valores entre 0 y 1 (siendo 1 si es seguro que suceda y 0 si es imposible que ocurra).

b- A partir de la probabilidad de ocurrencia, se evalúa el impacto del riesgo, en tres aspectos:

b.1 Sobre el tiempo: Cuánto retrasa al funcionamiento de la organización la ocurrencia del riesgo.

b.2 Sobre el desempeño: Cuánto impide el funcionamiento del activo la situación de riesgo, en qué porcentaje inhabilita sus funciones.

b.3 Sobre el costo: Si existen costos que genere la ocurrencia de la amenaza sobre el activo.

c- Sumar los valores probabilísticos obtenidos en los pasos anteriores y se promedian. De esta forma, se conocerán los riesgos mayores y a qué activos afectan.

d- Elaborar un gráfico o tabla clasificando los activos según la criticidad de éstos, siendo los más críticos aquellos recursos cuyos riesgos tienen una alta probabilidad de ocurrencia y un alto impacto en el costo, tiempo, o funcionalidad de estos recursos.

3 Esquema de gestión

Se utilizará este esquema para la actividad de gestión de riesgos de 4 fases:

- Analizar los riesgos
- Diseñar la gestión de los riesgos
- Implementar la gestión de los riesgos
- Diseñar el monitoreo del riesgo

El objetivo de este documento es describir las fases 1 y 2 de este esquema, ya que mediante las mismas, se realizará el primer relevamiento de los activos con una visión de Gestión de Riesgos, permitiendo luego describir las siguientes fases.

3.1 Análisis de los riesgos

En esta primera etapa se trabaja para conocer en profundidad cuales son los todos los procesos de la organización y se analizan los riesgos que amenazan a esos procesos. Tal análisis conduce a priorizar y agrupar los riesgos a gestionar.

Las siguientes actividades están orientadas a cumplir con esta fase:

3.1.1 Definir el alcance

Evaluar la confianza en los Sistemas de Información en el contexto de los procesos. Revisar los procesos para considerar si se deben incluir otros procesos en vista de los problemas/riesgos específicos de los sistemas informáticos.

3.1.2 Entender los objetivos de los procesos e indicadores (de existir indicadores)

Realizar un análisis de los indicadores específicos del sistema para entender la performance del proceso e identificar observaciones para mejorar la performance. En caso de no existir indicadores, se debería especificar algún indicador que especifique mínimamente el funcionamiento del sistema o proceso.

3.1.3 Entender el flujo del proceso

Cuando existan procesos complejos o altamente dependientes de la Tecnologías de la Información se debería preparar un diagrama de flujo detallando los elementos de los procesos definidos, los sistemas subyacentes y los flujos de información.

3.1.4 Identificar y categorizar los riesgos

Identificar los riesgos asociados a las Tecnologías de la Información y las Comunicaciones de los procesos. En caso de existir revisar documentación de procesos para identificar riesgos adicionales.

3.1.6 Identificar y categorizar las respuestas a los riesgos

Identificar y documentar las actividades de control llevadas a cabo para cada proceso documentado. En esta etapa se deberá detectar la no existencia de controles dejando para otro proceso el desarrollo de controles adecuados. En caso de existir controles se debe documentar el control, registro formal, frecuencia y responsable.

3.1.7 Evaluar riesgos graves

Revisar la evaluación de los riesgos en relación con los procesos más significativos.

- Considerar la efectividad de las respuestas a los riesgos
- Revisar la responsabilidad y existencia de problemas en el pasado enfocandose en la existencia de problemas ya detectados y como fueron solucionados.
- Evaluar el riesgo residual o la existencia de otros controles que pudieran reducir el riesgo

- Identificar oportunidades de mejora de los procesos e informar recomendaciones para la gestión
- Preparar recomendaciones para la gestión

Se presenta también una guía de actividades a seguir, con la finalidad de ayudar a lograr el cumplimiento de esta primera fase.

- 1. Definir el alcance
- 1.1. Identificar procesos clave:
    - Obtener organigramas de la organización.
    - Planificar entrevistas con responsables de las distintas áreas de la organización.
    - Ítems de entrevista: Objetivos del área. Cuáles son las actividades que realiza la misma. Qué áreas participan de cada actividad.
- 1.2. Identificar sistemas TI en los procesos: Identificar herramientas de hardware y software utilizadas en los procesos relevados.
- 2. Entender objetivos de procesos e indicadores
- 2.1. Identificar y analizar indicadores en los sistemas de TI:
    - Relevar indicadores claves de los sistemas de TI.
    - Existencia de Acuerdo de nivel de servicio / disponibilidad
    - Tiempo de actividad
    - Porcentaje de parches de seguridad
    - Tiempo máximo de retraso soportado
    - Número de incidentes ocurridos
    - Categorización de indicadores (de existir) Funcionales / Indicadores de Servicio / Satisfacción del Usuario
- 3. Entender el flujo del proceso

Elaborar cursogramas para los procesos.

