REGLA DE NEGOCIO 2021-RN-160

ENERO 15 DE 2021

Proceso Seguridad Digital y Continuidad de los Servicios de Tecnología

CONSIDERACIONES

En el marco de la Política de Seguridad de la Información y Ciberseguridad para el grupo EPM, aprobada en el Acta 1619 de Junta Directiva del 13 de diciembre de 2016, desplegada mediante el Lineamiento 2017-LINGG-20 - Sistema de Gestión de Seguridad de la Información y Ciberseguridad, es necesario definir la regla de negocio del proceso Seguridad Digital y Continuidad de los servicios de Tecnología.

El proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología tiene como objetivo desarrollar, mantener y evolucionar las capacidades de seguridad de la información y ciberseguridad (gobierno, identificación, prevención, detección, protección, defensa y recuperación), con el propósito de habilitar una operación sostenible y segura en la prestación de los servicios, proteger la información crítica y la infraestructura de operación industrial del grupo EPM.

Es importante reconocer que EPM posee procesos de negocio que manejan infraestructura identificada como crítica en el "*Catálogo de infraestructura crítica cibernética de Colombia*"; tal infraestructura abarca sistemas de automatización y control industrial. EPM como operador de tales activos deben asegurarse de que están cubiertos en términos de seguridad cibernética, acorde con lo que define el gobierno.

REGLA DE NEGOCIO

1. Responsabilidad compartida

Todos los usuarios son responsables de la protección de los activos de información, los activos y ciberactivos críticos asociados a los procesos de los negocios, acatando el marco normativo interno y externo de seguridad de la información y ciberseguridad y con el acompañamiento del personal del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología se identifican las amenazas, vulnerabilidades y controles existentes que puedan afectar la seguridad de la información y la ciberseguridad, así como en la formulación del plan de tratamiento de riesgos que se derive de este análisis.

La implementación y monitoreo de los controles de seguridad de la información y ciberseguridad que se definan para los procesos o proyectos, están a cargo de los responsables de estos con la asesoría del personal especializado del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología.

2. Arquitectura de referencia de ciberseguridad

Los responsables del desarrollo o cambio en los servicios de tecnología deben considerar la arquitectura de referencia de ciberseguridad definida por el proceso de seguridad digital y continuidad de los servicios de tecnología.

3. Perímetro de Seguridad Electrónica

Todos los servidores que tienen a cargo activos y ciberactivos críticos, deben hacer la gestión para que estos residan en un perímetro de seguridad electrónica debidamente identificado, documentado; y que los controles de seguridad (contramedidas), estén definidos e implementados a partir del análisis de riesgos.

4. identificación y documentación de los sistemas bajo consideración

Los responsables de los sistemas ya sean de control industrial o informáticos, deben garantizar que estos sean identificados y listados plenamente con sus componentes, sus interacciones, sus flujos de comunicación y su respectiva documentación.

5. Análisis de amenazas, vulnerabilidades y controles de seguridad digital

Los procesos y proyectos que manejen tecnología de información y operación deben aplicar la metodología de análisis de amenazas, vulnerabilidades y controles de seguridad digital en los activos y ciberactivos a su cargo, para identificar el nivel de riesgo y las oportunidades de mejora. Este documento se utiliza para comunicar a las partes interesadas, así como a los equipos de trabajo de desarrollo e implementación que realizan el diseño detallado, instalación, pruebas en fábrica (FAT), puesta en marcha y el comisionamiento, acerca de los requisitos de seguridad cibernética que se deben cumplir.

6. Declaración de Aplicabilidad de Controles de Seguridad

Todos los procesos y proyectos deben identificar e implementar los controles de seguridad de la información y ciberseguridad (contramedidas) para mitigar el riesgo. Estos controles se deben documentar en la “declaración de aplicabilidad de controles de seguridad” (contramedidas), de acuerdo con marcos de referencia, buenas prácticas y la regulación aplicable. El personal del proceso Seguridad Digital y Continuidad de los Servicios de Tecnología orienta en este propósito.

La declaración de aplicabilidad de controles de seguridad (contramedidas) deben tener en cuenta las condiciones de cada proceso tanto corporativo como de Operación

7. Planes de tratamiento de riesgos de seguridad digital

La formulación e implementación de los planes de tratamiento de riesgos relacionados con la seguridad digital para los procesos y proyectos están a cargo de los responsables de estos, el personal del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología apoya la definición y la implementación del plan de tratamiento de riesgos de seguridad digital.

8. Gestión de vulnerabilidades en los activos y ciberactivos

Los servidores del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología lideran la identificación de vulnerabilidades y participan en la definición de las medidas de protección de los activos y ciberactivos. En los procesos y proyectos se deben gestionar e implementar las medidas de protección de los activos y ciberactivos a su cargo.

En las tecnologías de operación las medidas de protección en los activos y ciberactivos se implementan siempre y cuando las pruebas y el análisis de impacto del cambio, indiquen que la medida es técnicamente viable y no afecta el correcto funcionamiento de la operación.

9. Requisitos regulatorios relacionados con seguridad de la información y ciberseguridad

Todos los requisitos regulatorios de negocio relacionados con seguridad de la información y ciberseguridad, deben ser analizados conjuntamente, antes de su implementación, con el personal del proceso de seguridad digital y continuidad de los servicios de tecnología, a fin de identificar la aplicabilidad y el uso de controles de seguridad de la información y ciberseguridad (contramedidas), realizar la validación de controles y así mismo, conjuntamente formular el plan de mejora que se debe implementar en el proceso al que le aplica la regulación.

