ANEXO IX

SEGURIDAD EN LAS COMUNICACIONES

1. OBJETIVO

Garantizar la adopción de las medidas necesarias para dar un marco de seguridad inherente a todos los procesos que se relacionen con las tecnologías de la información y la comunicación del Organismo, es decir con el conjunto de recursos (hardware, software, redes, etc.) usados en la obtención, procesamiento, almacenamiento, administración, emisión y transmisión de información. Asimismo, la información transmitida a través de las redes del Organismo debe ser protegida y controlada adecuadamente, tanto dentro de la organización como aquella que es transferida fuera de las instalaciones del Organismo.

2. ALCANCE

Todos los servicios de comunicaciones que incluyen la obtención, procesamiento, almacenamiento, administración, emisión y transmisión de información dentro y fuera de la S.R.T..

3. DEFINICIONES

Comunicaciones electrónicas: Es el tipo de anuncio o notificación que se desarrolla a través de una computadora o dispositivos similares como tablets y/o teléfonos inteligentes.

Comunicaciones inalámbricas: es aquella que no se encuentra unida por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio.

Enlaces L2L (Lan to Lan): es un servicio de transmisión de datos punto a punto, el cual permite conectar fácilmente dos sedes del Organismo sin necesidad de convertir protocolos o medios.

Firewall: Es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos.

Niveles de Servicio (SLA) (o *Service Level Agreement* por sus siglas en inglés): Es un acuerdo escrito entre el proveedor de servicio y el Organismo con el objeto de fijar el nivel acordado para la calidad del servicio.

Proxy: Un servidor proxy es un ordenador que puede conectarse como interfaz entre dos ordenadores o redes. Asume una función de intermediario, recibiendo peticiones y transmitiéndolas con su propia dirección IP a otra red.

Red: infraestructura y servicios de interconexión que permite el intercambio de información en el Organismo. Se entienden como servicios de red en el ámbito de la S.R.T.:

- Gestión de servicios de internet (enlaces de Comisiones Médicas)
- Gestión de enlaces L2L
- Gestión de Firewall Core y de borde
- Administración de solución de antivirus, antispam
- Gestión de servicios para navegación en Proxys
- Administración de equipamiento de comunicaciones, como switch, router, etc
- Gestión de conexiones y accesos remotos (VPN)
- Gestión de certificados para firmas digitales

Router: Es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino.

Switch: Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

VPN: La VPN de acceso remoto (Remote Access VPN) permite al personal conectarse a una red privada para acceder a servicios y recursos de forma remota. Esta conexión es segura y se realiza a través de internet mediante un servidor de acceso remoto.

VLAN: Se denominan redes de área local virtuales. Pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) debe definir junto con la Subgerencia de Sistemas (S.S.), según corresponda, las medidas de seguridad de los servicios de red, comunicaciones e intercambio de información de la S.R.T..

El RSI debe controlar los mecanismos de distribución y difusión de la información dentro de la S.R.T., en caso de ser requerido. Asimismo, debe analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet del personal.

Por otro lado, debe definir y documentar lineamientos respecto al uso aceptable de los dispositivos, correo electrónico e Internet, y elaborar procedimientos adecuados de concientización para del personal en materia de seguridad sobre estos aspectos.

El RSI debe, asimismo, emitir criterios respecto a la incorporación de cláusulas de confidencialidad o de no divulgación para la protección de la información de la S.R.T. en todos los acuerdos que se suscriban donde haya transferencia de información.

La S.S. colabora con el RSI en la definición de las medidas de seguridad sobre los servicios de red, comunicaciones e intercambio de información de la S.R.T., y coordina su implementación.

Debe llevar a cabo las actividades operativas de los procesos relacionados a la gestión de las comunicaciones, y asegurar el registro de las actividades realizadas.

La S.S. en conjunto con el RSI debe aprobar las plataformas para el intercambio de información autorizadas para su transporte cuando sea requerido, de acuerdo a su nivel de criticidad.

Los Titulares de las Unidades Organizativas determinan la autorización para la provisión del servicio de cuentas del correo electrónico institucional para el personal a su cargo, así como deben identificar la sensibilidad de la información y aprobar su transmisión como responsables de la información de su ámbito de competencia.

Todo el personal de la S.R.T. es responsable del cumplimiento de los lineamientos que se emitan sobre el uso aceptable de los dispositivos brindados por el organismo, correo electrónico institucional, Internet e Intranet. Todo el personal que se desempeñe en la S.R.T. debe hacer uso de la cuenta de correo electrónico institucional que le brinde el Organismo para toda comunicación vinculada con sus funciones.