- 4. Identificar y categorizar los riesgos

Elaborar un catálogo estandarizado de riesgos (Metodología Magerit). [5]

Categorías:

- Desastres naturales.
- De origen industrial.

- Errores y fallos no intencionados.
- Ataques intencionados.
- 5. Identificar y categorizar la respuesta a los riesgos
    - Asociar los riesgos a los activos relevados
    - Elaborar una tabla con los posibles riesgos que afectan a cada activo
    - Asignar una probabilidad de ocurrencia de los riesgos de cada activo
    - Elaborar una tabla con la escala a utilizar para la medición según la frecuencia de aparición de la amenaza o la certeza de que puede ocurrir el evento no deseado
    - Evaluar el impacto de los riesgos
    - Elaborar una tabla con la escala a utilizar para la medición del impacto del evento no deseado.

Ítems a considerar :

- Tiempo de recuperación.
- Impedimento en el desempeño del proceso
- Costo asociado o afectación de la imagen de la institución
- Calcular el valor de los riesgos
- Generar una tabla con el valor probabilístico de los riesgos para cada activo, a partir de la fórmula: riesgo = probabilidad * impacto.
- Visualizar los riesgos

En este momento del desarrollo del esquema ya es posible realizar un gráfico con los riesgos ordenados de mayor a menor, incluso para que el impacto visual sea más significativo se asignarán colores según el tipo de riesgo.

Tipos de riesgo: Crítico - Moderado - Mínimo

- 7. Evaluar riesgos críticos

Se deba realizar una buena comunicación con los responsables y dueños de los sistemas de información acerca de la existencia de riesgos críticos. En estos casos se deberían tomar decisiones y cursos de acción para su gestión adecuada.

3.2 Diseño del tratamiento de los riesgos

Las actividades que se pueden implementar en esta segunda etapa son:

- Identificar riesgos para la optimización
- Identificar temas comunes y relacionados con TI dentro de los riesgos.
- Identificar cómo se van a gestionar los riesgos
- Priorizar la gestión de los riesgos teniendo en cuenta la planificación del trabajo y la existencia de recursos dedicados a esta gestión
- Preparar casos de tratamientos de los riesgos enfocados en TI.
- Definir escenarios probables.
- Informar y comunicar formalmente los resultados y recomendaciones

Guía de actividades. Al igual que para la fase anterior, se presenta a continuación un esquema de actividades que se podrían realizar para cumplir con las tareas especificadas en esta segunda etapa.

- 1. Identificar riesgos candidatos para la optimización
- 1.1 Seleccionar los activos con mayor riesgo: Elaborar un listado con los activos TI con probabilidad de riesgos críticos.
- 1.2 Identificar escenarios de riesgo en activos: Listar situaciones de riesgo que se supone podría ocurrir, a partir de los riesgos asociados a cada activo.
- 2. Identificar tratamiento de los riesgos
- 2.1 Establecer las opciones de tratamiento del riesgo adecuadas: Identificar las posibles opciones para tratar el riesgo para cada activo.

Opciones:

  - Aceptar el riesgo de acuerdo al apetito de riesgo de la organización.
  - Aplicar los controles apropiados.
  - Evitar el riesgo.
  - Transferir el riesgo asociado a otras organizaciones.

- 3. Priorizar los tratamientos de los riesgos: Obtener evaluación de los tratamientos de los riesgos por parte del cliente:
  - Ítems de evaluación:
  - Relación costo-beneficio.
  - Recursos disponibles.
  - Recursos necesarios.
  - Posibilidad y magnitud de riesgo residual.

Listar los tratamientos ordenados por prioridad

- 4. Informar recomendaciones para la administración
- 4.1 Desarrollar casos de negocio para los tratamientos de los riesgos: Describir los beneficios y recursos requeridos para implementar los tratamientos de riesgos.
- 4.2 Resumir las futuras mejoras en el rendimiento: Describir las observaciones de mejora del rendimiento de la organización que se producirán al aplicar los tratamientos diseñados.

5. Cumplimiento de estándares

- ISO/IEC 27001:2005-Requisitos para un SGSI [6]

La norma ISO/IEC 27001:2005 plantea los requisitos para elaborar un Sistema de Gestión de Seguridad de la Información (SGSI).

Un SGSI basado en la norma ISO 27001 se fundamenta principalmente en la identificación y análisis de las principales amenazas para, a partir de este punto de partida, poder establecer una evaluación y planificación de dichos riesgos. Es decir, se puede asumir que la metodología descrita en este documento contribuye a la elaboración de un SGSI.