10. Adquisición de nueva tecnología

La adquisición de nuevas tecnologías debe cumplir con las especificaciones de seguridad de las aplicaciones y la infraestructura tecnológica que la soporta, exigidas en la arquitectura de ciberseguridad de referencia, salvo los casos excepcionales que puedan ser indicados por el proceso que adquiere la tecnología.

11. Principio de mínimo privilegio

En los procesos y proyectos, el responsable del control de acceso a los activos y ciberactivos debe partir de la premisa de otorgar a los usuarios los privilegios estrictamente necesarios para el desempeño de sus funciones o el cumplimiento de su relación contractual. Los privilegios adicionales que se otorguen deben estar debidamente sustentados, aprobados y documentados por el responsable del proceso o proyecto al que pertenece el activo y el ciberactivo.

12. Segregación de funciones

La aplicación del instructivo para la implementación del control de seguridad de segregación de funciones en procesos y proyectos está a cargo de los responsables de estos. La matriz de incompatibilidades resultante debe ser parte de la documentación del proceso o proyecto y estar disponible al momento de configurar los privilegios de acceso en los activos y ciberactivos. Así mismo, el catálogo de riesgos que se deriva de este análisis es

información clasificada y reservada de acceso restringido, y es base para la implementación de los procedimientos de monitoreo del proceso.

13. Gestión de acceso de usuarios

Todos los usuarios deben ser identificados individualmente a través del modelo de identidad que utiliza la organización, permitiendo la trazabilidad de sus operaciones e implementando medidas para evitar el no repudio de las mismas.
Los privilegios de acceso solo deben ser otorgados cuando se haya surtido el trámite formal de autorización en el que se validen los requisitos que deben cumplir los usuarios.

Los privilegios de acceso a los activos y ciberactivos deben actualizarse cada vez que ocurra un cambio en las funciones u obligaciones contractuales del usuario. Se deben deshabilitar o retirar inmediatamente los privilegios de acceso a los activos y ciberactivos a los usuarios cuando finalice su contrato o vinculo jurídico con la organización.

El responsable del activo y ciberactivo, debe garantizar el monitoreo periódico de los privilegios de acceso de los usuarios en donde sea técnicamente factible, de manera que se evite el acceso a personal no autorizado.

14. Evaluación de personal con acceso a activos y ciberactivos críticos

Los responsables de los activos y ciberactivos críticos deben asegurar que todo el personal con acceso lógico autorizado o acceso físico no escoltado a ciberactivos críticos, tenga una evaluación de riesgos del personal, que incluya confirmar la identidad de las personas y un estudio de seguridad con validación de la Unidad de Cumplimiento de EPM, y una revisión periódica acorde con la normativa.

15. Uso de información secreta para la autenticación

La cuenta de usuario y la contraseña de acceso a la red corporativa es personal e intransferible. Es responsabilidad de los usuarios de la tecnología mantener la confidencialidad de la información secreta para la autenticación.

16. Uso de cuentas técnicas de sistemas

Las cuentas técnicas solo deben ser utilizadas por los sistemas para ejecutar procesos o servicios automáticos, comunicación entre sistemas o equipos. Estas cuentas no deben ser usadas por ningún usuario para otros fines y la contraseña so
lo debe ser conocida por personal técnico responsable de la administración y configuración de la infraestructura, en razón de su función. Estas cuentas deben estar debidamente documentadas para efectos de trazabilidad y control. La creación de este tipo de cuentas debe ser autorizada por el responsable de la infraestructura, quien gestiona el cambio de contraseña cuando el personal interno o externo que conoce la cuenta técnica cambie de función o se retire de la organización.

17. Cuentas de usuario compartidas

No se permiten cuentas de red compartidas, las cuentas de red son asignadas exclusivamente a usuarios individuales. Las cuentas de usuario de sistemas independientes tampoco pueden ser compartidas y solo se permiten cuando el sistema en cuestión no admita usuarios individuales, en estos casos el responsable del proceso o proyecto debe garantizar que estas cuentas estén debidamente documentadas, de tal forma que se identifiquen las personas que tienen acceso y se garantice la trazabilidad de las acciones ejecutadas.

18. Cuentas predeterminadas

El responsable de la infraestructura tecnológica debe garantizar que las cuentas predeterminadas y otras cuentas genéricas proporcionadas por un proveedor sean eliminadas, renombradas o deshabilitadas antes del uso en producción. Si esto no es posible técnicamente, las contraseñas de las cuentas predeterminadas proporcionadas por el proveedor deben cambiarse. Así mismo, debe documentar las cuentas predeterminadas y otras cuentas genéricas que permanezcan habilitadas.

19. Procedimiento de autenticación

Todos los sistemas de información deben autenticarse acorde con lo definido en el modelo de identidad organizacional. Las excepciones deben estar debidamente sustentadas por los responsables de los procesos y proyectos y estarán relacionadas con características técnicas u operativas principalmente para los sistemas de control industrial. Esta sustentación es analizada por el personal del proceso de Seguridad Digital y Continuidad de los servicios de tecnología.

Para los procesos que se consideren críticos y de alto riesgo, los usuarios que inicien sesión en la estación de trabajo (dominio de red), deben hacerlo con algún mecanismo multifactor. Para los demás procesos de la organización los mecanismos multifactor deben ser utilizados siempre y cuando se cuente con los recursos para ello. Para el caso de los sistemas de control industrial y automatización, los mecanismos de autenticación se hacen teniendo en cuenta la viabilidad técnica y operacional.

Toda la infraestructura de servidores TI de la organización debe estar protegida con factor múltiple de autenticación; la infraestructura de servidores de TO debe usar el factor múltiple de autenticación cuando sea técnica y operacionalmente factible.