5. CONTENIDO

5.1 SEGURIDAD DE LOS SERVICIOS DE RED

Se deben definir las pautas para garantizar la seguridad de los servicios de red de la S.R.T., sean tanto públicos como privados. Asimismo, tanto para los servicios de red internos o externos

(subcontratados), deberán definirse requisitos en relación a la calidad de servicio mediante acuerdos de Niveles de Servicio (SLA) de acuerdo a la normativa interna vigente.

5.1.1 Seguridad de los Servicios de Red

Se deberá tener en cuenta los siguientes aspectos para establecer las pautas para garantizar la seguridad de todos los servicios de red de la S.R.T.:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados;
- Controlar el acceso físico y lógico a los servicios, tanto a su uso como a su administración;
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar;
- Instalar periódicamente las actualizaciones de seguridad;
- Revisar periódicamente dicha configuración.

5.1.2 Separación de Redes

Se deberá diseñar e implementar una estrategia respecto a una separación de redes que permita establecer la seguridad en las comunicaciones de la S.R.T. Para esto, se deberán tener en cuenta los siguientes aspectos:

- La infraestructura disponible en sedes y Comisiones Médicas, así como también sus principales elementos físicos;
- El tipo de redes disponibles. Las redes inalámbricas son particularmente vulnerables con respecto a la seguridad y esto deberá considerarse como parte de la estrategia de segregación;
- El tipo de segregación o separación (física o lógica).

5.2 GESTIÓN DE LA SEGURIDAD EN LA RED

5.2.1 Controles de Red

Se deben definir controles para garantizar la seguridad de los datos y los procesos de intercambio de información que involucren servicios de conectividad como redes, internet, enlaces privados, etc., considerando la ejecución de las siguientes acciones:

- Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias;
- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados;
- Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas;
- Garantizar, mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de comunicaciones;
- Verificar que los enlaces hayan sido configurados con los protocolos de seguridad adecuados;
- Verificar la configuración y operación de los dispositivos de seguridad -como firewall y soluciones perimetrales- que estén implementadas dentro de las oficinas S.R.T.;
- Para las redes de Comisiones Médicas, establecer lineamientos que permitan mantener una navegación segura;
- En las Comisiones Médicas y oficinas, relevar y corroborar que las VLAN establecidas correspondan con los servicios que están configurados de acuerdo con el modelo de operación establecido.

- Para el desarrollo de las acciones antes mencionadas, se considerarán los siguientes aspectos;
- La segregación, en la medida de las posibilidades, de los grupos de servicios de información, usuarios y sistemas en las redes;
- Los principales elementos físicos y virtuales a gestionar dentro de la red que le dan soporte y, especialmente, los que interconectan con el exterior (routers, switch, firewall, etc.), y todos los servicios inherentes a transmisión de datos;
- Cuando la información se transfiera a través de redes inalámbricas, considerar controles adicionales para mantener las conexiones (disponibilidad), la privacidad (confidencialidad) y la integridad de los datos.

5.2.2 Monitoreo y Registro

Se deben definir parámetros respecto al monitoreo y registro de las actividades en la red. El monitoreo será utilizado para establecer medidas preventivas, correctivas y, si es necesario, acciones de cambio tendientes a minimizar los posibles eventos de seguridad que fueran detectados.

5.3 TRANSFERENCIA DE INFORMACIÓN

El intercambio de información juega un rol muy importante en las comunicaciones que mantiene el personal de la S.R.T. en su quehacer cotidiano con otras partes interesadas, sean estas internas o externas al Organismo.

5.3.1 Criterios de utilización de los servicios de Red

Se deberán emitir criterios sobre el intercambio de información a través del uso de todos los tipos de instalaciones de comunicación, considerando lo siguiente:

- Protección de la información intercambiada en la intercepción, copiado, modificación, en la posibilidad de que sea mal dirigida, y en su destrucción;
- Detección y protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas;
- Definición del uso aceptable de las instalaciones de comunicación electrónicas;
- Uso seguro de comunicaciones inalámbricas;
- Responsabilidades del personal contratado, contratista y cualquier otra/o usuaria/o de no comprometer al Organismo, por ejemplo, a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación electrónica, compras no autorizadas y cualquier otro medio (ej.: redes sociales);
- Uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información, cuando esta sea requerida;
- Directrices de retención y eliminación para todas las comunicaciones electrónicas en concordancia con las leyes y regulaciones relevantes, locales y nacionales;
- Instrucción al personal sobre las precauciones que deben tomar a la hora de transmitir información de la S.R.T..