- ISO/IEC 22301:2012- Gestión de la Continuidad del Negocio [7]

Esta norma se centra en diversos aspectos de la organización que van a permitir su sustentabilidad, utilizando para ello ciertos elementos y controles que van a evitar las consecuencias de las distintas amenazas, así como también encontrar las causas que motivan el problema.

Un aspecto muy importante, que no tiene en cuenta la ISO 27001, son los tiempos de recuperación, una cuestión crucial para poder evaluar si el trabajo de gestión de riesgos es el adecuado para poder reanudar la actividad en unos niveles aceptables para la organización, una vez ha ocurrido el incidente.

- ISO/IEC 31000:2009-Gestión del Riesgo [8]

Esta norma tiene el objetivo de ayudar a generar un enfoque para mejorar la gestión de riesgos, de manera sistemática y brindar posibilidades para que exista una gestión que permita conseguir los objetivos que persigue la organización.

Para lograr tal fin, establece todos los procesos y principios que se deben seguir para realizar gestión del riesgo, en la que recomienda a las empresas el desarrollo, la implantación y el mejoramiento continuo como un importante componente de los sistemas de gestión.

5. Conclusión

La información, su acceso autorizado y el uso que se hace de ella son vitales para el desarrollo y buen desempeño de las organizaciones, lo que explica la relevancia que han tomado los activos informáticos en los últimos años. No obstante, todos los activos de una organización están expuestos a riesgos que, de concretarse, pueden afectar negativamente el negocio y los objetivos que dicha organización persigue, interrumpiendo además la continuidad del servicio. Es menos recomendable afrontar un evento no deseado una vez ocurrido, que implementar los controles necesarios para poder evitarlo o reducirlo. Para reducir o mitigar estos riesgos, se deben implantar controles utilizando una metodología que gestione las potenciales amenazas.

Esta metodología de gestión de riesgos nos ayudará a identificar los activos, sus vulnerabilidades/amenazas que los afectan, calcular el nivel de los riesgos a los que están expuestos, y elaborar controles para mitigarlos o reducirlos en caso de que superen el nivel aceptable para la organización.

Una vez clasificados los riesgos a través de su criticidad, será más claro determinar cuáles son los riesgos que se van a gestionar primero. Este trabajo intenta desarrollar en forma descriptiva las primeras fases de este proceso en donde se podrán listar los activos de información y su tratamiento desde un enfoque de Administración de Riesgos, luego de realizada esta tarea se deberá definir el sistema de gestión contando con esta información para su mejor desempeño.

Las organizaciones deberían adoptar un proceso de gestión de Riegos ya que todas dependen en mayor o menor grado de los activos informáticos para desarrollar sus actividades. Si bien este esquema de Administración de Riesgos y relevamiento de activos informáticos se desarrolló para ser implementado en la Universidad Nacional de Río Negro, se destaca la facilidad con la que este proceso se puede reproducir en otras organizaciones.

Referencias

1. ESET. (2017). ESET Security Report Latinoamérica 2017. Buenos Aires, Argentina. Recuperado de https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf [Consultado 24 Feb., 2018]
2. ISO/IEC. (2009). ISO/IEC 73:2009- Gestión del Riesgo- Terminología- Líneas directrices para su uso en las normas. Suiza: ISO/IEC.
3. Instituto Nacional de Ciberseguridad. (2015). Gestión de riesgos: Una guía de aproximación para el empresario. Madrid, España: Ministerio de Industria, Energía y Turismo. Gobierno de España. Recuperado de https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf [Consultado 20 Feb., 2018]
4. Project Management Institute. (2013). Capítulo 11: Gestión de los riesgos del proyecto. En Project Management Institute. (Ed.). Guía del PMBOK, 5ta Edición. Pensilvania, Estados Unidos: Project Management Institute.

5. Consejo Superior de Administración Electrónica. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 1era ed. Madrid, España: Ministerio de Hacienda y Administraciones Públicas, Gobierno de España. Recuperado de http://administracionelectronica.gob.es/ [Consultado 15 Mar., 2018]
6. ISO/IEC. (2005). ISO/IEC 27001:2005- Tecnología de la información — Técnicas de seguridad — Sistema de Gestión de Seguridad de la Información— Requerimientos (1era ed.). Suiza: ISO/IEC.
7. ISO/IEC. (2012). ISO/IEC 22301:2012- Seguridad Societal — Gestión de Continuidad del Negocio — Requerimientos (1era ed.). ISO/IEC.
8. ISO/IEC. (2009). ISO/IEC 31000:2009- Gestión del Riesgo: Procesos y guías (1era edición). Suiza: ISO/IEC.