Todas las aplicaciones donde se ejecuten transacciones sensibles (transacción de negocios que tiene el potencial de afectar los estados financieros de una compañía, es decir, sensible al riesgo de fraude) deben utilizar doble factor de autenticación para el ingreso a la aplicación o al momento de iniciar la transacción.

20. Restricciones de acceso a la información y funcionalidad de los sistemas de información

Los privilegios de acceso sobre la infraestructura de tecnología de información y operación y los recursos compartidos en los servidores en los que está instalada la infraestructura y las funcionalidades que soportan los sistemas de información deben ser identificados, documentados y monitoreados por el responsable de la respectiva infraestructura y estar ajustados al principio de mínimo privilegio. No se deben otorgar permisos a los empleados o contratistas para modificar datos en forma directa en las bases de datos, por lo que, si se incumple, podría dar lugar a posibles procesos disciplinarios, las excepciones que se presenten deben corresponder a situaciones de emergencia y por tiempo limitado, estar debidamente sustentadas, ser trazables y autorizadas por el responsable del activo, ciber activo o información.

21. Información de activos críticos y ciberactivos

Los responsables de la información asociada a los activos críticos y ciberactivos críticos la deben identificar, clasificar, etiquetar y proteger con los controles requeridos para la misma.

22. Uso de programas de software utilitario privilegiado

Los responsables de instalar y administrar software deben restringir, controlar y monitorear el uso de programas de software utilitario. La utilización de este tipo de software estará acorde con las funciones y los listados de software permitido en la organización.

23. Gestión de derechos de acceso privilegiado

Los derechos de acceso privilegiado deben ser gestionados por los responsables de los activos y ciberactivos, garantizando que estén documentados y con la debida trazabilidad, de tal manera que sea siempre identificable quién, y durante que periodo tuvo el privilegio. Así mismo, definir actividades de monitoreo periódico de las transacciones realizadas por los usuarios con acceso privilegiado.

24. Controles de acceso lógico y físico

Los responsables de los activos y ciberactivos deben gestionar la implementación de los controles de acceso lógico y físico que definan los procesos de Seguridad Digital y Continuidad de los Servicios de Tecnología y el proceso de seguridad de infraestructura (seguridad física).

25. Acceso de contratistas a información organizacional

Los interventores de contrato deben asegurar que el acceso que tenga el contratista a la información organizacional cumpla con el principio del mínimo privilegio, adelantar las actividades necesarias para una adecuada gestión de privilegios relacionados con el contratista, así como el cumplimiento de los requisitos del manejo adecuado y seguro de la información que este utilice.

26. Protección de los datos personales

Los responsables del diseño, arquitectura y configuración predeterminada de las infraestructuras y software que soportan los activos de información, deben considerar los

requisitos de privacidad de los datos personales en la solución propuesta, para lo cual se deben apoyar en el instructivo de privacidad.

27. Protección de la información clasificada y reservada

El responsable de la información contenida en el Índice de la Información Clasificada y Reservada debe garantizar que el personal que tenga acceso a esta información, firme los acuerdos de confidencialidad sobre la misma, así como de la implementación de mecanismos de seguridad que eviten la fuga de esta información. Los responsables del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología orientarán acerca de las medidas técnicas y de seguridad a implementar sobre la información clasificada y reservada, para evitar su divulgación no autorizada.

28. Pruebas de aceptación del sistema

El personal que tenga a su cargo las pruebas de aceptación del sistema debe incluir como parte de la validación, los requisitos de seguridad y la adherencia a prácticas de desarrollo seguro.

29. Pruebas de aceptación de Tecnologías de Operación (TO)

Las pruebas de aceptación en Tecnologías de Operación deben cumplir los requisitos de seguridad cibernética especificados tanto para pruebas en fábrica como pruebas en sitio y a su vez mantener la cadena de custodia hasta la entrega a EPM.

Es importante que en dichas pruebas participe el personal del proceso Seguridad Digital y Continuidad de los Servicios de Tecnología, para realizar y documentar el análisis de riesgo y vulnerabilidades e identificar las secciones débiles con el fin de crear un plan de contramedidas.

Las pruebas de los controles de seguridad cibernética (contramedidas) deben realizarse como parte de la fase de puesta en servicio. Estas deben asegurar la funcionalidad correcta del control industrial y su relación armoniosa con tales contramedidas.

30. Desarrollo de software contratado externamente

Para el desarrollo de software contratado externamente, se debe verificar la existencia de las certificaciones de las pruebas para garantizar el cumplimiento de los requisitos de seguridad y las pruebas de vulnerabilidad realizadas por el contratista.

31. Transferencia de información

La Gerencia de Tecnología e Información debe definir los mecanismos de transferencia de información entre sistemas e implementar los controles de seguridad (contramedidas) que eviten la interceptación, copiado, modificación y borrado de información. Cuando la información que se transmita sea sensible (transacciones sensibles, datos personales, información clasificada y reservada), se debe implementar controles adicionales como cifrado de información, autenticidad de contenido, prueba de envío, prueba de recepción, no rechazo de origen y acuerdos de confidencialidad, u otros controles validados con el personal del proceso de seguridad digital y continuidad de los servicios tecnología.

La Gerencia de Tecnología e Información debe definir e implementar procedimientos para la detección de software malicioso y protección contra este, durante la transferencia de información.
El cifrado de información en tecnología de operación debe considerar la viabilidad técnica y el funcionamiento correcto del sistema. Las comunicaciones entre centros de control deben estar cifradas usando los protocolos pertinentes para los fines de la operación.