Las medidas de seguridad deberán definirse en función de la naturaleza del remitente, el destinatario y los soportes utilizados.

Asimismo, se deben establecer lineamientos sobre el uso aceptable de dispositivos, correo electrónico, herramientas colaborativas (como la mensajería instantánea) e Internet.

5.3.2 Consideraciones sobre el uso de plataformas y medios digitales externos

Se deberá emitir criterios respecto de los requisitos de seguridad y los controles a ejecutar sobre las diversas plataformas y medios digitales que se utilicen como medio de contacto institucional de la S.R.T. para el intercambio de información.

Se deberán considerar las siguientes medidas de seguridad en los intercambios de información por medio de estas plataformas y medios digitales:

- Protección de la información ante el acceso no autorizado, modificaciones o denegación de servicio;
- Confiabilidad y disponibilidad general del servicio;
- Consideraciones legales, por ejemplo, requerimientos para firmas digitales o electrónicas;
- Obtención de aprobación previa al uso de los servicios públicos externos;
- Controles de autenticación para los accesos desde las redes públicamente accesibles.

5.3.3 Acuerdos de intercambio de información

Cuando se celebren acuerdos de servicios (a través de diversas plataformas, ya sean virtuales, mensajería, aplicativos o software), se deberán establecer mecanismos de transferencia segura para el intercambio de información. Para ello se deben tener en cuenta los siguientes aspectos:

- Identificación de la sensibilidad de la información y aprobación de los Propietarios de la Información;
- Responsabilidades y vigencias para el control y la notificación de transmisiones, envíos y recepciones;
- Pautas técnicas para el encapsulado, la transmisión, la notificación de emisión, envío y recepción;
- Responsabilidades y obligaciones en caso de pérdida, exposición o divulgación no autorizada de datos;
- Información sobre la propiedad de la información suministrada y las condiciones de su uso;
- Pautas técnicas para la grabación y lectura de la información, en caso de corresponder.

5.3.4 Controles sobre el servicio de correo electrónico

Se deberá exigir el uso de la cuenta de correo electrónico institucional a todos los agentes y funcionarios del Organismo para toda comunicación vinculada con sus funciones, e informar los riesgos de su incumplimiento.

Por su parte, se deben considerar las siguientes medidas de seguridad y establecer los controles pertinentes para el servicio de correo electrónico institucional:

- Protección de mensajes contra el acceso no autorizado, modificaciones o denegación de servicio;
- Correcta asignación de la dirección y el transporte del mensaje;
- Confiabilidad y disponibilidad general del servicio;
- Consideraciones legales, por ejemplo, requerimientos para firmas electrónicas;
- Estrategias sobre los controles de autenticación para los accesos.

Asimismo, se deberá tener en cuenta la inclusión de un descargo de responsabilidad respecto al tratamiento y la confidencialidad de la información perteneciente a la S.R.T..

Por otra parte, se deberá determinar a qué personas internas y a qué personas externas se les autorizará a tener una cuenta del correo electrónico institucional, y se deberá gestionar la asignación de una cuenta de correo electrónico a las personas autorizadas a recibir este servicio.

5.3.5 Convenio de confidencialidad y divulgación por transferencia de información

Se deben definir, implementar y revisar regularmente los convenios de confidencialidad para la protección de la información de la S.R.T. cumpliendo con toda legislación o normativa que alcance a la S.R.T. en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal de la S.R.T. como con aquellos/as terceros/as que se relacionen de alguna manera con su información.

Los acuerdos deben contemplar, entre otros, los siguientes aspectos:

- La naturaleza de la información;
- La duración del acuerdo;
- El proceso a llevar a cabo en caso de rescisión;
- Las responsabilidades y las propiedades sobre la información;
- El uso permitido de la información;
- Las penalidades en caso de una infracción;
- Cláusulas que obliguen a mantener el deber de confidencialidad incluso una vez extinta la relación profesional entre las dos partes involucradas;
- El conocimiento de la PSI S.R.T..

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66585749-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO IX Seguridad en las Comunicaciones-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 7 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:40:51 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:52:58 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:52:59 -03:00