32. Ambientes de desarrollo, pruebas y producción

Los responsables de la infraestructura tecnológica deben implementar los ambientes de desarrollo, pruebas y producción claramente identificables, garantizando la implementación de un sistema de prevención de pérdida de información. Así mismo, se debe validar que estos ambientes cuenten con actualización del sistema operativo vigente y antivirus, donde sea técnica y operacionalmente posible, de lo contrario deben implementar controles de seguridad compensatorios. Los cambios realizados a los ambientes deben ser trazables y disponer de procedimientos de restauración de ambientes.

33. Control de los datos de prueba

Para la información que contenga datos personales (o considerada de protección especial por la ley), o información considerada sensible, clasificada o reservada, se debe restringir la extracción de información del ambiente de producción para ser utilizada en los ambientes de desarrollo y pruebas, sin medidas de protección (enmascaramiento) que eviten la divulgación de esta información.

Las excepciones que se presenten deben ser definidas por los responsables del proceso seguridad digital y Continuidad de los Servicios de Tecnología y contar con controles complementarios, estos controles incluyen procedimientos de control de acceso, autorización del responsable del activo para la copia de información operacional a ambientes de desarrollo y prueba, borrado de información una vez finalizada las pruebas y trazabilidad del manejo de la información.

34. Uso de controles criptográficos

Todos los usuarios que almacenen información empresarial que se clasifique como confidencial, deben solicitar el cifrado de su equipo a la Dirección Servicios de Infraestructura a través de la mesa de servicios.

Todos los usuarios y demás partes interesadas que manejen información en tránsito, como copias de seguridad (USB, CD, cintas) y equipos portátiles, deben garantizar la implementación de controles criptográficos para la protección de la información. En el caso de las tecnologías de operación, los controles criptográficos se implementan teniendo en cuenta su viabilidad técnica y operativa.

Los responsables del análisis, diseño e implementación de servicios de tecnología, deben garantizar que la información transmitida por los sistemas de información cuente con controles criptográficos para proteger la integridad y confidencialidad; de igual manera, garantizar que toda la información en reposo o almacenada en los sistemas de información que corresponda a información sensible (datos personales, información clasificada y

reservada), esté cifrada en los ambientes productivos y enmascarada en ambientes no productivos.

Los controles criptográficos y la gestión de llaves deben estar acorde con lo definido en el documento “modelo de controles criptográficos de la organización”.

35. Ciberseguridad en diseño e ingeniería y tecnología de operación

Los entregables de la fase de ingeniería de detalle elaborados por el CET diseño y estudios deben incorporar los controles de seguridad (contramedidas) específicos de acuerdo con los requisitos de ciberseguridad definidos.

Durante la ingeniería de detalle, debe asegurarse que el nivel de seguridad alcanzado con los controles de seguridad implementados (contramedidas) correspondan con la especificación de requisitos de ciberseguridad. El riesgo evidenciado por falta de cumplimiento debe ser mitigado con contramedidas compensatorias, debidamente sustentadas.

Los servidores de EPM responsables de los diseños de sistemas de control industrial que involucren activos y ciberactivos críticos, deben considerar la ciberseguridad como premisa, identificando los controles de seguridad (contramedidas) que deben ser implementados, para lo cual deben realizar análisis de amenazas, vulnerabilidades y controles, así mismo, tener en cuenta la arquitectura de ciberseguridad de referencia.

Los requerimientos de control de acceso físico deben ser incluidos como parte del diseño del activo (plantas de generación, subestaciones, estaciones o sistemas de control industrial, etc.), en cualquiera de los negocios de la organización.

36. Líneas base de seguridad

El responsable de los activos y ciberactivos debe asegurar que se haya definido e implementado una línea base de ciberseguridad y validar que esté debidamente documentada, actualizada con respecto a cambios y que sea concordante con el proceso. El personal del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología apoya al responsable de los activos y ciberactivos en la definición de las líneas base de seguridad.

37. Desarrollo de software seguro

Los responsables de la adquisición o desarrollo de software, sistema o servicio deben verificar que se implementen las prácticas de desarrollo seguro en el producto o servicio a entregar a la organización.

38. Control de cambios

El responsable de los activos de información y ciberactivos críticos debe validar que, como parte de la implementación de cambios en los mismos, se realice un análisis de impacto del cambio, con el fin de identificar los controles de seguridad (contramedidas) a implementar.

Cuando el análisis del impacto del cambio indique que este puede afectar la ciberseguridad, se debe realizar el *test* de vulnerabilidad previo al paso a producción.

Los parches de seguridad y las actualizaciones de los dispositivos que hacen parte de los sistemas de monitoreo y control industrial deben ser aplicados una vez se compruebe la viabilidad técnica con los fabricantes del producto, además de realizar previamente las pruebas técnicas correspondientes. Los responsables de los activos (de T.O. y T.I.) y ciberactivos deben asegurar que se cumpla con los procedimientos descritos en el esquema de administración de parches definido en la organización.

39. Gestión de la configuración

Los servidores de EPM, responsables técnicos de cada sistema de información, servicio o componente de control industrial de tecnología de operación tienen a cargo la identificación de los elementos de configuración, su documentación y la actualización de la línea base de estos elementos cuando se presenten cambios. Estos elementos incluyen el código fuente (cuando aplique), instaladores, diseños, especificaciones, planes de verificación, parches y validación, etc. Los elementos de configuración deben ser almacenados en repositorios debidamente respaldados y asegurados, que permitan el control de versiones, la gestión de acceso y la trazabilidad de los cambios, garantizando la integridad, disponibilidad y confidencialidad de los mismos. El acceso a los códigos fuente desarrollados a la medida, debe estar en concordancia con el principio de mínimo privilegio.

Los usuarios de tecnología de información no deben instalar, desinstalar o cambiar la configuración de sus componentes de *hardware* o *software* corporativo. Cualquier modificación debe ser canalizada por la Dirección Servicios de Infraestructura a través de la mesa de servicios y debidamente autorizada si es necesario.

40. Respaldo de la información

Toda información de EPM que los empleados almacenen en el equipo de cómputo asignado por EPM debe ser respaldada en los recursos dispuestos por la empresa para tal fin.

La estrategia de respaldo de información para las tecnologías de operación debe considerar aspectos como la recuperación de datos e información, acorde con lo identificado en el análisis de impacto del negocio y en los planes de recuperación. Los respaldos deben estar debidamente almacenados, documentados, probados y asegurados para garantizar la recuperación y la continuidad de los procesos.

41. Restricciones sobre la instalación de *software*

Los equipos de cómputo son entregados a los usuarios autorizados por el responsable del Proceso con el *software* necesario para el cumplimiento de sus funciones u obligaciones contractuales. Se prohíbe la instalación de *software* en los equipos de cómputo por parte de los usuarios. En caso de requerirse instalación de software adicional, se debe hacer la solicitud a la Dirección Servicios de Infraestructura a través de la mesa de servicio de TI con la justificación debidamente documentada.

Para los equipos que soporten tecnologías de operación se deben seguir los procedimientos definidos para la instalación de software para los sistemas de control industrial.

Los empleados de EPM responsables de instalar y administrar software deben restringir, controlar y monitorear el uso de programas de software utilitario. La utilización de este tipo de software debe estar acorde con las funciones y los listados de software permitidos en la organización.

42. Disposición de Medios

Antes de realizar reintegro o disposición final de los dispositivos de cómputo corporativos que contengan almacenamiento, la Dirección Servicios de Infraestructura a través de la mesa de servicios debe realizar procedimientos de borrado seguro que sean acordes a la tecnología y actualizados con los cambios tecnológicos que haya en el momento y, garantizar la trazabilidad y la ejecución del procedimiento. En los casos en que no sea posible un borrado seguro, se debe destruir el dispositivo de almacenamiento para evitar la recuperación de la información o los datos.

43. Devolución de los activos de información y ciberactivos

Tanto los equipos de cómputo, activos y ciberactivos de propiedad de EPM como los elementos relacionados con estos, deben ser devueltos a los responsables del proceso al terminar la relación laboral y/o contractual con EPM (equipos, software, información, llaves de acceso, licencias en hardware etc.). Así mismo, los jefes y los interventores de contratos deben garantizar como parte del proceso de finalización de la relación laboral y contractual el retiro de los privilegios de acceso a los activos y ciberactivos.

44. Conexiones temporales a sistemas de control y monitoreo

Las conexiones temporales a los sistemas de control deben ser aprobadas por el responsable del ciberactivo, estas deben ser aseguradas, documentadas y monitoreadas por este, para garantizar que una vez cumplan su objetivo sean deshabilitadas, acorde con los procedimientos definidos por la Unidad Soporte a las Tecnologías de la Operación.

45. Registros de auditoría

Los responsables de la información determinan las transacciones sensibles operativas sobre las cuales se habilitan los registros de auditoría en los sistemas de información, así como la habilitación del monitoreo de estos registros.

En los sistemas de control industrial los registros de auditoría se habilitan cuando sea técnica y operativamente posible.

46. Gestión de medios removibles

Los equipos de cómputo de EPM no permiten el uso de dispositivos de almacenamiento removibles. Cualquier excepción debe ser solicitada formalmente a través de un requerimiento con la debida justificación y aprobación del jefe inmediato del servidor que lo solicita.

47. Dispositivos móviles

Todos los usuarios de los dispositivos de cómputo móviles y fijos corporativos, son responsables de los mismos y deben estar a cargo de la custodia del equipo en los términos de su relación contractual o laboral con EPM. Al momento de la entrega de los equipos, se debe notificar al usuario el software autorizado. Cualquier cambio en la configuración, el software y el hardware debe ser autorizado por el jefe y realizado por la Dirección Servicios de Infraestructura a través de la mesa de servicios.

Cuando los dispositivos móviles corporativos usen tecnologías de geolocalización que por su necesidad de uso deban estar activas, esta condición se le notifica al usuario al momento de la entrega del equipo.

Si el dispositivo almacena información incluida en el índice de Información Clasificada y Reservada, el usuario responsable del equipo de cómputo debe gestionar el cifrado de la misma.

Los usuarios autorizados para usar recursos corporativos en sus dispositivos móviles personales deben aplicar el procedimiento de registro del dispositivo en la herramienta de administración de dispositivos móviles de EPM. En caso de pérdida del dispositivo, se debe notificar a la Dirección Servicios de Infraestructura a través de la mesa de servicios para realizar un borrado remoto de los datos.

Los equipos móviles que sean utilizados para el soporte y mantenimiento de sistemas de control industrial deben ser usados solo para este fin. Estos deben ser asegurados y configurados cumpliendo con las políticas de seguridad definidas por la Unidad Soporte a las Tecnología de la Operación.

48. Monitoreo de infraestructura

Los responsables de administrar la infraestructura tecnológica que soporta la tecnología de información deben monitorear continuamente las conexiones remotas de los computadores conectados a las redes en busca de actividades maliciosas para mantener y asegurar el uso de software y las funcionalidades aprobadas, prevenir y detectar intrusiones indeseadas, monitoreando la actividad generada desde estos sistemas.

Para el caso de las tecnologías de operación de los diferentes procesos industriales, los responsables de los activos y ciberactivos críticos y demás sistemas automatizados y de control industrial, deben validar que todos los perímetros de ciberseguridad y sus ciberactivos estén correctamente monitoreados y que se incluyan aspectos como el monitoreo de conexiones remotas y de acciones maliciosas dentro de sus sistemas automatizados, con el fin de minimizar los riesgos asociados a estas.

49. Revisión del cumplimiento técnico

Los responsables de todos los sistemas de información deben gestionar previo al paso a producción, la revisión del cumplimiento técnico de la ciberseguridad establecida en la etapa de planeación, para ser realizado por personal competente y autorizado del proceso Seguridad Digital y Continuidad de los Servicios de Tecnología. Las revisiones de cumplimiento técnico implican la revisión de los controles de seguridad en el hardware y

software y que se hayan implementado correctamente y hacer las pruebas de valoración de vulnerabilidades sobre los elementos que componen el sistema.

50. Herramientas de prevención de software Malicioso (malware)

Se instala software de detección y eliminación de código malicioso a los distintos ciberactivos de la organización revisando la información en reposo y en movimiento. Para aquellos ciberactivos de Tecnologías de Operación que no soporten por restricciones operacionales los chequeos de información en reposo, el servidor responsable del proceso debe implementar controles suplementarios que mitiguen el riesgo existente.

Se debe garantizar que todos los ciberactivos que tengan la capacidad técnica de instalarle antivirus, sean protegidos con este mecanismo. Las excepciones de instalación de antivirus están relacionadas con la viabilidad técnica y las recomendaciones del fabricante contenidas en el manual de instalación del producto, así como considerar el buen funcionamiento del sistema, para las tecnologías de operación.

Los usuarios autorizados para estar conectados a la red corporativa que sospechen de una infección por código malicioso en sus equipos de cómputo deben apagar el equipo involucrado, desconectarlo de red y notificar a la Dirección Servicios de Infraestructura a través de la mesa de servicios para que ejecute los procedimientos establecidos.

Para el caso de los sistemas de control industrial, el producto de protección contra malware (programa malicioso) debe configurarse de acuerdo con las pautas del proveedor contenidas en el manual de instalación del producto y las condiciones del proceso industrial para garantizar que no interfiera con el funcionamiento del sistema de control industrial.

51. Software autorizado

Está prohibido a los servidores, la transferencia de software (subir y bajar) desde y hacia sistemas que se encuentren por fuera de EPM. La instalación de cualquier software debe gestionarse por la Dirección Servicios de Infraestructura a través de la mesa de servicios, quien valida el licenciamiento y la confiabilidad del sitio de descarga del software.

La Dirección Servicios de Infraestructura a través de la mesa de servicios elimina del hardware los programas de ordenador o software instalados que no hayan sido autorizados, en atención a los riesgos de ataques a la información empresarial, así como a los riesgos que puedan existir derivados de la afectación a la propiedad intelectual.

Para los equipos que soportan tecnologías de operación se debe realizar la gestión de inventario de software autorizado y sustentar la utilización de software que no esté incluido en este inventario.

52. Cooperación y colaboración

Para mantener actualizado el estado del arte de la estrategia de gestión de incidentes de seguridad digital y tener un apoyo conjunto en la atención y respuesta a eventos e

incidentes, el personal del Proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología deben establecer mecanismos de cooperación y colaboración mediante los respectivos contratos con diferentes entidades nacionales e internacionales especialistas en temas de seguridad de la información y ciberseguridad.

53. Reporte de eventos de seguridad de la información

Todos los empleados de EPM deben reportar las anomalías o eventos sospechosos tan pronto como sea posible, con el fin de evitar que ocurran incidentes de seguridad de la información y ciberseguridad en la operación.

Para el reporte de estos eventos, se actúa conforme a lo definido en el instructivo “gestión de incidentes de la seguridad de la información”, que está a cargo del personal del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología.

54. Planes de contingencia y recuperación de TI /TO

Los responsables de los activos y ciberactivos a su cargo gestionan la elaboración o actualización de los planes de contingencia y recuperación. Estos planes incluyen la documentación necesaria para la restauración o recuperación de un servicio o componente del sistema, de tal forma que se garantice la continuidad de la operación. La documentación y los planes de contingencia deben ser revisados y probados periódicamente, acorde con la normatividad que les aplique.

55. Análisis de Impacto de tecnología

Los responsables de los activos y ciberactivos deben realizar los análisis de impacto de las tecnologías de información y las tecnologías de operación, para identificar los requisitos de continuidad de las tecnologías que se encuentren a su cargo, los cuales deben estar alineados con el Análisis de Impacto del Negocio (BIA) realizado por el proceso de gestión de riesgos, identificando los tiempos objetivos de recuperación (RTO) y los puntos objetivos de recuperación (RPO).

56. Estrategia de recuperación tecnológica

Los responsables del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología apoyan la definición de las estrategias de recuperación tecnológica en TI. Los responsables de los procesos de negocios deben definir y disponer de los recursos y planes requeridos para la implementación de las estrategias de recuperación de tecnología, con el propósito de apalancar la continuidad del negocio, aumentando la resiliencia organizacional.

Para las tecnologías de operación, la definición de las estrategias de recuperación tecnológica está a cargo de los responsables de los procesos con el acompañamiento del personal del proceso de seguridad digital y continuidad de los servicios de tecnología, así como del personal de gestión de riesgos.

57. Plan de pruebas

Los servidores del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología junto con los responsables del macroproceso de tecnología e información definen el plan de pruebas anual para los planes de recuperación de tecnología de información. Dentro de la planeación anual, se consideran los recursos y las personas necesarios para las pruebas que se definan.

Para el caso de las tecnologías de operación se debe seguir el plan de pruebas de recuperación definido por los responsables de los procesos del negocio, con el acompañamiento del proceso de gestión de seguridad digital y continuidad de los servicios de tecnología.

58. Plan de recuperación de desastres (DRP)

Los proveedores de tecnología que suministren servicios o que soporten activos de información críticos para la organización deben evidenciar en los términos contractuales y en el contrato la definición e implementación de un plan de recuperación de desastres de acuerdo con el análisis de riesgos elaborado. Esta condición debe ser verificada por los responsables de los procesos o proyectos que requieren el servicio o la tecnología

Las presentes reglas de negocio rigen a partir de su publicación y sustituyen las reglas de negocio 1.5 y 1.6 contenidas en el manual de reglas de negocio asociadas al proceso diseño del servicio de TI pertenecientes al macroproceso gestión de tecnología de información.

Dado en Medellín, en ENERO 15 DE 2021

VPE. NUEVOS NEGOC, INNOV Y TEC | **DARIO AMAR FLOREZ**

ANEXO 1. GLOSARIO DE TÉRMINOS

El glosario de términos completo puede ser consultado en el sitio del sistema de gestión de seguridad de la información y ciberseguridad.

https://webapp.epm.com.co/site/SIG/DVG/DTL_ISO_27001/Forms/AllItems.aspx?RootFolder=%2Fsite%2FSIG%2FDVG%2FDTL%5FISO%5F27001%2FDocumentos%20de%20referencia&FolderCTID=0x0120009F6CB89B3665904FAE752A7FFB1AF40F&View=%7BFECE6DF8%2D5028%2D4815%2D9EC2%2D062FA33DEDAE%7D

A continuación, se listan las definiciones más relevantes para la comprensión de la regla de negocio.

DEFINICIONES

Acceso lógico: Es un acceso en red a través de la intranet de la compañía o de Internet. Los "puertos" son distintos tipos de accesos lógicos para entrar, acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información de identidad, con claves o direcciones de IP (Protocolo de Internet) en una lista permitida. (Techlandia, n.d.)

Acceso físico no escoltado. Son las restricciones que se implementan sobre un lugar, para evitar que a este accedan personas no autorizadas, esto se hace con el fin de mantener la seguridad sobre las instalaciones y las personas que normalmente se encuentran en ahí, además de proteger información y objetos valiosos. (guías prácticas.com, n.d.)

Activo crítico: Instalaciones, sistemas o equipo eléctrico que, si es destruido, degradado o puesto indisponible, afecte la confiablidad u operatividad del sistema eléctrico. Acorde con las recomendaciones del Comité Tecnológico del Concejo Nacional de Operación (CNO) para la definición de activos críticos que comprometan la seguridad de operación del Sistema Interconectado Nacional (SIN). (CNO, 2015)

Acuerdo de confidencialidad: Es un contrato por medio del cual las partes se comprometen a no revelar la información de carácter confidencial que les es suministrada. Dependiendo del contexto, estos acuerdos pueden tener efectos unilaterales o bilaterales. (Asuntos Legales, 2020)

Amenaza: Posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí. (CONPES 3995)

Arquitectura de referencia: Una arquitectura de referencia está formada por un documento o un conjunto de documentos que ofrecen estructuras e integraciones recomendadas de productos y servicios de TI para formar una solución. La arquitectura de referencia incorpora las mejores prácticas aceptadas del sector, que normalmente sugieren el método de entrega o las tecnologías concretas óptimas. (Hewlett Packard, n.d.)

Ataque cibernético: Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia). (Conpes 3701)

Ciber activo: Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota. (CNO, 2015)

Ciber activo crítico: Dispositivo para la operación confiable de activos críticos que cumple los atributos descritos a continuación:

- El ciber activo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
- El ciber activo usa un protocolo enrutable con un centro de control. o,
- El ciber activo es accesible por marcación (CNO, 2015)

Cifrado de Datos: En el mundo de la informática, el cifrado es la conversión de datos de un formato legible a un formato codificado, que solo se pueden leer o procesar después de haberlos descifrado. (Kaspersky, n.d.)

Ciberseguridad: Se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin. (CONPES3995)

Código fuente. Se entiende todo texto legible por un ser humano y redactado en un lenguaje de programación determinado. El objetivo del código fuente es crear normas y disposiciones claras para el ordenador y que este sea capaz de traducirlas a su propio

lenguaje. De este modo, el texto fuente es la base de los programas y de las páginas web. (IONOS,2020)

Confidencialidad. Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados. (Icontec, 2017)

Confiabilidad. Propiedad de la consistencia del comportamiento deseado y los resultados. (Icontec, 2017)

Controles criptográficos. La criptografía es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado. Existen dos tipos principales de criptografía: por un lado, la conocida como criptografía simétrica, más tradicional, y la criptografía asimétrica o de clave pública. (INCIBE , 2017)

Control de acceso. Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos (2.63) de negocio y de seguridad. (Icontec, 2017)

Cuenta técnica: Son las cuentas utilizadas por los sistemas de información o la tecnología para efectos de ejecución de los procesos, servicios o la comunicación.

Cuenta de usuario compartida: Una cuenta utilizada por varios usuarios para funciones comerciales normales por empleados o contratistas. Por lo general, en un dispositivo que no admite usuarios individuales
Cuentas (NERC CIP-007-006

CSIRT: Equipo de Respuesta a Incidentes de Seguridad cibernética, por su sigla en inglés. Se refiere a una institución definida y concreta que tiene la responsabilidad de proveer capacidades de gestión de incidentes a una organización/sector en especial. Su objetivo es minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes. (CONPES3995)

Declaración de aplicabilidad: Es un elemento básico que establece los controles necesarios para gestión de riesgos. A la Declaración de Aplicabilidad también se le conoce en inglés como Statement of Applicability o SoA. (ISOTools, n.d.)
Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada. (Icontec, 2017)

Evento de seguridad de la información: Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, una falla en los controles o una situación previa desconocida hasta el momento y que puede ser relevante para la seguridad. (Icontec, 2017)
Por ejemplo: un usuario se conecta a un sistema, un intento fallido de un usuario para ingresar a una aplicación, el firewall que permite o bloquea un acceso, una notificación de un cambio de contraseña de un usuario privilegiado, etc. Un Evento de seguridad de la información no es necesariamente una ocurrencia maliciosa o adversa.

Gestión de incidentes de seguridad de la información: Procesos para la detección, reporte, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de la información. (Icontec, 2017)

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de
amenazar la seguridad de la información. (Icontec, 2017)

Un Incidente de Seguridad de la Información es la violación o amenaza inminente a la violación implícita o explícita de una política de seguridad de la información. También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad). Un incidente puede ser denunciado por los involucrados, o indicado por un único o una serie de eventos de seguridad informática. [NIST800-61, ISO 18044]. Como ejemplos de incidentes de seguridad podemos enumerar:

- Acceso no autorizado
- Robo de contraseñas
- Robo de información
- Denegación de servicio

Infraestructura crítica: Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación. (Resolución CRC 2258 de 2009). (Conpes 3701)

Infraestructura crítica: Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación. (Resolución CRC 2258 de 2009).

Mínimo Privilegio: Operar bajo el principio del menor privilegio, tal como su nombre lo indica, parte de la premisa de otorgar los permisos necesarios y suficientes a un usuario para desempeñar sus actividades, por un tiempo limitado, y con el mínimo de derechos necesarios para sus tareas. Una práctica que se puede implementar en cuanto al uso de la tecnología, con el objetivo de procurar la seguridad de la información, así como nuestra privacidad. (Welivesecurity, 2018)

No repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las entidades que lo originaron. (Icontec, 2017)

Perímetro de Seguridad Electrónica: Es la frontera lógica con acceso controlado, que rodea una red dentro de la cual están conectados los Ciber Activos Críticos. (CNO, 2015)

Perímetro de Seguridad Física: Es la frontera física con acceso controlado, completamente contenida ("seis paredes") que rodea cuartos de control, cuartos de comunicaciones. centros de operación y otros sitios que alojan Ciber Activos Críticos. Puntos de acceso al (los) perímetro(s) de Seguridad Electrónica: Incluye todos los terminales de comunicación externamente conectados (por ejemplo: módems de marcación) que conecten con cualquier dispositivo dentro del Perímetro de Seguridad Electrónica. (CNO, 2015)

Plan de Recuperación de Desastres (DRP): Proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos. Esto también debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave, aunque esto no sea cubierto en este artículo, el propósito es la protección de datos.

Plan de tratamiento de riesgo: El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad (controles), y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad. (MinTic, 2019)

Principio de mínimo privilegio. El principio del menor privilegio es una estrategia de seguridad, aplicable a distintos ámbitos, que se apoya en la idea de otorgar únicamente permisos cuando son necesarios para el desempeño de cierta actividad. (welivesecurity, 2018)

Puntos de acceso al (los) perímetro(s) de Seguridad Electrónica: Incluye todos los terminales de comunicación externamente conectados (por ejemplo: módems de marcación) que conecten con cualquier dispositivo dentro del Perímetro de Seguridad Electrónica. (CNO, 2015)

Resiliencia: La resiliencia se refiere al proceso de, capacidad para, o resultado de una adaptación exitosa a pesar de circunstancias desafiantes o amenazantes" (Masten, Best, & Garmezy, 1991).
Una capacidad universal que permite a una persona, un grupo o una comunidad impedir, disminuir o superar los efectos nocivos de la adversidad.
Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Conpes 3854)

Riesgo de seguridad digital: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan. (CONPES, 2016)

Segregación de funciones: Método que usan las organizaciones para separar las responsabilidades de las diversas actividades que intervienen en la elaboración de los estados financieros, incluyendo la autorización y registro de transacciones, así como mantener la custodia de activos. La segregación de funciones también representa una actividad de control clave que afecta a todas las aseveraciones en los estados financieros. Como resultado, una segregación de funciones o inapropiada puede representar un aspecto importante para las organizaciones originando debilidades materiales o deficiencias significativas en los controles internos. Esto es porque dichas deficiencias pueden resultar en una mayor posibilidad de fraude, errores, o irregularidades en los procesos, en el procesamiento de transacciones y en reportes financieros. (KPMG, n.d.)

Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información. (Icontec, 2017)

Seguridad Lógica: Consiste en la aplicación de barreras que resguarden el acceso a los datos y solo se permite acceder a ellos a las personas autorizadas. (http://www.segu-info.com). (Conpes 3701)

TIC (Tecnologías de la Información y las Comunicaciones): Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC). (Conpes 3701)

Tecnologías de la Operación (T.O.): Están dedicada a detectar o cambiar los procesos físicos a través de la monitorización y el control de dispositivos también físicos, como tuberías o válvulas, sensores, controladores, actuadores, etc.

Transacción: Evento que genera o modifica los datos que se encuentran eventualmente almacenados en un sistema de información.
Tomado de*: Perspectivas relacionadas con el riesgo de TI: "Un enfoque basado en riesgos para la segregación de funciones" de Ernst & Young.*

Transacción Sensible: Una transacción de negocios que tiene el potencial de afectar los estados financieros de una compañía.
Tomado de*: Perspectivas relacionadas con el riesgo de TI: "Un enfoque basado en riesgos para la segregación de funciones" de Ernst & Young*

Usuario. Para efectos de la Regla de Negocio, **"**Usuario" son los empleados, miembros de junta directiva, contratistas y demás personas autorizadas por el responsable del Proceso que acceden a los activos y ciber activos de la organización.

Vulnerabilidad. Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3995)